Application Firewall PRO версия 4.5.0

Руководство администратора

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 25.09.2026

Содержание

1. Об этом документе ... 9
   - 1.1. Условные обозначения ... 9
   - 1.2. Другие источники информации о PT AF ... 10
2. О PT AF ... 11
3. Архитектура PT AF ... 12
4. Аппаратные и программные требования ... 18
   - 4.1. Аппаратные требования ... 18
   - 4.2. Программные требования ... 19
   - 4.3. Требования к сетевой инфраструктуре ... 20
5. Лицензирование ... 23
6. Вход в PT AF ... 27
7. Интерфейс PT AF ... 28
   - 7.1. Главное меню ... 28
   - 7.2. Страница События безопасности ... 29
   - 7.3. Страница События агрегации ... 31
   - 7.4. Страница Схема конфигурации ... 31
   - 7.5. Страница Система ... 33
   - 7.6. Просмотр состояния применения конфигурации ... 34
   - 7.7. Смена языка интерфейса ... 36
   - 7.8. Смена темы интерфейса ... 36
8. Настройка защиты веб-приложений ... 37
   - 8.1. Режимы защиты веб-приложений ... 37
   - 8.2. Настройка защиты веб-приложения в изолированном пространстве с типом PT AF ... 38
     - 8.2.1. Настройка защищаемых серверов ... 41
       - 8.2.1.1. Добавление защищаемого сервера ... 41
       - 8.2.1.2. Добавление защищаемого сервера на основе существующего ... 41
       - 8.2.1.3. Удаление защищаемого сервера ... 42
     - 8.2.2. Настройка IP-адресов для прослушивания ... 42
       - 8.2.2.1. Создание прослушиваемого IP-адреса ... 43
       - 8.2.2.2. Создание прослушиваемого IP-адреса на основе существующего ... 44
       - 8.2.2.3. Удаление прослушиваемого IP-адреса ... 44
     - 8.2.3. Настройка исходящих IP-адресов ... 45
       - 8.2.3.1. Создание исходящего IP-адреса ... 45
       - 8.2.3.2. Создание исходящего IP-адреса на основе существующего ... 45
       - 8.2.3.3. Удаление исходящего IP-адреса ... 46
     - 8.2.4. Добавление SSL-сертификата ... 46
     - 8.2.5. Добавление закрытого ключа ... 47
     - 8.2.6. Настройка профилей трафика ... 47
       - 8.2.6.1. Создание профиля трафика с внутренней балансировкой нагрузки ... 47
       - 8.2.6.2. Создание профиля трафика с внешней балансировкой нагрузки без контроля IP-адресов ... 48
       - 8.2.6.3. Создание профиля трафика с внешней балансировкой нагрузки и контролем IP-адресов ... 49

8.2.6.4. Создание профиля трафика на основе существующего ... 50
8.2.6.5. Удаление профиля трафика ... 51
8.2.7. Управление списками отозванных сертификатов ... 51
8.2.7.1. Добавление списка отозванных сертификатов ... 51
8.2.7.2. Синхронизация списка отозванных сертификатов ... 52
8.2.8. Создание действия для управления HTTP-заголовками ... 52
8.2.9. Создание веб-приложения в изолированном пространстве с типом PT AF ... 54
8.2.9.1. Создание нового веб-приложения ... 54
8.2.9.2. Создание веб-приложения на основе существующего ... 57
8.2.10. Настройка конфигураций SSL ... 57
8.3. Настройка защиты веб-приложения в изолированном пространстве с типом Агент ... 59
8.4. Алгоритм выбора веб-приложения для обработки и проксирования запроса ... 61
9. Работа с политиками и шаблонами политик безопасности ... 63
9.1. О политиках и шаблонах политик безопасности ... 63
9.2. Создание шаблона политики безопасности веб-приложений ... 64
9.3. Изменение политик безопасности нескольких веб-приложений ... 64
9.4. Изменение политики безопасности одного веб-приложения ... 65
10. Работа с правилами обработки трафика ... 66
10.1. О наборах правил ... 66
10.2. Группы правил обработки трафика ... 67
10.3. Параметры правил обработки трафика ... 69
10.4. Группировка правил ... 69
10.5. Изменение правила политики безопасности веб-приложения ... 70
10.6. Отключение правила обработки трафика ... 70
10.7. Исключение ложных срабатываний правила ... 70
10.8. Изменение ответа защищаемого сервера ... 72
10.9. Создание правила и добавление его в пользовательский набор ... 73
11. Работа с действиями ... 75
11.1. Создание действия ... 75
11.2. Изменение действия ... 76
11.3. Удаление действия ... 77
11.4. Типы действий ... 77
11.5. Ограничения на использование действий в правилах обработки трафика ... 83
11.6. Переменные для создания действий ... 83
12. Работа с глобальными списками ... 88
12.1. Создание статического списка ... 89
12.2. Создание динамического списка ... 89
12.3. Изменение статического списка ... 89
12.4. Удаление глобального списка ... 90
12.5. Применение изменений в статических списках ... 90
12.6. Поиск IP-адреса в глобальных списках ... 91
12.7. Добавление IP-адресов в динамический список вручную ... 91
12.8. Удаление IP-адреса из динамического списка ... 91
12.9. Экспорт данных глобального списка ... 91
12.10. Настройка пользовательского правила с использованием глобального списка ... 92

12.11. Настройка исключений с использованием глобального списка ... 93
13. Работа с событиями безопасности ... 94
13.1. Работа со списком событий безопасности ... 97
13.2. Фильтрация событий безопасности ... 98
13.3. Работа с личными фильтрами ... 99
13.4. Просмотр карточки события безопасности ... 101
13.4.1. Просмотр информации о событии безопасности ... 101
13.4.2. Просмотр данных запроса и ответа в необработанном виде ... 101
13.5. Запись информации о событии безопасности в БД системы ... 102
13.6. Работа с отчетами о событиях безопасности ... 103
14. Работа с событиями агрегации ... 105
14.1. О событиях агрегации ... 105
14.2. Работа со списком событий агрегации ... 106
14.3. Фильтрация событий агрегации ... 107
14.4. Просмотр карточки события агрегации ... 108
14.5. Настройка агрегации ... 108
15. Администрирование PT AF ... 110
15.1. Управление учетными записями ... 111
15.1.1. Создание локальной учетной записи ... 111
15.1.2. Приглашение пользователя другого изолированного пространства ... 112
15.1.3. Изменение локальной учетной записи ... 113
15.1.4. Удаление локальной учетной записи ... 113
15.1.5. Настройка параметров безопасности учетных записей ... 113
15.2. Смена своего пароля ... 114
15.3. Настройка LDAP-подключений ... 115
15.3.1. Создание LDAP-подключения ... 115
15.3.2. Изменение LDAP-подключения ... 116
15.3.3. Удаление LDAP-подключения ... 117
15.3.4. Настройка соответствия ролей PT AF и групп Microsoft Active Directory ... 117
15.3.5. Изменение соответствия ролей PT AF и групп Microsoft Active Directory ... 118
15.3.6. Удаление соответствия ролей PT AF и групп Microsoft Active Directory ... 118
15.3.7. Запуск синхронизации с Microsoft Active Directory вручную ... 119
15.4. Настройка OAuth-подключений ... 119
15.5. Управление ролями ... 121
15.5.1. Создание роли ... 122
15.5.2. Изменение роли ... 122
15.5.3. Удаление роли ... 123
15.6. Управление изолированными пространствами ... 123
15.6.1. Создание изолированного пространства ... 124
15.6.2. Изменение изолированного пространства ... 125
15.6.3. Удаление изолированного пространства ... 125
15.6.4. Особенности применения конфигурации в зависимости от количества подов ... 126
15.6.5. Особенности обработки трафика на сервере Envoy ... 126
15.6.6. Особенности обработки трафика на сервере nginx ... 127
15.7. Тонкая настройка обработки трафика в изолированных пространствах ... 127

15.7.1. Настройка утилиты traffic_settings.py ... 128
15.7.2. Определение значения параметра base_url ... 129
15.7.3. Изменение параметров изолированного пространства с помощью утилиты ... 129
15.7.4. Настройка отображения информации о неуспешных попытках аутентификации по сертификатам ... 137
15.8. Управление ICAP-серверами ... 138
15.8.1. Добавление ICAP-сервера ... 138
15.8.2. Изменение параметров ICAP-сервера ... 139
15.8.3. Удаление ICAP-сервера ... 140
15.9. Управление кластером Kubernetes ... 140
15.9.1. Подготовка узла к добавлению в кластер ... 140
15.9.2. Добавление узла в кластер ... 141
15.9.3. Изменение имени узла кластера ... 142
15.9.4. Удаление узла из кластера ... 143
15.10. Мониторинг состояния PT AF ... 144
15.10.1. Мониторинг встроенными средствами ... 144
15.10.2. Мониторинг состояния в Grafana ... 145
15.11. Установка доверенного сертификата для веб-интерфейса PT AF ... 146
15.12. Обновление базы знаний ... 147
15.12.1. Обновление базы знаний через веб-интерфейс ... 147
15.12.2. Проверка обновления на наличие конфликтов ... 148
15.12.3. Просмотр отчета об обновлении ... 149
15.13. Работа с лицензией ... 149
15.13.1. Получение фингерпринта ... 150
15.13.2. Загрузка лицензии ... 150
15.13.3. Активация лицензии ... 151
15.13.4. Просмотр информации о лицензии PT AF ... 151
15.14. Об архивации журнала событий ... 152
15.15. Настройка взаимной TLS-аутентификации клиента с агентом PT AF ... 152
15.16. Настройка отправки сообщений о событиях аудита на удаленный syslog-сервер ... 152
15.17. Резервное копирование и восстановление данных PT AF ... 153
15.17.1. Создание резервной копии ... 154
15.17.2. Восстановление данных из резервной копии ... 154
15.17.3. Скачивание резервной копии ... 155
15.17.4. Удаление резервной копии ... 155
15.18. Экспорт и импорт параметров защиты приложений ... 155
15.18.1. Экспорт параметров защиты приложений ... 156
15.18.2. Импорт параметров защиты приложений ... 157
15.18.3. Управление асинхронным импортом параметров защиты ... 157
15.19. Синхронизация объектов между экземплярами PT AF ... 158
15.19.1. Настройка экземпляров PT AF для синхронизации ... 159
15.19.2. Управление учетной записью синхронизации ... 161
15.19.2.1. Активация учетной записи (включение синхронизации) ... 161
15.19.2.2. Генерация новой строки подключения ... 161
15.19.2.3. Деактивация учетной записи (выключение синхронизации) ... 162
15.19.3. Выбор экземпляров PT AF для синхронизации ... 162

15.19.4. Управление состоянием синхронизации экземпляров ... 163
15.19.5. Включение автоматической синхронизации ... 164
15.20. Настройка декодирования запросов и ответов ... 165
15.21. Тонкая настройка применения конфигурации ... 166
15.21.1. Настройка механизма поэтапного применения конфигурации ... 166
15.21.2. Настройка разделения подов на виртуальные группы ... 169
15.21.3. Настройка механизма плавного завершения сессии ... 169
15.22. Настройка журналирования работы агента ... 172
15.23. Настройка отправки данных из журналов access.log и error.log во внешние SIEM-системы ... 173
15.24. Отправка событий от агентов в SIEM-системы ... 178
15.24.1. Установка Fluent Bit в виде deb-пакета ... 179
15.24.2. Установка Fluent Bit в виде Helm Chart ... 181
15.24.3. Настройка агента для отправки событий в SIEM-систему ... 185
15.25. Обновление базы GeoIP для агента ... 187
15.25.1. Агент установлен из deb-пакета или ISO-образа ... 187
15.25.2. Агент установлен из Docker-образа ... 188
15.26. Изменение списка NTP-серверов ... 189
15.27. Скрытие информации о версии nginx из сообщения об ошибке ... 190
16. Интеграция PT AF с Grafana ... 192
16.1. Установка Grafana ... 192
16.2. Смена сертификата для веб-интерфейса Grafana ... 192
16.3. Настройка передачи данных о работе PT AF на отдельный сервер с Grafana ... 193
17. Решение проблем ... 194
17.1. Просмотр информации о системе PT AF ... 194
17.2. Проблемы, связанные с лицензиями ... 195
17.3. Ошибки при установке PT AF ... 195
17.4. Не переименовались сетевые интерфейсы ... 199
17.5. Метрики для мониторинга работы PT AF ... 199
17.6. Ошибка при обновлении узла PT AF ... 204
17.7. Не запускается под после обновления ... 205
17.8. Не отправляются события на syslog-сервер после обновления Docker-агента ... 205
17.9. На схеме конфигурации не отображается сервер и профиль обработки трафика ... 206
17.10. Ошибка восстановления из резервной копии ... 207
17.11. Исключение узла из обработки трафика ... 208
17.12. Особенности маршрутизации исходящего трафика ... 208
17.13. Проблема подключения агента ... 209
17.14. Сбор системных журналов ... 210
17.14.1. Выгрузка системного журнала с помощью сервиса Grafana ... 210
17.14.2. Выгрузка журнала сетевых событий на клиентской стороне ... 211
17.14.3. Выгрузка системных журналов с помощью утилиты harvester ... 212
17.14.4. Выгрузка системных журналов уровня debug ... 213
18. О технической поддержке ... 215
Приложение A. Команды оболочки WSC ... 219
A.1. Служебные команды WSC ... 220
A.2. Информационные команды WSC ... 223

А.3. Команды настройки подключения WSC к сервису конфигурации ... 224
А.4. Команды настройки параметров DHCP-клиента ... 225
А.5. Команды настройки сетевых интерфейсов ... 226
А.6. Команды сбора и реконфигурации кластера Kubernetes ... 230
А.7. Команды генерации ключей SSH ... 235
А.8. Команды настройки пула NTP-серверов ... 235
А.9. Команды управления сетевыми маршрутами ... 236
А.10. Команды настройки виртуальных IP-адресов ... 242
А.11. Часто задаваемые вопросы о работе с WSC ... 243
Приложение Б. Справочник по языку пользовательских правил ... 245
Б.1. Переменные ... 247
Б.1.1. Локальные переменные ... 247
Б.1.2. Параметры правила ... 248
Б.1.3. Контекстные переменные ... 249
Б.2. Функции ... 257
Б.3. Операторы ... 263
Б.4. Типы данных ... 265
Б.5. Прочие элементы языка ... 266
Приложение В. Конструктор исключений для запуска правила ... 268
Приложение Г. Справочник по языку фильтрации событий безопасности ... 271
Приложение Д. Индикаторы состояния PT AF в Grafana ... 278
Д.1. Индикатор ClickHouse ... 279
Д.2. Индикатор Consul ... 280
Д.3. Индикатор CPU ... 281
Д.4. Индикатор DISK ... 284
Д.5. Индикатор ETCD ... 286
Д.6. Индикатор K8S ... 287
Д.7. Индикатор Minio ... 294
Д.8. Индикатор Network ... 295
Д.9. Индикатор Nodes ... 308
Д.10. Индикатор PG SQL ... 310
Д.11. Индикатор PTAF Backend ... 312
Д.12. Индикатор RabbitMQ ... 313
Д.13. Индикатор RAM ... 315
Д.14. Индикатор RPS / app errors ... 318
Предметный указатель ... 319
Глоссарий ... 322

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию Positive Technologies Application Firewall (далее также — PT AF). Руководство также содержит инструкции по установке PT AF и использованию основных функций продукта.

Руководство адресовано специалистам, администрирующим PT AF.

Комплект документации PT AF включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке и обновлению продукта.
- Справочное руководство — содержит дополнительную справочную информацию о правилах обработки трафика в PT AF.
- Справочное руководство по REST API — содержит информацию о доступных функциях сервиса REST API в PT AF.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о PT AF (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите **ОК**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример	Описание
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT AF

Вы можете найти дополнительную информацию о PT AF на справочном портале help.ptsecurity.com и на Позитивном портале. Через Позитивный портал вы также можете обратиться в техническую поддержку (см. раздел 18).

2. О PT AF

PT AF — инновационная система защиты, которая точно обнаруживает и блокирует атаки, включая самые опасные атаки по версии организаций OWASP и WASC, DDoS-атаки на уровне приложения и атаки нулевого дня. PT AF обеспечивает непрерывную защиту приложений, пользователей и инфраструктуры и помогает соответствовать стандартам безопасности.

Преимуществами PT AF перед другими средствами защиты веб-приложений являются:

— высокий уровень защиты при минимальном количестве ложных срабатываний;

— высокий уровень автоматизации;

— блокирование современных атак, таких как HPP, HPC и XXE;

— гибкие модели развертывания (программно-аппаратный комплекс, виртуальный комплекс);

— возможность построения отказоустойчивой конфигурации active — active с поддержкой механизмов горизонтального масштабирования, без потери производительности и остановки сервиса;

— мультиарендность, заложенная в основу архитектуры системы;

— возможность подключения нескольких площадок за счет использования агентов или дополнительных серверов обработки трафика.

3. Архитектура PT AF

PT AF разработан на основе платформы управления контейнерами Kubernetes. Благодаря особенностям архитектуры вы можете подключать дополнительные аппаратные ресурсы, а также масштабировать отдельные модули в составе комплекса. Это позволяет внедрять PT AF в компаниях любого размера и адаптировать его к различным типам нагрузки.

В состав PT AF входят:

- Веб-интерфейс для взаимодействия с пользователем (см. раздел 7) и интерфейс для взаимодействия с внешними системами автоматизации (см. Справочное руководство по REST API).
- Сервисы для управления конфигурацией, выполнения периодических задач, мониторинга и поддержания работы всех составляющих системы.
- Встроенные базы данных и системы хранения:
  - ClickHouse — хранит информацию о событиях безопасности и действиях пользователей системы.
  - PostgreSQL — хранит конфигурацию PT AF.
  - MinIO — хранит крупные бинарные объекты (например, резервные копии и отчеты).
- Сервисы, отвечающие за обработку защищаемого трафика.

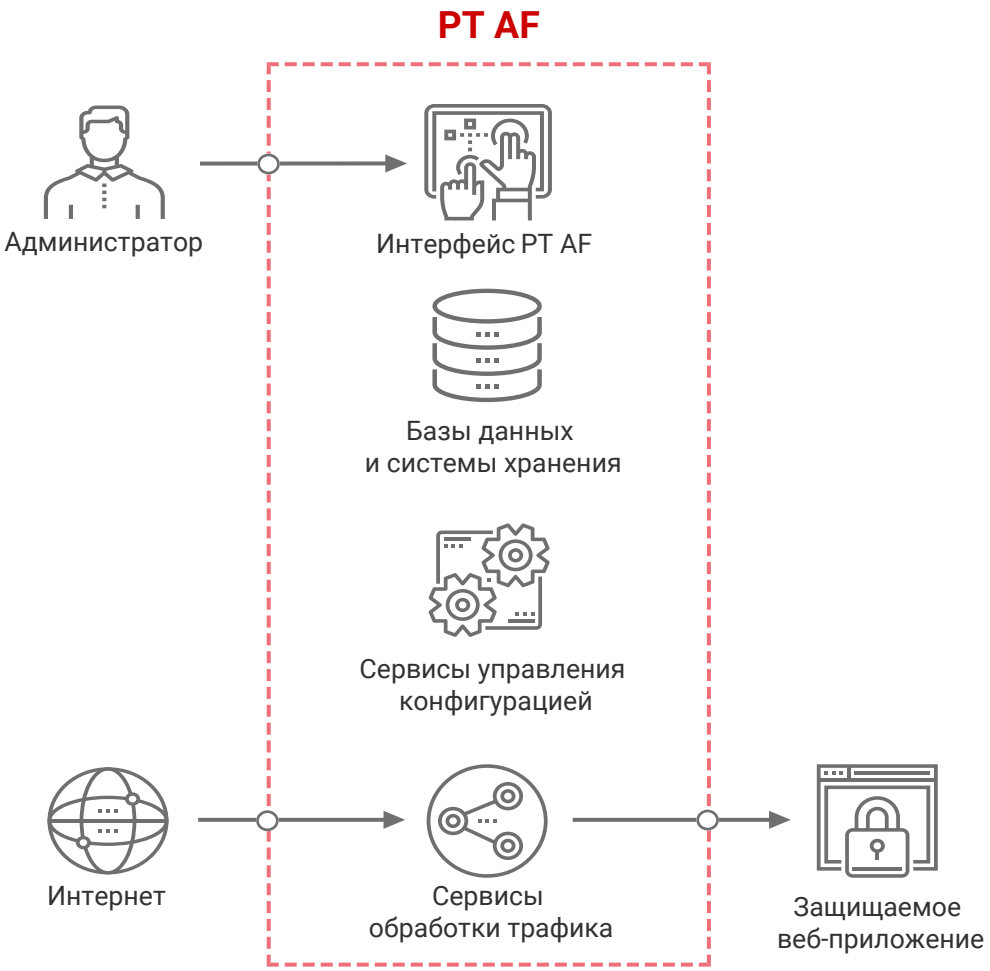


Рисунок 1. Архитектура системы

PT AF спроектирован с учетом возможности распределенной установки и архитектурно состоит из сервисов, что упрощает масштабирование и настройку. В качестве системы оркестрации сервисов используется платформа Kubernetes.

Kubernetes состоит из подов и сервисов. Под — минимальная рабочая единица приложения в Kubernetes, набор контейнеров, которые совместно используют ресурсы, конфигурацию и хранилища. Сервис — сущность Kubernetes, которая предоставляет доступ к приложению независимо от количества доступных подов. Сервис оперирует информацией о подах в приложении и распределяет нагрузку. Если одно приложение в Kubernetes обращается к другому, запрос попадет на сервис второго приложения и далее распределится на один из подов.

Масштабирование PT AF обеспечивается с помощью кластерной конфигурации с добавлением дополнительных узлов. Дополнительные узлы используются для повышения пропускной способности, обеспечения защиты большого количества веб-приложений и размещения системы в определенных сетевых сегментах.

Вне зависимости от количества узлов Kubernetes позволяет управлять большим объемом ресурсов, выделяемых для разных задач, обеспечивая высокую доступность, а также позволяет легко выполнить установку, так как сервисы распределяются по узлам кластера автоматически.

Схема взаимодействия компонентов

В рамках взаимодействия от сервисов управления конфигурацией PT AF к сервисам обработки трафика передаются конфигурация и параметры безопасности, а в обратном направлении — информация о событиях безопасности и данные мониторинга. Такое разделение необходимо для обеспечения возможности отчуждения сервисов обработки трафика не только на соседние узлы в основном центре обработки данных, но и на узлы, находящиеся в дополнительном центре.

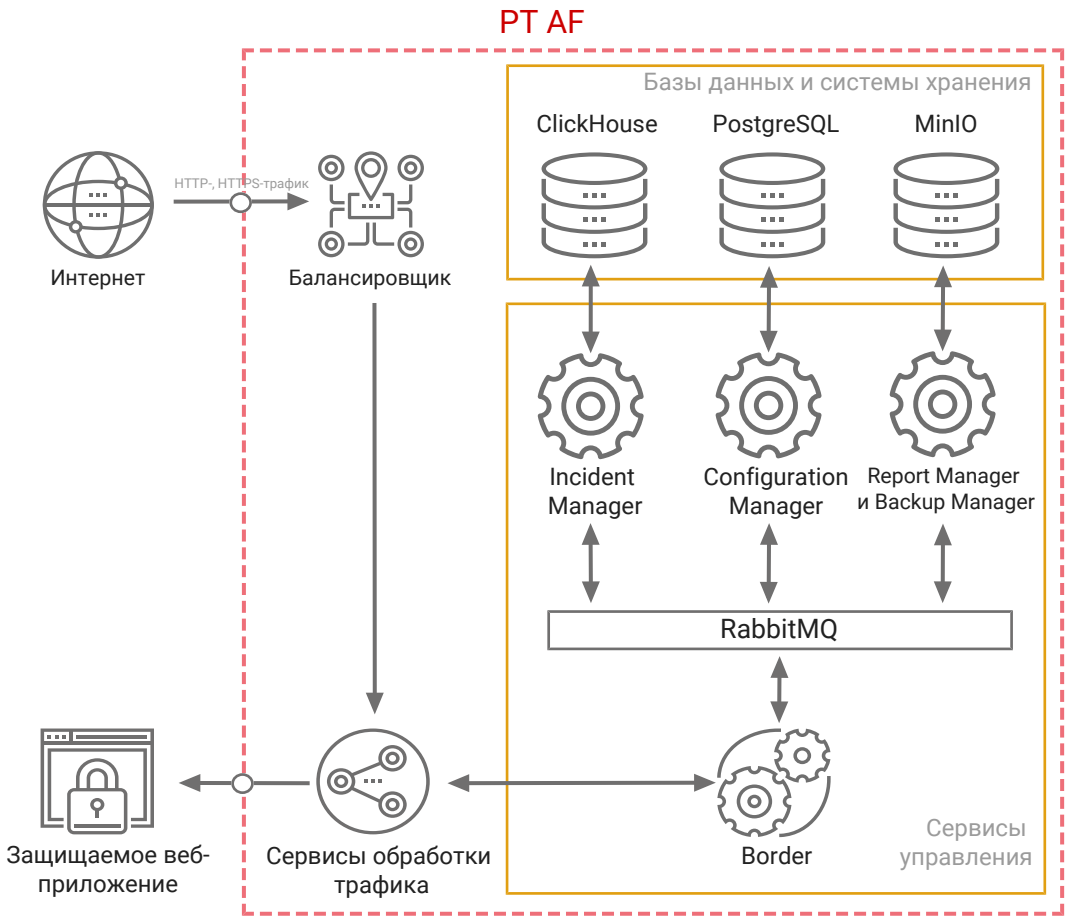


Рисунок 2. Схема взаимодействия компонентов

Сервисы управления конфигурацией и мониторинга состояния

Внутреннее взаимодействие сервисов PT AF выполняется через брокер сообщений RabbitMQ.

Сервисы для управления конфигурацией PT AF и мониторинга его состояния выполняют следующие функции:

— управляют данными пользователей, а также генерируют токены аутентификации;

— обеспечивают взаимодействие с сервисами обработки трафика;

— обеспечивают сохранение и выборку событий безопасности в СУБД ClickHouse (Incident Manager);

— осуществляют передачу данных между базами данных и их обработку;

— выполняют взаимодействие с внешними системами;

— размещают объекты в файловом хранилище MinIO (Report Manager, Backup Manager);

— анализируют состояние узлов обработки трафика;

— выполняют отправку запросов к REST API и веб-интерфейсу (REST Proxy);

— анализируют состояние задач (Task Manager) и управляют их запуском;

— управляют уведомлениями в PT AF;

— обеспечивают работу сервисов Consul и Grafana (в том числе Grafana Loki);

— выполняют сбор метрик контейнеров в Kubernetes.

Обработка трафика

Сервисы обработки трафика обрабатывают и проксируют клиентский трафик, а также проверяют полученные события безопасности при помощи правил агрегации. Перед каждым модулем с сервисами обработки трафика расположен балансировщик нагрузки. Поскольку балансировщик нагрузки может находиться на любом из узлов кластера, для приема трафика используется виртуальный IP-адрес. Минимальное количество модулей обработки трафика — 2. При повышении нагрузки количество обработчиков может быть увеличено до 30.

Модуль обработки трафика может размещаться на базовых и дополнительных узлах кластера или на агенте PT AF.

Агент PT AF — это компонент, который обеспечивает обработку трафика и взаимодействие с основным центром обработки данных PT AF для получения политик безопасности и отправки событий безопасности. Агенты устанавливаются на отдельные веб-серверы nginx и используются для снижения нагрузки на систему и при нестабильном соединении между основным центром обработки данных и дополнительными узлами.

При потере соединения с центром обработки данных агент некоторое время может обрабатывать трафик без подключения к PT AF. При этом изменения в политике безопасности будут применены для обработки трафика на агенте только после восстановления соединения. В связи с этим для корректной обработки трафика при потере соединения с PT AF не рекомендуется останавливать работу nginx.

Ограничением на количество агентов служит лицензируемая максимальная полоса пропускания.

Балансировка трафика

По умолчанию трафик распределяется между узлами с помощью внутреннего балансировщика Ingress Kubernetes, который назначает узел для приема трафика и узлы для его обработки.

В PT AF предусмотрена возможность получения трафика от внешнего управляемого балансировщика. Такие балансировщики должны развертываться перед модулями обработки трафика и распределять нагрузку по узлам PT AF, отправляя запросы HealthCheck и анализируя ответы на них.

Возможны следующие варианты внешних балансировщиков нагрузки:

— Без контроля IP-адресов — трафик распределяется между узлами как с помощью PT AF, так и с помощью внешнего балансировщика. PT AF отображает информацию о доступных IP-адресах и портах, на которых может прослушиваться трафик, а также предоставляет сведения о количестве подов, используемых на каждом узле для обработки трафика. Созданием таких подов управляет кластер Kubertenes, который может не создавать поды на всех узлах кластера. Данные о доступных IP-адресах, порте для прослушивания и обрабатывающих трафик подах необходимо использовать для настройки внешнего балансировщика и оптимального распределения трафика.

— С контролем IP-адресов — трафик распределяется между выбранными вами узлами с помощью внешнего балансировщика.

Внешний балансировщик может быть развернут в дополнительном центре обработки трафика или в той же сети, что и базовые узлы кластера.

Подробнее о балансировке нагрузки см. в разделе о настройкой о настройке защиты веб-приложения (см. раздел 8).

Изолированные пространства

Изолированное пространство (англ. tenant) — это ограниченная среда, которая позволяет двум или более пользователям независимо использовать одну и ту же систему. По умолчанию в PT AF настроено изолированное пространство, в котором работает администратор.

Трафик изолированного пространства обрабатывается на узлах PT AF или на агенте. При использовании кластера настраиваются зоны доступности, которые определяют, на каких узлах кластера будет выполняться обработка трафика. Обработчики трафика взаимодействуют с сервисами управления конфигурацией PT AF через сервис Border (ptaf-border). При этом защищаемые веб-приложения, события безопасности, политики безопасности, сетевые параметры и прочие объекты системы индивидуальны для каждого изолированного пространства.

> **Примечание.** Минимальное количество обработчиков трафика для изолированного пространства — два, при повышении нагрузки количество обработчиков может быть увеличено до тридцати.

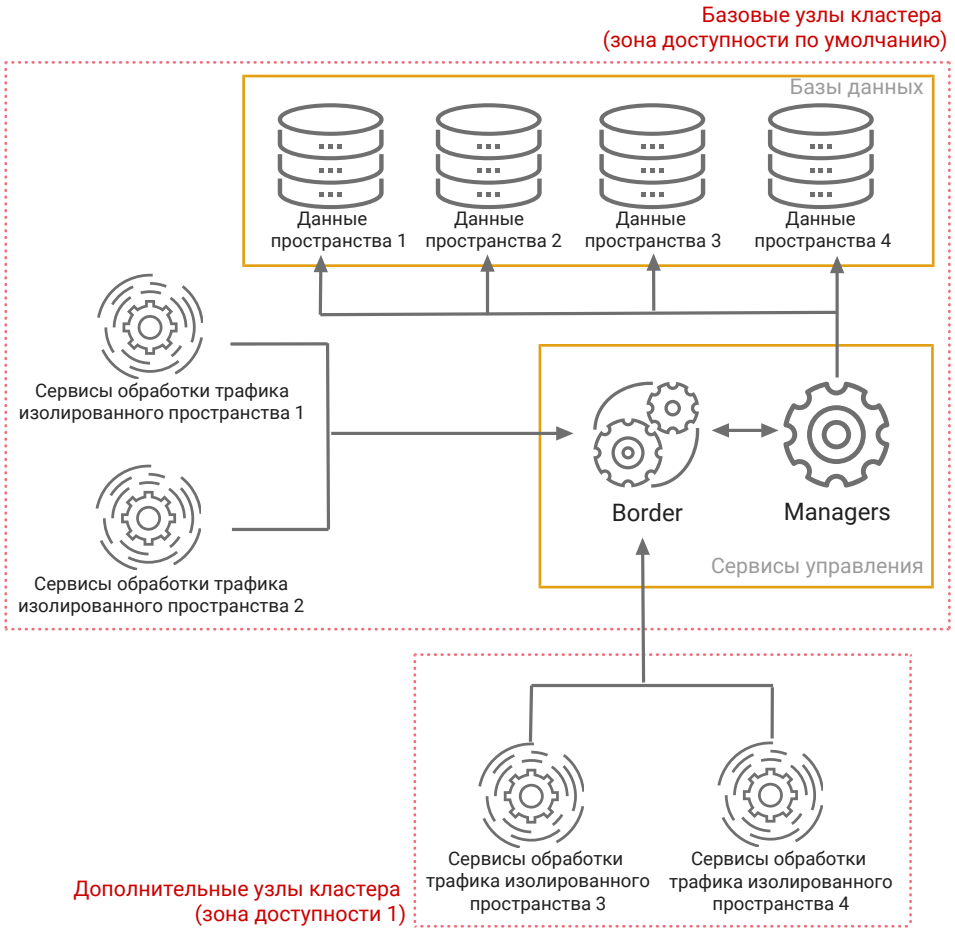


Рисунок 3. Изолированные пространства в кластерной конфигурации

При повышении нагрузки в одном из изолированных пространств автоматически увеличивается количество подов, на которых развернуты сервисы обработки трафика, независимо от количества подов для обработки трафика других пространств (при доступности системных ресурсов).

Подробности в разделе «Управление изолированными пространствами (см. раздел 15.6)».

Принцип работы с трафиком

PT AF может работать с сетевым трафиком в режиме обратного прокси-сервера. Этот режим обеспечивает соединение «в разрыв», в котором PT AF выступает в качестве прокси-сервера между клиентом и защищаемым веб-приложением.

4. Аппаратные и программные требования

В этом разделе приведены аппаратные и программные требования для установки и работы PT AF.

В этом разделе

Аппаратные требования (см. раздел 4.1)

Программные требования (см. раздел 4.2)

Требования к сетевой инфраструктуре (см. раздел 4.3)

4.1. Аппаратные требования

Внимание! В этом разделе приведены минимальные аппаратные требования, достаточные лишь для обработки небольшого объема трафика. Для полноценного и продуктивного функционирования PT AF рекомендуется определить необходимые ресурсы совместно с менеджером Positive Technologies, исходя из требуемой производительности системы.

Вы можете развертывать PT AF как на физических серверах, так и в виртуальной среде.

Требования к физическому серверу

При установке PT AF на блочные устройства поддерживаются аппаратные RAID-контроллеры MegaRAID серий 93xx, 94xx и 95xx. Не поддерживаются виртуальные RAID-контроллеры VROC.

Рекомендуемые чипсеты сетевых карт — Intel X722, Intel X710, Intel 82599ES или Intel i350.

Таблица 2. Минимальные требования к физическому серверу

Компонент	Минимальные требования
Центральный процессор	Суммарно 16 логических ядер, поддержка инструкций AVX
Память (ОЗУ)	32 ГБ
Жесткий диск (HDD)	1 ТБ
Твердотельный накопитель (SSD)	480 ГБ [2]
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый

2 При синхронной записи на накопитель 99 перцентиль задержки не должен превышать 10 миллисекунд.

Требования к виртуальной машине

Для развертывания PT AF в виртуальной среде рекомендуется использовать системы виртуализации KVM, zVirt или VMware ESXi (версий не ниже 6.0). Вычислительные ресурсы для виртуальных машин нужно выделять без переподписки.

Таблица 3. Минимальные требования к виртуальной машине

Компонент	Минимальные требования
Центральный процессор	Суммарно 12 логических ядер. Поддержка инструкций AVX и технологий виртуализации Intel-VT и AMD-V
Память (ОЗУ)	24 ГБ
Жесткий диск (HDD)	300 ГБ
Твердотельный накопитель (SSD)	128 ГБ [2]
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый

Таблица 4. Минимальные требования к виртуальной машине для агента

Компонент	Минимальные требования
Центральный процессор	1 логическое ядро. Поддержка инструкций AVX2 и технологий виртуализации Intel-VT и AMD-V
Память (ОЗУ)	8 ГБ [1]
Жесткий диск (HDD)	При установке агента из ISO-образа — 108 ГБ, для остальных вариантов установки — 10 ГБ
Сетевой адаптер	1 порт со скоростью 1 Гбит/с

Примечание. В дальнейшем планируется поддержка процессоров с инструкциями AVX-512. Рекомендуется заранее перейти на серверы с такими процессорами.

4.2. Программные требования

PT AF совместим с 64-разрядными серверными англоязычными версиями операционных систем Debian 11 и Astra Linux Special Edition версий 1.7.10 и 1.8.5 в режиме защищенности «Воронеж». Кроме того, агент поддерживает работу на Debian 11, Debian 12 и на Astra Linux версий 1.7.10 и 1.8.5.

1 Указанный минимальный объем ОЗУ требуется для корректной работы модуля разделяемой памяти (shared memory). Во избежание возникновения большинства ошибок выделения страниц разделяемой памяти рекомендуется увеличить объем ОЗУ до 64 ГБ.

Внимание! Не рекомендуется устанавливать антивирусы в операционной системе. Это может помешать установке PT AF, вызвать сбои в его работе или привести к другим непредсказуемым последствиям.

Для установки агента из deb-пакета вам потребуется веб-сервер nginx или Envoy. Список версий веб-серверов в зависимости от установленной ОС приведен в таблице ниже.

Таблица 5. Версии веб-серверов для установки агента

ОС	Версии nginx	Версии Envoy
Astra Linux	1.26.0	—
Debian 11	1.18.0, 1.24.0, 1.30.2	1.35.3
Debian 12	1.30.2	1.35.3

Если нет возможности установить поддерживаемую версию веб-сервера, вы можете отправить запрос в службу технической поддержки Positive Technologies для разработки агента под вашу версию веб-сервера.

Внимание! Во избежание конфликтов между модулями PT AF и nginx для установки агентов рекомендуется использовать ptaf-nginx — веб-сервер nginx, модифицированный для нужд PT AF.

Для работы в веб-интерфейсе PT AF рекомендуется использовать браузер Google Chrome версии 60.0 или выше.

4.3. Требования к сетевой инфраструктуре

На узлах PT AF нужно разрешить входящие и исходящие подключения к портам, указанным в таблице.

Внимание! Взаимодействие между узлами PT AF через сетевые интерфейсы с ролью `CLUSTER` не нужно ограничивать правилами межсетевого экрана.

Таблица 6. Порты взаимодействия узлов PT AF с компонентами информационной системы

Компонент	Протокол и порт	Роль сетевого интерфейса	Назначение
Входящие подключения			
Клиент веб-приложения	HTTP или HTTPS (TCP, любой порт[7])	WAN	Обмен трафиком через прослушиваемые IP-адреса (см. раздел 8.2.2)
Рабочая станция администратора	SSH (TCP 22013[3] или TCP 22[4])	MGMT	Удаленный доступ к серверу PT AF
	HTTPS (TCP 443[5])	MGMT	Доступ к интерфейсу PT AF и к сервису публичного API
	HTTPS (TCP 3000[5])	MGMT	Мониторинг состояния PT AF
Агент	TCP 8443[5]	MGMT	Получение событий безопасности, управление конфигурацией агента
Приложение, взаимодействующее с PT AF через API	HTTPS (TCP 443[5])	MGMT	Доступ к сервису публичного API
Исходящие подключения			
Защищаемый веб-сервер	HTTP или HTTPS (TCP, любой порт)	LAN	Обмен трафиком через исходящие IP-адреса (см. раздел 8.2.3)
DNS-сервер	DNS (TCP 53, UDP 53)	MGMT	Разрешение доменных имен
Syslog-сервер	Syslog (TCP 514, UDP 514)	MGMT	Отправка сообщений стандарта syslog в MaxPatrol SIEM или другие системы для централизованного сбора и анализа событий ИБ

7 Для каждого профиля трафика с внешней балансировкой нагрузки без контроля IP-адресов PT AF открывает динамический порт из диапазона 30001—65535. При использовании других вариантов балансировки (см. раздел 8.2) порт указывает пользователь.

3 Если PT AF развернут на Debian.

4 Если PT AF развернут на Astra Linux.

5 Порт по умолчанию. Вы можете сменить порт при настройке виртуальных IP-адресов.

Компонент	Протокол и порт	Роль сетевого интерфейса	Назначение
NTP-сервер	NTP (UDP 123 [6])	MGMT	Синхронизация времени

6 Требуется только для узла предварительной настройки кластера.

5. Лицензирование

Для работы PT AF и его защиты от нелегального использования нужна лицензия.

Основные параметры лицензирования

Основными параметрами лицензирования являются полоса пропускания трафика в Мбит/с и максимально возможная производительность (RPS). Полоса пропускания трафика — это сумма всего трафика, проходящего через все обработчики трафика PT AF (включая агенты). Полоса распределяется между подключенными обработчиками трафика динамически. Если через один из обработчиков трафик не проходит, то и полоса пропускания на него не расходуется.

Таблица 7. Возможная пропускная способность PT AF

Максимально возможная производительность, RPS	**Полоса пропускания трафика, Мбит/с**
1000	100
3000	300
5000	500
10 000	1000
20 000	2000
50 000	5000
100 000	10 000

Типы лицензий

Лицензии различаются по сроку действия и по производительности системы.

По сроку действия выделяются следующие типы лицензий:

- **Срочные.** Такие лицензии имеют обозначенный срок действия, который отображается в веб-интерфейсе PT AF. До окончания срока действия необходимо приобрести лицензию на продление. Без продления срочной лицензии PT AF перестанет обрабатывать трафик защищаемого приложения, а доступ к веб-интерфейсу будет заблокирован.
- **Бессрочные.** Такие лицензии ограничены только сроком технической поддержки Positive Technologies и возможностью обновлять базу знаний через веб-интерфейс. После отключения поддержки PT AF продолжит обрабатывать трафик, веб-интерфейс PT AF будет доступен.

По производительности системы выделяются следующие типы лицензий:

- **Лицензия на один сервер (Standalone).** Подходит для случаев, когда трафик защищаемого приложения проходит через один сервер, на котором находятся сервисы для хранения параметров безопасности и информации об атаках. Максимальная полоса пропускания для установки на одном сервере — 1000 Мбит/с, максимально возможная производительность — 10 000 RPS.
- **Лицензия на кластер (Cluster).** Подходит для случаев, когда от PT AF требуется повышенная отказоустойчивость. Отказоустойчивый кластер продолжит полноценную работу даже при выходе из строя одного из узлов. Минимальное количество базовых узлов кластера — 3. Общее количество базовых узлов всегда может быть только нечетным. Максимальная полоса пропускания для кластера, состоящего только из трех базовых узлов — 2000 Мбит/с, максимально возможная производительность — 20 000 RPS. Также вы можете использовать в кластере дополнительные узлы для обработки трафика, что увеличит количество обрабатываемых запросов и максимальную производительность.

  Примечание. Если мощностей текущей лицензии недостаточно, вы можете расширить лицензию (см. раздел 5). Для этого обратитесь к вашему менеджеру Positive Technologies.

Рекомендации по выбору лицензии

Вы можете выбрать лицензию в зависимости от необходимого количества узлов и производительности системы.

Таблица 8. Рекомендуемые варианты лицензии

Количество базовых узлов	Вариант масштабирования	100 Мбит/с (1000 RPS)	300 Мбит/с (3000 RPS)	500 Мбит/с (5000 RPS)	1000 Мбит/с (10 000 RPS)	2000 Мбит/с (20 000 RPS)	5000 Мбит/с (50 000 RPS)	10 000 Мбит/с (100 000 RPS)	15 000/20 000 Мбит/с (150 000/200 000 RPS)
1	–	+	+	+	+	–	–	–	–
3	–	+	+	+	+	+	–	–	–
	От 2 до 4 узлов обработки трафика или агентов	–	–	–	–	+	+	+	–

Количество базовых узлов	Вариант масштаби-рования	100 Мбит/с (1000 RPS)	300 Мбит/с (3000 RPS)	500 Мбит/с (5000 RPS)	1000 Мбит/с (10 000 RPS)	2000 Мбит/с (20 000 RPS)	5000 Мбит/с (50 000 RPS)	10 000 Мбит/с (100 000 RPS)	15 000/20 000 Мбит/с (150 000/200 000 RPS)
5	От 6 до 8 узлов обработки трафика или агентов	–	–	–	–	–	–	+	+

В таблице указаны рекомендуемые варианты лицензии. Вы можете подключать агенты к любой конфигурации, а также неограниченное количество дополнительных узлов обработки трафика при использовании лицензии на кластер. Дополнительные серверы обработки трафика могут быть частично или полностью заменены агентами. Способы расширения лицензии описаны ниже.

Способы расширения лицензии

Вы можете расширить лицензию, если текущих мощностей серверов недостаточно.

Способы расширения лицензии на один сервер:

— Приобрести лицензию расширения, если необходимо увеличить полосу пропускания или максимальную производительность системы.

— Подключить агенты, если необходимо снизить нагрузку на сервер и увеличить количество процессоров для обработки запросов. Количество агентов не ограничено лицензией, но при прохождении трафика через агенты расходуется общая полоса пропускания, прописанная в лицензии.

Примечание. Максимальная полоса пропускания для лицензии на один сервер — 1000 Мбит/с, максимальная производительность — 10 000 RPS.

Способы расширения лицензии на кластер:

— Увеличить количество базовых узлов. Для этого необходимо приобрести дополнительную лицензию на два базовых узла, так как их общее количество может быть только нечетным. Этот вариант рекомендуется при большом количестве запросов и построении

разнообразной отчетности. Также увеличение количества базовых узлов потребуется при построении кластера для обработки более 10 000 Мбит/с трафика (100 000 RPS). Общее количество базовых узлов ограничено лицензией.

— Если основная нагрузка приходится на обработку трафика, то можно добавить только дополнительные узлы обработки трафика. Они включены в кластер, и PT AF следит за их состоянием. Такой вариант удобен, когда нужно обрабатывать трафик на нескольких площадках. В этом случае на основной площадке размещается управляющий кластер, а на дополнительных площадках разворачиваются дополнительные серверы обработки трафика.

  Количество дополнительных узлов обработки трафика не ограничено лицензией.

  При подключении дополнительных узлов максимальная полоса пропускания для кластера из трех базовых узлов — 10 000 Мбит/с, максимальная производительность — 100 000 RPS.

— Подключить агенты. Подключение агентов похоже на использование дополнительных узлов обработки трафика: можно так же подключать площадки и увеличивать вычислительные мощности для обработки трафика. При этом есть существенное отличие: управляющий кластер PT AF поставляет на агенты только конфигурацию параметров безопасности и не следит за состоянием агентов или синхронизацией между конфигурациями параметров безопасности и проксирования трафика. Использование агентов рекомендуется в средах с внешним автоматизированным управлением и мониторингом. Количество агентов не ограничено лицензией, но при прохождении трафика через агенты расходуется общая полоса пропускания, прописанная в лицензии.

  При подключении внешних агентов максимальная полоса пропускания для кластера из трех основных узлов — 10 000 Мбит/с, максимальная производительность — 100 000 RPS.

Процесс лицензирования

Процесс лицензирования состоит из следующих шагов:

1. Вы получаете ключ инициализации от вашего менеджера Positive Technologies по электронной почте.
2. В веб-интерфейсе PT AF вы вводите ключ инициализации, и PT AF создает фингерпринт.
3. Вы отправляете фингерпринт вашему менеджеру Positive Technologies по электронной почте, он создает файл лицензии и присылает его вам.
4. Вы загружаете файл лицензии через веб-интерфейс PT AF.

   Примечание. Если при добавлении лицензии в PT AF возникли ошибки, обратитесь в службу технической поддержки Positive Technologies.

Номер лицензии и срок ее действия вы можете проверить в веб-интерфейсе PT AF на странице **Лицензии**.

6. Вход в PT AF

Для входа в PT AF вам потребуются ссылка и учетные данные пользователя.

Вход с помощью логина и пароля

Для входа потребуются логин и пароль пользователя, также необходимо знать тип его учетной записи (локальная или доменная).

- Чтобы войти в PT AF:

  1. В адресной строке браузера введите ссылку.
  2. Введите логин и пароль.

     Примечание. При бездействии пользователя его сессия автоматически завершится через 15 минут. Вы можете продлить сессию, установив флажок **Запомнить меня** — тогда она завершится по истечении срока, установленного администратором (см. раздел 15.1.5).
  3. Если в PT AF настроено LDAP-подключение, установите флажок **Войти через LDAP**.
  4. Нажмите **Войти**.

     PT AF проверит введенные учетные данные. Если данные верные, откроется страница веб-интерфейса в соответствии с назначенными пользователю правами доступа. Если данные неверные — отобразится сообщение об ошибке.

Вход с помощью OAuth-подключения

Если в PT AF настроено OAuth-подключение (см. раздел 15.4), вы можете войти с помощью стороннего сервиса аутентификации.

- Чтобы войти в PT AF:

  1. В адресной строке браузера введите ссылку.
  2. Нажмите название OAuth-подключения.

     Вы будете перенаправлены на станицу ввода учетных данных внешнего сервиса аутентификации.
  3. Введите учетные данные для входа во внешний сервис аутентификации.

  При успешной аутентификации пользователя во внешнем сервисе PT AF получит токены доступа, откроется страница веб-интерфейса PT AF в соответствии с назначенными пользователю правами.

7. Интерфейс PT AF

В этом разделе приводится описание основных элементов пользовательского интерфейса, доступных после входа в PT AF.

В этом разделе

Главное меню (см. раздел 7.1)

Страница События безопасности (см. раздел 7.2)

Страница События агрегации (см. раздел 7.3)

Страница Схема конфигурации (см. раздел 7.4)

Страница Система (см. раздел 7.5)

Просмотр состояния применения конфигурации (см. раздел 7.6)

Смена языка интерфейса (см. раздел 7.7)

Смена темы интерфейса (см. раздел 7.8)

7.1. Главное меню

В верхней части любой страницы находится главное меню, которое обеспечивает доступ к основным функциям PT AF.



Рисунок 4. Главное меню PT AF

В главном меню находятся:

— Разделы для перехода к страницам PT AF:

- **События безопасности** — для работы с событиями безопасности (см. раздел 13).
- **События агрегации** — для работы с событиями агрегации (см. раздел 14).
- **Схема конфигурации** — для настройки защиты веб-приложений (см. раздел 8).
- **Система** — для управления изолированными пространствами (см. раздел 15.6), учетными записями пользователей (см. раздел 15.1) и их ролями (см. раздел 15.5), для работы с отчетами (см. раздел 13.6) и резервными копиями (см. раздел 15.17), для просмотра записей журнала аудита и информации о состоянии системы и ее сервисов, а также для синхронизации параметров защиты между экземплярами (см. раздел 15.19) PT AF.

— Кнопка для выбора изолированного пространства. При нажатии кнопки раскрывается список доступных пользователю (см. раздел 15.1.2) изолированных пространств. Справа от кнопки отображается название текущего изолированного пространства.

— Индикатор применения конфигурации (см. раздел 7.6).

— Кнопка для просмотра информации о системе (см. раздел 17.1) и лицензиях (см. раздел 15.13.4), просмотра руководства администратора, а также для перехода на портал технической поддержки Positive Technologies.

— Кнопка для смены языка интерфейса (см. раздел 7.7) и темы (см. раздел 7.8), а также для выхода из системы.

7.2. Страница События безопасности

На странице **События безопасности** находятся следующие элементы пользовательского интерфейса.

Диаграмма интенсивности трафика

Находится под главным меню (см. раздел 7.1) и показывает интенсивность трафика — количество запросов в секунду ко всем веб-приложениям изолированного пространства в определенный момент времени. С помощью этой диаграммы удобно анализировать всплески сетевой активности в сети организации.

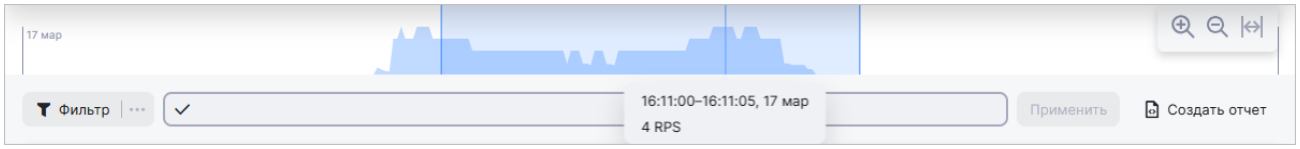


Рисунок 5. Диаграмма интенсивности трафика

При наведении курсора на диаграмму отображаются дата, время и скорость трафика. При выделении участка на диаграмме данные в рабочей области страницы будут отфильтрованы в соответствии с выделенным временным периодом. В правой части диаграммы находятся кнопки для увеличения , уменьшения и сброса масштаба.

Панель фильтрации

Позволяет фильтровать события безопасности с помощью условий.



Рисунок 6. Панель фильтрации

Условия определяют содержимое диаграммы и таблицы событий безопасности. В левой части панели находятся кнопки для работы с личными фильтрами (см. раздел 13.3), в правой части — кнопка **Создать отчет** для создания отчетов (см. раздел 13.6).

Диаграмма событий безопасности

Показывает статистику событий безопасности за выбранный период. При наведении курсора на столбец диаграммы отображается количество событий по уровням опасности за временной промежуток, соответствующий выбранному столбцу. При выделении участка на диаграмме данные в рабочей области страницы будут отфильтрованы в соответствии с выделенным временным периодом.

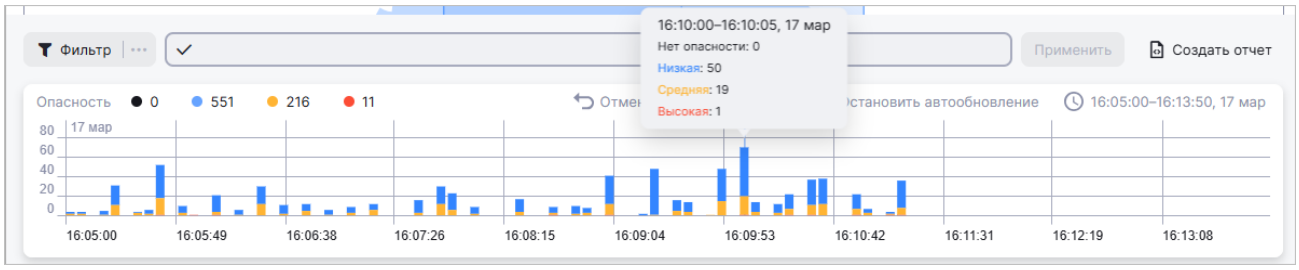


Рисунок 7. Диаграмма событий безопасности

Над диаграммой в левой верхней части панели приведена статистика по уровням опасности событий за выбранный период: каждому уровню соответствует цветной значок, справа от значка отображается количество событий этого уровня. Вы можете фильтровать события по нажатию на значок.

В правой верхней части панели находятся кнопки для остановки и запуска автоматического обновления диаграммы, для обновления диаграммы вручную, а также для выбора периода фильтрации.

Таблица событий безопасности

В таблице отображаются события, соответствующие выбранным условиям фильтрации.

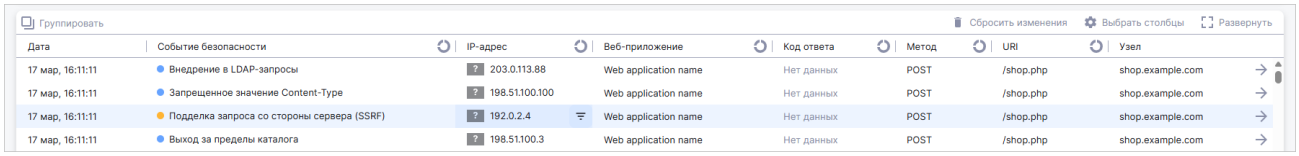


Рисунок 8. Таблица событий безопасности

Над таблицей находятся кнопки для группировки событий, выбора отображаемых в таблице параметров событий и изменения ее размера. Также вы можете сортировать записи о событиях, просматривать статистику по событиям и информацию о каждом событии (см. раздел 13.4.1), изменять размер и расположение столбцов в таблице, перетаскивая их мышью.

Расположение столбцов можно вернуть к изначальному виду по кнопке **Выбрать столбцы** → **Сбросить**. По умолчанию данные в таблице обновляются каждые 10 секунд, автообновление можно отключить.

7.3. Страница События агрегации

На странице **События агрегации** находятся следующие элементы пользовательского интерфейса.

Панель фильтрации

Находится под главным меню (см. раздел 7.1) и позволяет фильтровать события агрегации по IP-адресу, названиям правил и приложений, по времени, а также отображать только те события, для которых период блокировки IP-адреса еще не закончился.

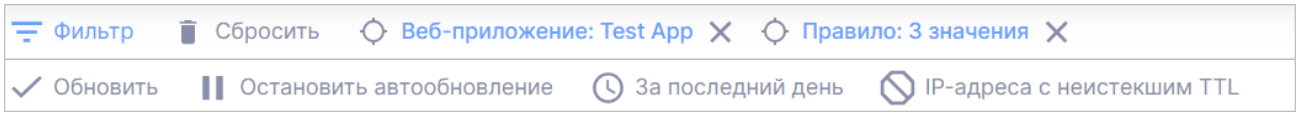


Рисунок 9. Панель фильтрации

Таблица событий агрегации

В таблице отображаются события, соответствующие выбранным условиям фильтрации.

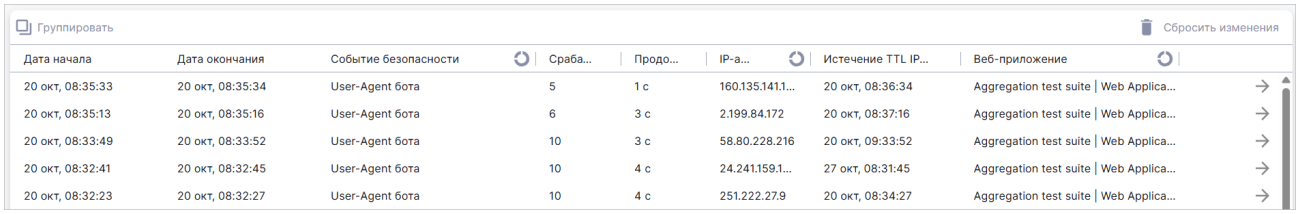


Рисунок 10. Таблица событий агрегации

Вы можете группировать и сортировать события, просматривать статистику по событиям и информацию о каждом событии (см. раздел 14.4), изменять размер и расположение столбцов в таблице, перетаскивая их мышью.

Таблицу можно вернуть к изначальному виду по кнопке **Сбросить изменения**. По умолчанию данные в таблице обновляются каждые 10 секунд, автообновление можно отключить.

7.4. Страница Схема конфигурации

На странице **Схема конфигурации** находятся следующие раскрывающиеся блоки:

- **Профили трафика** — такие объекты, как профили обработки входящего трафика, прослушиваемые IP-адреса, созданные в рамках изолированного пространства.
- **IP-адреса для прослушивания** — IP-адреса, которые PT AF будет использовать для приема клиентских запросов и проксирования их на защищаемое веб-приложение, а также для внутренней балансировки трафика между узлами кластера и для внешней балансировки в качестве доверенных.

— **Сертификаты SSL** — цепочки сертификатов для расшифровки HTTPS-трафика, отправляемого на защищаемые серверы.

— **Закрытые ключи SSL**— ключи для расшифровки HTTPS-трафика, отправляемого на защищаемые серверы.

— **Веб-приложения** — веб-приложения, защита которых настроена в рамках изолированного пространства.

— **Шаблоны политик безопасности** — пользовательские шаблоны политик безопасности, созданные в рамках изолированного пространства.

— **Набор пользовательских правил** — пользовательские правила, созданные в рамках изолированного пространства.

— **Наборы системных правил** — системные шаблоны политик безопасности, доступные во всех изолированных пространствах.

— **Действия** — пользовательские действия с трафиком при срабатывании правила, созданные в рамках изолированного пространства.

— **Глобальные списки** — списки IP-адресов в формате CIDR. Списки используются для блокировки адресов при обращении к приложению или исключения их из блокировки.

— **Защищаемые серверы** — серверы с веб-приложениями, защита которых настроена в рамках изолированного пространства.

— **IP-адреса для исходящих запросов** — IP-адреса, которые PT AF будет использовать для исходящих запросов на защищаемые серверы.

На странице **Схема конфигурации** по нажатию на кнопку в строке какого-либо объекта будут показаны все связи этого объекта. Строка выбранного объекта подсвечивается голубым цветом. Также голубым цветом подсвечиваются связанные объекты из блоков **Профили трафика**, **Веб-приложения**, **IP-адреса для прослушивания** и **Защищаемые серверы**: эти связи позволяют проследить перенаправление трафика. Все прочие связанные объекты заштриховываются.

На схеме конфигурации вы можете:

— просмотреть параметры объекта PT AF по кнопке ;

— просмотреть состояние объекта PT AF по нажатию на строку с названием объекта;

— добавить объект PT AF по кнопке в соответствующем блоке схемы;

— экспортировать или импортировать параметры защиты приложений (см. раздел 15.18) по кнопке .

См. также

На схеме конфигурации не отображается сервер и профиль обработки трафика (см. раздел 17.9)

7.5. Страница Система

На странице **Система** находятся вкладки, сгруппированные по следующим темам.

Контроль доступа

Группа содержит вкладки:

- **Роли** — для просмотра списка ролей, для их создания (см. раздел 15.5.1), изменения (см. раздел 15.5.2) и удаления (см. раздел 15.5.3).
- **Пользователи** — для просмотра списка учетных записей пользователей, для их создания (см. раздел 15.1.1), изменения (см. раздел 15.1.3) и удаления (см. раздел 15.1.4), а также для приглашения пользователей других изолированных пространств (см. раздел 15.1.2) в свое изолированное пространство.
- **Изолированные пространства** — для просмотра списка изолированных пространств, для их создания (см. раздел 15.6.1), изменения (см. раздел 15.6.2) и удаления (см. раздел 15.6.3), а также для выбора синхронизируемых экземпляров (см. раздел 15.19.3) PT AF и для настройки автоматической синхронизации (см. раздел 15.19.5) между экземплярами.
- **Безопасность учетных записей** — для настройки парольной политики и времени жизни сессии (см. раздел 15.1.5).
- **LDAP-подключения** — для просмотра и настройки LDAP-подключений (см. раздел 15.3.1), просмотра и настройки соответствия ролей и групп (см. раздел 15.3.4), а также для запуска синхронизации учетных записей (см. раздел 15.3.7) с Microsoft Active Directory.
- **OAuth-подключения** — для просмотра и настройки OAuth-подключений (см. раздел 15.4), которые позволяют пользователям входить в PT AF с помощью внешних сервисов аутентификации.
- **Учетная запись синхронизации** — для включения синхронизации объектов (см. раздел 15.19) с экземпляром-источником. Вкладка отображается в интерфейсе экземпляра-приемника.

Инструменты

Группа содержит вкладки:

- **Отчеты** — для просмотра списка выпущенных отчетов, а также для создания, скачивания и удаления отчета (см. раздел 13.6).
- **Резервные копии** — для создания резервной копии, сохранения копии в файл и ее загрузки из файла, для восстановления данных из резервной копии, а также для просмотра списка резервных копий и их удаления.
- **Импорт параметров защиты** — для импорта параметров защиты (см. раздел 15.18.2), а также для просмотра списка задач импорта и их статусов.

— **Отправка событий аудита** — для настройки отправки сообщений о событиях аудита на удаленный syslog-сервер.

— **ICAP-серверы** — для просмотра списка ICAP-серверов, для их добавления (см. раздел 15.8.1), изменения (см. раздел 15.8.2) и удаления (см. раздел 15.8.3).

— **Декодирование запросов и ответов** — для настройки декодирования запросов и ответов (см. раздел 15.20).

Мониторинг

Группа содержит вкладки:

— **Система** — для просмотра информации об общем состоянии системы и ее сервисов.

— **Журнал аудита** — для просмотра записей о действиях пользователей в PT AF, а также для просмотра записей о системных операциях и обновлениях базы знаний.

Синхронизация параметров защиты

Группа доступна только в веб-интерфейсе экземпляра-источника и содержит вкладки:

— **Экземпляры** — для управления экземплярами (см. раздел 15.19.1) PT AF, установленными в разных ЦОД.

— **Состояние синхронизации** — для синхронизации объектов между экземплярами (см. раздел 15.19.4) PT AF.

7.6. Просмотр состояния применения конфигурации

Для подов и агентов отслеживается статус применения конфигурации. Конфигурация — набор совместимых между собой компонентов из конфигурационных файлов. Вы можете посмотреть состояние применения конфигурации для подов и агентов в интерфейсе PT AF. Кнопка для просмотра состояния располагается в правой части главного меню (см. раздел 7.1).

В зависимости от состояния применения конфигурации кнопка может принимать вид:

✓ — все поды и агенты имеют актуальную конфигурацию.

◌ — производится применение новой конфигурации для подов и агентов.

! — возникли проблемы при применении конфигурации. Состояние означает, что конфигурация применяется более 5 минут или ее не удалось применить на подах или агентах. Если конфигурацию не удалось применить, поды и агенты продолжают работать на старой конфигурации. При возникновении проблем с применением конфигурации рекомендуется обратиться в техническую поддержку.

— конфигурация не была отправлена. Состояние означает, что для изолированного пространства типа PT AF не было настроено ни одного веб-приложения с подключенным к нему профилем трафика или для изолированного пространства типа «агент» не было подключено ни одного агента.

— примененная конфигурация является нерабочей, или есть поды или агенты без примененной конфигурации. Если есть поды или агенты на которых не удалось применить конфигурацию, рекомендуется обратиться в техническую поддержку. Если конфигурация является нерабочей, рекомендуется проверить правильность адресов и доступность защищаемых серверов или обратиться в техническую поддержку.

По нажатию на кнопку откроется всплывающая подсказка с информацией о статусе применения конфигурации статических и динамических подов или агентов, относящихся к текущему изолированному пространству. Каждому поду или агенту соответствует блок, который в зависимости от статуса применения конфигурации может:

- гореть зеленым — на поде или агенте применена актуальная конфигурация;
- мигать зеленым — конфигурация применяется на одном из подов или агентов;
- гореть желтым — новая конфигурация не применена из-за ошибок, при этом под или агент работает на старой конфигурации и обрабатывает трафик;
- гореть красным — новая конфигурация не применена из-за ошибок, старая конфигурация отсутствует, при этом модули не обрабатывают трафик;
- гореть черным — на поде отсутствует конфигурация, новый под на котором еще не началось применение конфигурации.

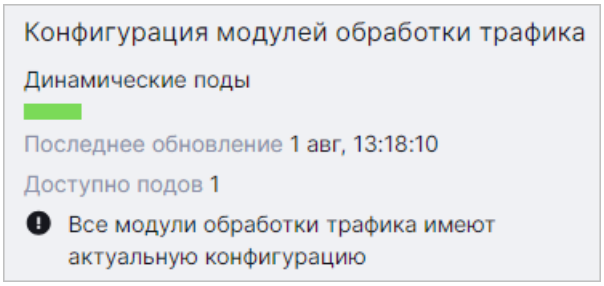


Рисунок 11. Окно состояния применения конфигурации

Также во всплывающей подсказке отображается следующая информация о применении конфигурации:

- Для агентов — список агентов с их IP-адресами и информацией о применении конфигурации на каждом из агентов.
- Время последнего обновления конфигурации.
- Количество подов или агентов. Если в этот момент конфигурация применяется, отображается количество подов или агентов, на которых произошло обновление.

— Время начала текущего обновления при применении конфигурации.

— Сообщения об ошибках, произошедших при применении конфигурации.

7.7. Смена языка интерфейса

Интерфейс PT AF доступен на русском и английском языках. По умолчанию язык интерфейса соответствует языку браузера, в котором вы открываете PT AF.

- Чтобы сменить язык интерфейса,

  в главном меню нажмите и в раскрывшемся меню выберите язык интерфейса.

7.8. Смена темы интерфейса

Интерфейс PT AF доступен в двух темах: светлой и темной. По умолчанию интерфейс темный.

- Чтобы сменить тему интерфейса,

  в главном меню нажмите и в раскрывшемся меню выберите тему.

8. Настройка защиты веб-приложений

В разделе приведены инструкции по настройке защиты веб-приложений. В каждом изолированном пространстве вы можете настроить защиту не более 30 веб-приложений.

> **Примечание.** Если вы создали изолированное пространство в PT AF версии ниже 4.2.0, а затем обновили PT AF на версию 4.2.0 и выше, для изолированного пространства будет действовать ограничение в 10 веб-приложений. Вы можете увеличить максимальное количество веб-приложений (см. раздел 15.7) до 30 с помощью параметра `max_applications_count`.

В этом разделе

Режимы защиты веб-приложений (см. раздел 8.1)

Настройка защиты веб-приложения в изолированном пространстве с типом PT AF (см. раздел 8.2)

Настройка защиты веб-приложения в изолированном пространстве с типом Агент (см. раздел 8.3)

Алгоритм выбора веб-приложения для обработки и проксирования запроса (см. раздел 8.4)

8.1. Режимы защиты веб-приложений

При настройке защиты веб-приложения необходимо выбрать режим защиты, который определяет реакцию PT AF на срабатывание правил обработки трафика. Краткое описание и назначение режимов защиты приведены в таблице ниже.

Таблица 9. Режимы защиты веб-приложения

Режим защиты	Описание	Назначение
Без мер защиты	PT AF не обрабатывает трафик, не блокирует атаки и не записывает события безопасности. PT AF выступает в качестве обратного прокси для веб-приложения	Проверка работы приложения после подключения к нему PT AF. Ситуации, когда необходимо прекратить блокировку трафика и запись событий безопасности
Обнаружение и изменение содержимого	PT AF обрабатывает трафик, записывает события безопасности, но не применяет к запросам действия **Block**, **CAPTCHA**, **Close connection without response**.	Настройка политики безопасности приложения

Режим защиты	Описание	Назначение
	Правила, срабатывающие при использовании режима: — **Превышение ограничения для HTTP**; — **Предварительно декодировать параметры HTTP**. Правила, модифицирующие трафик при использовании режима: — **Разглашение важной информации в заголовке ответа**; — **Добавлять CSRF-токен**; — **Валидировать CSRF-токен**; — правила группы **Политики браузера**	
Все меры защиты	PT AF обрабатывает трафик, записывает события безопасности и применяет к запросами все действия, в том числе блокирующие	Основной режим защиты веб-приложения

8.2. Настройка защиты веб-приложения в изолированном пространстве с типом PT AF

В таблице ниже описана последовательность действий для настройки защиты веб-приложения в изолированном пространстве с типом **PT AF**. Выполнение того или иного этапа может зависеть от используемого варианта балансировки нагрузки.

Таблица 10. Настройка защиты в изолированном пространстве с типом PT AF

Этап	Название этапа	Обязательный	Балансировка нагрузки		
			Внутренняя	Внешняя без контроля IP-адресов	Внешняя с контролем IP-адресов
1	Добавление защищаемого сервера (см. раздел 8.2.1.1)	Да	✓	✓	✓
2	Создание IP-адреса для прослушивания (см. раздел 8.2.2.1)	Да	✓	–	✓
3	Создание исходящего IP-адреса (см. раздел 8.2.3.1)	Нет	–	–	✓
4	Добавление SSL-сертификата (см. раздел 8.2.4) и закрытого ключа (см. раздел 8.2.5)	Нет	✓	✓	✓
5	Создание профиля трафика (см. раздел 8.2.6)	Да	✓	✓	✓
6	Добавление списка отозванных сертификатов (см. раздел 8.2.7.1)	Нет	✓	✓	✓

Этап	Название этапа	Обязательный	Балансировка нагрузки		
			Внутренняя	Внешняя без контроля IP-адресов	Внешняя с контролем IP-адресов
7	Создание действия для управления HTTP-заголовками (см. раздел 8.2.8)	Нет	✓	✓	✓
8	Создание веб-приложения (см. раздел 8.2.9)	Да	✓	✓	✓

О балансировке нагрузки

В системе PT AF предусмотрены следующие варианты балансировки нагрузки:

- **Внутренний балансировщик.** Трафик распределяется между узлами кластера с помощью PT AF, который назначает узел для приема трафика и узлы для его обработки. Этот вариант балансировки потребляет дополнительные ресурсы PT AF для создания и работы сервисов и подов.
- **Внешний балансировщик без контроля IP-адресов.** Трафик распределяется между узлами как с помощью PT AF, так и с помощью внешнего балансировщика. PT AF отображает информацию о доступных IP-адресах и порте, на которых может прослушиваться трафик, а также предоставляет сведения о количестве подов, используемых на каждом узле для обработки трафика. Созданием таких подов управляет кластер Kubertenes, который может не создавать поды на всех узлах кластера. Данные о доступных IP-адресах, порте для прослушивания и обрабатывающих трафик подах необходимо использовать для настройки внешнего балансировщика и оптимального распределения трафика.
- **Внешний балансировщик с контролем IP-адресов.** Трафик распределяется между выбранными вами узлами с помощью внешнего балансировщика.

В этом разделе

Настройка защищаемых серверов (см. раздел 8.2.1)

Настройка IP-адресов для прослушивания (см. раздел 8.2.2)

Настройка исходящих IP-адресов (см. раздел 8.2.3)

Добавление SSL-сертификата (см. раздел 8.2.4)

Добавление закрытого ключа (см. раздел 8.2.5)

Настройка профилей трафика (см. раздел 8.2.6)

Управление списками отозванных сертификатов (см. раздел 8.2.7)

Создание действия для управления HTTP-заголовками (см. раздел 8.2.8)

Создание веб-приложения в изолированном пространстве с типом PT AF (см. раздел 8.2.9)

Настройка конфигураций SSL (см. раздел 8.2.10)

8.2.1. Настройка защищаемых серверов

Вы можете управлять защищаемыми серверами на странице **Схема конфигурации** → **Защищаемые серверы**.

В этом разделе

Добавление защищаемого сервера (см. раздел 8.2.1.1)

Добавление защищаемого сервера на основе существующего (см. раздел 8.2.1.2)

Удаление защищаемого сервера (см. раздел 8.2.1.3)

8.2.1.1. Добавление защищаемого сервера

- Чтобы добавить защищаемый сервер:

  1. В раскрывающемся блоке **Защищаемые серверы** нажмите +.
  2. Введите название защищаемого сервера.
  3. Введите IP-адрес или доменное имя сервера.
  4. Введите номер порта сервера для получения трафика от PT AF.
  5. Выберите протокол для обмена трафиком между PT AF и сервером.
  6. Нажмите **Добавить**.

8.2.1.2. Добавление защищаемого сервера на основе существующего

- Чтобы добавить защищаемый сервер на основе существующего:

  1. В раскрывающемся блоке **Защищаемые серверы** в строке сервера нажмите →.
  2. Нажмите **Действия** → **Копировать**.

Откроется окно добавления защищаемого сервера. Поля будут заполнены значениями параметров защищаемого сервера, на основе которого создается новый защищаемый сервер.

3. Измените название, IP-адрес или имя узла, порт и внесите другие необходимые изменения.

   Примечание. Сочетание IP-адреса или имени узла и порта защищаемого сервера должно быть уникальным в рамках изолированного пространства.

4. Нажмите **Добавить**.

8.2.1.3. Удаление защищаемого сервера

Вы можете удалить только защищаемые серверы, не назначенные на профили трафика.

► Чтобы удалить защищаемый сервер:

1. В раскрывающемся блоке **Защищаемые серверы** в строке сервера нажмите →.
2. Нажмите **Действия** → **Удалить** и подтвердите удаление.

8.2.2. Настройка IP-адресов для прослушивания

PT AF принимает запросы от клиентов веб-приложений через IP-адреса для прослушивания (прослушиваемые IP-адреса). Вы можете добавлять прослушиваемые IP-адреса двух типов: привязанные и не привязанные к узлу, обрабатывающему трафик (имеющему роль `worker-traffic`). В зависимости от варианта балансировки нагрузки (см. раздел 8.2), выбранного в профиле трафика (см. раздел 8.2.6), прослушиваемый IP-адрес указывается пользователем или автоматически назначается PT AF.

С внутренней балансировкой нагрузки используется прослушиваемый IP-адрес, не привязанный к узлу — обработчику трафика. Такой IP-адрес указывается пользователем в профиле трафика, а затем PT AF присваивает IP-адрес сетевому интерфейсу с ролью `WAN` на одном из узлов-обработчиков. Распределением подов для обработки трафика между узлами управляет Kubernetes, поэтому трафик, получаемый через непривязанный IP-адрес, может быть обработан не только на том узле, на котором он был получен. Например, в кластере из трех узлов трафик может обрабатываться как на всех узлах, так и только на двух или только на одном. При потере работоспособности узла с непривязанным IP-адресом система автоматически назначит этот IP-адрес сетевому интерфейсу другого узла.

С внешним балансировщиком без контроля IP-адресов прослушиваемые IP-адреса определяет PT AF: ими являются IP-адреса сетевых интерфейсов с ролью `WAN` на каждом узле-обработчике. Поскольку созданием подов для обработки трафика управляет Kubernetes, трафик может обрабатываться не всеми узлами кластера.

С внешним балансировщиком и контролем IP-адресов используются прослушиваемые IP-адреса, привязанные к узлу. При создании такого IP-адреса нужно указать узел, который будет обрабатывать трафик, поступающий на этот IP-адрес. PT AF присвоит привязанный IP-адрес сетевому интерфейсу с ролью `WAN` на этом узле. На нем же будет обрабатываться трафик. Вы можете привязать несколько IP-адресов к одному узлу.

В качестве прослушиваемого IP-адреса рекомендуется указывать виртуальный IP-адрес. Вам необходимо обеспечить доступность указанного виртуального адреса для всех интерфейсов с ролью `WAN` на узлах, обрабатывающих трафик. Кроме того, прослушиваемый IP-адрес может совпадать с IP-адресом физического интерфейса при развертывании PT AF на одном узле.

Также при создании прослушиваемого IP-адреса вы можете настроить маршрутизацию трафика от этого адреса. Одному прослушиваемому IP-адресу могут соответствовать несколько маршрутов с разными адресами сети назначения. Все настроенные маршруты создаются для сетевого интерфейса с ролью `WAN`. Если нужно, вы можете выбрать другой интерфейс, переназначив роль `WAN`.

> **Примечание.** В веб-интерфейсе PT AF вы можете настроить маршрутизацию прослушиваемых IP-адресов. Для настройки других сетевых маршрутов необходимо использовать команды секции `route` в WSC (см. приложение А.9).

Вы можете управлять прослушиваемыми IP-адресами на странице **Схема конфигурации** → **IP-адреса для прослушивания**.

В этом разделе

Создание прослушиваемого IP-адреса (см. раздел 8.2.2.1)

Создание прослушиваемого IP-адреса на основе существующего (см. раздел 8.2.2.2)

Удаление прослушиваемого IP-адреса (см. раздел 8.2.2.3)

8.2.2.1. Создание прослушиваемого IP-адреса

- Чтобы создать прослушиваемый IP-адрес:

1. В раскрывающемся блоке **IP-адреса для прослушивания** нажмите +.
2. Введите имя IP-адреса для прослушивания.

   Примечание. Введенное имя будет отображаться при выборе IP-адреса для прослушивания клиентских запросов при создании или изменении профиля трафика (см. раздел 8.2.3.1). Вы можете не вводить имя IP-адреса для прослушивания, в таком случае поле автоматически заполнится значением, указанным в поле **IP-адрес для прослушивания клиентских запросов**.
3. Выберите тип IP-адреса.
4. Укажите прослушиваемый IP-адрес.

   Примечание. Поддерживается только IPv4-адрес без маски и префикса.

5. Если IP-адрес привязан к узлу, выберите узел PT AF, который будет обрабатывать трафик, поступающий на этот IP-адрес.
6. В блоке параметров **Маршруты** нажмите **Добавить** и введите адреса для маршрутизации ответов на запросы, передаваемых через прослушиваемый IP-адрес:
   - Введите адрес сети или узла назначения.

     Примечание. Поддерживаются только IPv4-адрес или IPv4-подсеть в формате CIDR. Для указания маршрута по умолчанию нужно ввести `0.0.0.0/0` или `default`.
   - Введите адрес шлюза.

     Примечание. Поддерживается только IPv4-адрес без маски и префикса.
7. Нажмите **Сохранить**.

8.2.2.2. Создание прослушиваемого IP-адреса на основе существующего

- Чтобы создать прослушиваемый IP-адрес на основе существующего:

  1. В раскрывающемся блоке **IP-адреса для прослушивания** в строке IP-адреса нажмите →.
  2. Нажмите **Действия** → **Копировать**.

     Откроется окно создания IP-адреса для прослушивания. Поля будут заполнены значениями параметров прослушиваемого IP-адреса, на основе которого создается новый IP-адрес.
  3. Измените IP-адрес для прослушивания клиентских запросов, его имя и внесите другие необходимые изменения.

     Примечание. IP-адрес для прослушивания и его имя должны быть уникальными в рамках одного изолированного пространства. Вы можете не вводить имя IP-адреса для прослушивания, в таком случае поле автоматически заполнится значением, указанным в поле **IP-адрес для прослушивания клиентских запросов**.
  4. Нажмите **Сохранить**.

8.2.2.3. Удаление прослушиваемого IP-адреса

Вы можете удалить только не привязанные к профилям трафика IP-адреса для прослушивания.

- Чтобы удалить прослушиваемый IP-адрес:

  1. В раскрывающемся блоке **IP-адреса для прослушивания** в строке IP-адреса нажмите →.
  2. Нажмите **Действия** → **Удалить** и подтвердите удаление.

8.2.3. Настройка исходящих IP-адресов

Трафик передается на защищаемые серверы с тех узлов кластера, на которых он был обработан. По умолчанию для передачи трафика используются реальные IP-адреса сетевых интерфейсов с ролью LAN, количество которых ограничено. Если нужно поддерживать большое число активных соединений, вы можете создать несколько виртуальных исходящих IP-адресов для каждого узла и использовать их вместо реальных IP-адресов в профиле трафика.

Вы можете управлять исходящими IP-адресами на странице **Схема конфигурации** → **IP-адреса для исходящих запросов**.

В этом разделе

Создание исходящего IP-адреса (см. раздел 8.2.3.1)

Создание исходящего IP-адреса на основе существующего (см. раздел 8.2.3.2)

Удаление исходящего IP-адреса (см. раздел 8.2.3.3)

8.2.3.1. Создание исходящего IP-адреса

- Чтобы создать исходящий IP-адрес:

  1. В раскрывающемся блоке **IP-адреса для исходящих запросов** нажмите +.
  2. В поле **IP-адрес для исходящих запросов** введите IP-адрес.
  3. В раскрывающемся блоке **Узел обработки трафика** выберите узел PT AF, с которого будет отправляться трафик.
  4. Нажмите **Добавить**.

8.2.3.2. Создание исходящего IP-адреса на основе существующего

- Чтобы создать исходящий IP-адрес на основе существующего:

  1. В раскрывающемся блоке **IP-адреса для исходящих запросов** в строке IP-адреса нажмите →.
  2. Нажмите **Действия** → **Копировать**.

     Откроется окно создания исходящего IP-адреса. Поля будут заполнены значениями параметров исходящего IP-адреса, на основе которого создается новый IP-адрес.
  3. Измените IP-адрес для исходящих запросов.

Примечание. IP-адрес для исходящих запросов не должен совпадать с другими IP-адресами для исходящих запросов и с IP-адресами для прослушивания в рамках изолированного пространства.

4. Нажмите **Добавить**.

8.2.3.3. Удаление исходящего IP-адреса

Вы можете удалять не привязанные к профилям трафика исходящие IP-адреса.

- Чтобы удалить исходящий IP-адрес:

1. В раскрывающемся блоке **IP-адреса для исходящих запросов** в строке IP-адреса нажмите →.
2. Нажмите **Действия** → **Удалить** и подтвердите удаление.

8.2.4. Добавление SSL-сертификата

PT AF не сможет обработать трафик, если он зашифрован. Для расшифровки HTTPS-трафика нужно добавить сертификат (цепочку сертификатов) и его закрытый ключ. Кроме того, если нужно проверять подлинность сертификата защищаемого веб-приложения, вы можете добавить сертификат удостоверяющего центра, который будет использоваться для проверки.

Внимание! Не поддерживается добавление сертификатов удостоверяющего центра при обработке трафика на сервере Envoy (см. раздел 15.6.5).

Поддерживаемый формат файлов сертификатов и ключей — PEM, поддерживаемые алгоритмы шифрования — RSA, ECC (ECDSA) и ГОСТ.

- Чтобы добавить сертификат:

1. На странице **Схема конфигурации** в раскрывающемся блоке **Сертификаты SSL** нажмите +.
2. Выберите тип сертификата.
3. Введите имя сертификата.
4. Нажмите **Загрузить**.
5. В открывшемся окне выберите файл сертификата и нажмите **Открыть**.
6. Если добавляете сертификат сервера, в раскрывающемся списке **Закрытый ключ** выберите его закрытый ключ.

   Примечание. Если в списке нет нужного ключа, вы можете добавить его (см. раздел 8.2.5) по кнопке **Добавить закрытый ключ**.
7. Нажмите **Добавить**.

8.2.5. Добавление закрытого ключа

- Чтобы добавить закрытый ключ:

  1. На странице **Схема конфигурации** в раскрывающемся блоке **Закрытые ключи SSL** нажмите +.
  2. Введите имя ключа.
  3. Нажмите кнопку **Прочесть из файла**.
  4. В открывшемся окне выберите файл открытого ключа и нажмите кнопку **Открыть**.
  5. Если ключ зашифрован паролем, в поле **Парольная фраза** введите пароль.
  6. Нажмите **Добавить**.

8.2.6. Настройка профилей трафика

Профиль трафика обеспечивает соединение клиента с защищаемым веб-приложением.

Вы можете управлять профилями трафика на странице **Схема конфигурации** → **Профили трафика**.

В этом разделе

Создание профиля трафика с внутренней балансировкой нагрузки (см. раздел 8.2.6.1)

Создание профиля трафика с внешней балансировкой нагрузки без контроля IP-адресов (см. раздел 8.2.6.2)

Создание профиля трафика с внешней балансировкой нагрузки и контролем IP-адресов (см. раздел 8.2.6.3)

Создание профиля трафика на основе существующего (см. раздел 8.2.6.4)

Удаление профиля трафика (см. раздел 8.2.6.5)

8.2.6.1. Создание профиля трафика с внутренней балансировкой нагрузки

- Чтобы создать профиль трафика:

  1. В раскрывающемся списке **Профили трафика** нажмите +.
  2. Введите название профиля трафика.
  3. В блоке параметров **Балансировщик нагрузки** выберите вариант **Внутренний**.
  4. В раскрывающемся списке **IP-адрес для прослушивания клиентских запросов** выберите прослушиваемый IP-адрес.

Примечание. Для выбора доступны IP-адреса, не привязанные к узлу. Если в списке нет нужного IP-адреса, вы можете добавить его (см. раздел 8.2.2.1) по кнопке **Добавить**.

5. В поле **Порт для прослушивания клиентских запросов** введите номер порта для приема трафика от клиентов защищаемого веб-приложения.
6. В блоке параметров **Протокол для клиентских запросов** выберите протокол для приема трафика от клиентов защищаемого веб-приложения.
7. Если нужно перенаправлять HTTP-запросы на HTTPS-порт, включите перенаправление и укажите HTTP-порт, с которого будут переадресовываться HTTP-запросы.
8. В блоке параметров **Группа защищаемых серверов** в раскрывающемся списке **Защищаемый сервер** выберите сервер защищаемого веб-приложения.

   Примечание. Если в списке нет нужного защищаемого сервера, вы можете добавить его (см. раздел 8.2.1.1) по кнопке **Добавить**.
9. Если трафик веб-приложения обрабатывается несколькими серверами, добавьте их по кнопке **Добавить сервер**.

   Примечание. Также в блоке параметров **Группа защищаемых серверов** вы можете настроить балансировку нагрузки между серверами: выбрать способ балансировки, указать вес для каждого сервера и максимальное количество неудачных попыток соединения. NTLM-аутентификация распознается и поддерживается автоматически, без дополнительных действий со стороны пользователя.
10. Нажмите **Создать**.

Сервисы и поды, необходимые для работы профиля трафика с внутренней балансировкой, будут созданы и запущены только после его использования в профиле для защиты веб-приложения.

8.2.6.2. Создание профиля трафика с внешней балансировкой нагрузки без контроля IP-адресов

- Чтобы создать профиль трафика:

1. В раскрывающемся списке **Профили трафика** нажмите +.
2. Введите название профиля трафика.
3. В блоке параметров **Балансировщик нагрузки** выберите вариант **Внешний без контроля IP-адресов**.

   В блоке параметров **Доступные IP-адреса** отобразятся прослушиваемые IP-адреса. Они совпадают с IP-адресами сетевых интерфейсов с ролью WAN каждого узла кластера.
4. В блоке параметров **Протокол для клиентских запросов** выберите протокол для приема трафика от клиентов защищаемого веб-приложения.

5. В блоке параметров **Группа защищаемых серверов** в раскрывающемся списке **Защищаемый сервер** выберите сервер защищаемого веб-приложения.

   Примечание. Если в списке нет нужного защищаемого сервера, вы можете добавить его (см. раздел 8.2.1.1) по кнопке **Добавить**.

6. Если трафик веб-приложения обрабатывается несколькими серверами, добавьте их по кнопке **Добавить сервер**.

   Примечание. Также в блоке параметров **Группа защищаемых серверов** вы можете настроить балансировку нагрузки между серверами: выбрать способ балансировки, указать вес для каждого сервера и максимальное количество неудачных попыток соединения. NTLM-аутентификация распознается и поддерживается автоматически, без дополнительных действий со стороны пользователя.

7. Нажмите **Создать**.

Порты для приема запросов от клиентов и для проверки наличия подов (health-порты) будут автоматически назначены после создания профиля. Вы можете узнать количество подов, используемых на каждом узле для обработки трафика, с помощью GET-запроса `http://<Прослушиваемый (доступный) IP-адрес>:<Health-порт>/healthz` и затем использовать эти данные для настройки внешнего балансировщика. Если узел содержит поды для обработки трафика, в ответе возвращается код 200 и количество подов в параметре `localEndpoints`. Если не содержит — код 503 и ноль в параметре `localEndpoints`.

8.2.6.3. Создание профиля трафика с внешней балансировкой нагрузки и контролем IP-адресов

Внимание! Этот вариант балансировки не поддерживает NTLM-аутентификацию и HTTP-заголовки, имена которых содержат символы в кодировке, отличной от ASCII. Соединения с такими заголовками автоматически разрываются на уровне протокола.

- Чтобы создать профиль трафика:

  1. В раскрывающемся списке **Профили трафика** нажмите +.
  2. Введите название профиля трафика.
  3. В блоке параметров **Балансировщик нагрузки** выберите вариант **Внешний с контролем IP-адресов**.
  4. В раскрывающемся списке **IP-адрес для прослушивания клиентских запросов** выберите прослушиваемые IP-адреса.

     Примечание. Для выбора доступны IP-адреса, привязанные к узлу. Если в списке нет нужного IP-адреса, вы можете добавить его (см. раздел 8.2.2.1) по кнопке **Добавить**.

  5. В поле **Порт для прослушивания клиентских запросов** введите номер порта для приема трафика от клиентов защищаемого веб-приложения.

6. В блоке параметров **Протокол для клиентских запросов** выберите протокол для приема трафика от клиентов защищаемого веб-приложения.
7. Если нужно передавать трафик на защищаемые серверы с нескольких IP-адресов, в раскрывающемся списке **IP-адреса для исходящих запросов** выберите эти IP-адреса.

   Примечание. Если в списке нет нужного IP-адреса, вы можете добавить его (см. раздел 8.2.3.1) по кнопке **Добавить**. Прослушиваемый и исходящий IP-адреса должны быть связаны с одним и тем же узлом.
8. Если нужно перенаправлять HTTP-запросы на HTTPS-порт, включите перенаправление и укажите HTTP-порт, с которого будут переадресовываться HTTP-запросы.
9. В блоке параметров **Группа защищаемых серверов** в раскрывающемся списке **Защищаемый сервер** выберите сервер защищаемого веб-приложения.

   Примечание. Если в списке нет нужного защищаемого сервера, вы можете добавить его (см. раздел 8.2.1.1) по кнопке **Добавить**.
10. Если трафик веб-приложения обрабатывается несколькими серверами, добавьте их по кнопке **Добавить сервер**.

    Примечание. Также в блоке параметров **Группа защищаемых серверов** вы можете настроить балансировку нагрузки между серверами: выбрать способ балансировки, указать вес для каждого сервера и максимальное количество неудачных попыток соединения.
11. Нажмите **Создать**.

8.2.6.4. Создание профиля трафика на основе существующего

► Чтобы создать профиль трафика на основе существующего:

1. В раскрывающемся блоке **Профили трафика** в строке профиля трафика нажмите →.
2. Нажмите **Действия** → **Копировать**.

   Откроется окно создания профиля трафика. Поля будут заполнены значениями параметров профиля трафика, на основе которого создается новый профиль.
3. Измените название профиля трафика и внесите другие необходимые изменения.

   Примечание. Название профиля трафика должно быть уникальным для изолированного пространства.
4. Нажмите **Создать**.

8.2.6.5. Удаление профиля трафика

Вы можете удалить только те профили трафика, которые не используются в веб-приложениях.

- Чтобы удалить профиль трафика:

  1. В раскрывающемся блоке **Профили трафика** в строке профиля трафика нажмите →.
  2. Нажмите **Действия** → **Удалить** и подтвердите удаление.

8.2.7. Управление списками отозванных сертификатов

В изолированных пространствах с типом обработки трафика **PT AF** и с сервером обработки трафика nginx вы можете настроить аутентификацию клиентов по сертификатам, а также проверять их действительность с помощью списков отозванных сертификатов.

> **Внимание!** На сервере Envoy (см. раздел 15.6.5) аутентификация клиентов по клиентским сертификатам не поддерживается.

Вы можете управлять списками отозванных сертификатов на странице **Схема конфигурации** → **Списки отозванных сертификатов**.

В этом разделе

Добавление списка отозванных сертификатов (см. раздел 8.2.7.1)

Синхронизация списка отозванных сертификатов (см. раздел 8.2.7.2)

8.2.7.1. Добавление списка отозванных сертификатов

- Чтобы добавить список отозванных сертификатов:

  1. В раскрывающемся блоке **Списки отозванных сертификатов** нажмите +.
  2. Введите имя списка.
  3. Выберите источник списка.

     Примечание. PT AF поддерживает файлы со списками в формате PEM размером не более 5 МБ независимо от выбранного источника.
  4. Если вы выбрали URL в качестве источника, введите URL, на котором размещен список.
  5. Если вы выбрали локальный источник:

     - Нажмите **Загрузить**.

- В открывшемся окне выберите файл со списком и нажмите **Открыть**.

6. Нажмите **Добавить**.

Теперь вы можете выбрать список отозванных сертификатов при настройке веб-приложения. Сертификаты клиентов защищаемого приложения будут проверяться по этому списку.

8.2.7.2. Синхронизация списка отозванных сертификатов

Если в качестве источника списка отозванных сертификатов используется URL, вы можете синхронизировать список для получения актуальных отозванных сертификатов.

► Чтобы синхронизировать список отозванных сертификатов:

1. В раскрывающемся блоке **Списки отозванных сертификатов** в строке списка с источником URL нажмите →.
2. Нажмите **Синхронизировать**.

   Дата и время синхронизации списка изменятся на текущие.

8.2.8. Создание действия для управления HTTP-заголовками

Для изолированных пространств с типом обработки трафика **PT AF** и с сервером обработки трафика nginx доступно управление HTTP-заголовками в запросах к веб-приложениям. Управление заголовками выполняется с помощью специальных действий, которые определяют, какой заголовок и каким образом нужно изменить.

> **Внимание!** Также вы можете изменять заголовки с помощью действия (см. раздел 11.4) с типом **Изменять заголовок запроса** в правилах обработки трафика. Не рекомендуется использовать одновременно для одного веб-приложения два действия над одним и тем же заголовком: действие с типом **Изменять заголовок запроса** в правилах и действие для управления HTTP-заголовками в веб-приложении. Поскольку эти действия имеют разное назначение и выполняются на разных этапах обработки трафика, конфликт между ними может привести к непредсказуемому изменению значений заголовков в итоговом запросе.

Вы можете создавать действия для управления HTTP-заголовками на странице **Схема конфигурации** → **Управление заголовками**.

► Чтобы создать действие для управления HTTP-заголовками:

1. В раскрывающемся блоке **Управление заголовками** нажмите +.

   Откроется карточка для создания действия.
2. Введите название действия.
3. Выберите тип действия.

Примечание. Действие с типом **Задать значение заголовка** не дублирует заголовок, а перезаписывает его значение на указанное в параметрах действия.

4. Укажите изменяемый HTTP-заголовок и значения других параметров (см. таблицу 11) в зависимости от выбранного типа действия.

   Внимание! Если в качестве HTTP-заголовка вы укажете переменную, связанную с информацией о сертификате клиента, необходимо также при настройке веб-приложения, которое будет использовать создаваемое действие с заголовком, включить проверку сертификата клиента. Если не включить проверку, информация, связанная с сертификатом, не будет передаваться в HTTP-заголовках.

5. Выберите область действия.

   Примечание. Область действия определяет набор IP-адресов, при получении запросов от которых будет выполняться создаваемое действие. Доверенные подсети вы можете указать в параметре **Доверенные подсети и IP-адреса в нотации CIDR** при настройке веб-приложения.

6. Нажмите **Добавить**.

Теперь вы можете выбрать созданное действие при настройке веб-приложения.

Таблица 11. Описание переменных для действий с заголовками

Переменная	Описание
`%CLIENT_IP`	Достоверный IP-адрес клиента, который принимается в качестве источника запроса к PT AF, например, при использовании балансировщика нагрузки. Если доверенный IP-адрес не был получен из заголовка запроса или прокси-протокола, вместо доверенного IP-адреса будет подставлен удаленный IP-адрес (`%REMOTE_IP`)
`%REMOTE_IP`	Удаленный IP-адрес клиента, с которого непосредственно был отправлен запрос к PT AF
`%SSL_CLIENT_VERIFY`	Результат проверки сертификата клиента
`%SSL_CLIENT_ESCAPED_CERT`	Сертификат клиента в формате `PEM`
`%SSL_CLIENT_S_DN`	Строка `subject DN` сертификата клиента согласно RFC 2253
`%SSL_CLIENT_I_DN`	Строка `issuer DN` сертификата клиента согласно RFC 2253
`%SSL_CLIENT_SERIAL`	Серийный номер сертификата клиента
`%SSL_CLIENT_FINGERPRINT`	SHA-1 отпечаток сертификата клиента
`%SSL_CLIENT_V_START`	Дата начала срока действия сертификата клиента
`%SSL_CLIENT_V_END`	Дата окончания действия сертификата клиента

Переменная	Описание
%SSL_CLIENT_V_REMAIN	Количество дней до истечения срока действия сертификата клиента

8.2.9. Создание веб-приложения в изолированном пространстве с типом PT AF

Последовательность создания веб-приложения зависит от того, настроена ли синхронизация (см. раздел 15.19) между экземплярами PT AF.

Вы можете создавать веб-приложения на странице **Схема конфигурации** → **Веб приложения**.

В этом разделе

Создание нового веб-приложения (см. раздел 8.2.9.1)

Создание веб-приложения на основе существующего (см. раздел 8.2.9.2)

8.2.9.1. Создание нового веб-приложения

- Чтобы создать веб-приложение:

1. В раскрывающемся блоке **Веб-приложения** нажмите +.
2. Введите название веб-приложения.
3. В раскрывающемся списке **Шаблон политики безопасности** выберите шаблон политики безопасности.

   Если в списке нет нужного шаблона, вы можете добавить его (см. раздел 9.2) по кнопке **Добавить**.
4. В раскрывающемся списке **Профили трафика** выберите профиль для приема и передачи трафика на серверы защищаемого веб-приложения.

   Если в списке нет нужного профиля, вы можете добавить его (см. раздел 8.2.6) по кнопке **Добавить**.

   Примечание. Вы можете выбрать несколько профилей трафика. Эти профили должны использовать прослушиваемые IP-адреса одного типа: или только не привязанные к узлу, или только привязанные. Одновременный выбор нескольких профилей с разными типами IP-адресов не поддерживается.
5. Если трафик веб-приложения зашифрован, укажите параметры для расшифровки трафика:

- В раскрывающемся списке **Цепочка сертификатов SSL** выберите сертификаты для расшифровки трафика. Если в списке нет нужного сертификата, вы можете добавить его (см. раздел 8.2.4) по кнопке **Добавить**.

  Примечание. Вы можете выбрать не более двух сертификатов. Они должны поддерживать разные алгоритмы шифрования.

- В раскрывающемся списке **Конфигурация SSL** выберите конфигурацию для протоколов TLS с набором шифров. Вы можете добавить собственную конфигурацию (см. раздел 8.2.10) по кнопке **Добавить**.

- Если нужно проверять подлинность сертификата приложения, включите проверку и в раскрывающемся списке выберите сертификат удостоверяющего центра, который будет использоваться для проверки.

  Внимание! Не поддерживаются добавление и выбор сертификатов удостоверяющего центра при обработке трафика на сервере Envoy (см. раздел 15.6.5).

6. Если нужно настроить аутентификацию клиентов в веб-приложении по клиентским сертификатам, включите проверку подлинности сертификатов клиентов и настройте следующие параметры:

   - Выберите сертификат удостоверяющего центра для проверки сертификатов клиентов.
   - Укажите глубину проверки сертификата клиента в цепочке сертификатов.
   - Если нужно проверять сертификаты клиентов по спискам отозванных сертификатов, включите проверку и выберите список отозванных сертификатов. Вы можете добавить новый список по кнопке **Добавить**.

     Внимание! На сервере Envoy (см. раздел 15.6.5) аутентификация клиентов по клиентским сертификатам не поддерживается.

     Примечание. При попытке аутентификации пользователя по невалидному клиентскому сертификату или при отсутствии сертификата в ответе вернется ошибка с кодом 403 и заголовок `X-Block-Type: id003`. Вы можете настроить запись неуспешных попыток аутентификации по клиентским сертификатам в журнал access.log (см. раздел 15.7.4). В журнале error.log такие записи будут отображаться, если на сервере установлен уровень логирования `debug`.

7. Если защищаемое приложение использует протокол WebSocket, включите его поддержку.
8. Выберите режим защиты (см. раздел 8.1).
9. В блоке параметров **Узлы** нажмите кнопку **Добавить** и в появившемся поле введите IP-адрес или доменное имя защищаемого приложения.

   Вы можете использовать символ звездочки (*) для подстановки любого количества символов в начале или в конце имени (например, `*.example.com` или `example.*`).

10. Если вы хотите защитить только некоторые части веб-приложения, в поле **Расположение** введите пути к ним.

Вы можете добавить несколько путей по кнопке **Добавить**. Можно использовать символы ^ (начало пути), $ (конец пути) и * (любое количество произвольных символов).

Внимание! Использование любого из символов ^ (начало пути), $ (конец пути) и * (любое количество произвольных символов) в поле **Расположение** приводит к поиску совпадений по указанной подстроке. Если перечисленные символы не используются, поиск выполняется по указанному префиксу (по началу строки).

11. Если перед PT AF находится внешний балансировщик или прокси-сервер, выберите вариант получения IP-адреса клиента.

    Внимание! Не поддерживается одновременное получение IP-адресов клиентов из протоколов PROXY и HTTP.

12. Если вы выбрали вариант получения IP-адреса из протокола PROXY, в блоке параметров **Доверенные подсети и IP-адреса в нотации CIDR** нажмите кнопку **Добавить** и в появившемся поле введите доверенный IP-адрес балансировщика нагрузки в нотации CIDR.

    Примечание. Если используется цепочка серверов, нужно указывать IP-адрес последнего балансировщика нагрузки. Кроме того, все серверы в цепочке должны использовать один и тот же способ получения IP-адреса — из протокола PROXY.

13. Если вы выбрали вариант получения IP-адреса из HTTP-заголовка:

    - В блоке параметров **Доверенные подсети и IP-адреса в нотации CIDR** нажмите кнопку **Добавить** и в появившемся поле введите доверенный IP-адрес прокси-сервера в нотации CIDR.

      Примечание. Если используется цепочка серверов, нужно указывать IP-адрес последнего прокси-сервера (сервера внешнего балансировщика). Кроме того, все серверы в цепочке должны использовать один и тот же способ получения IP-адреса — из HTTP-заголовка.

    - В поле **Имя HTTP-заголовка** введите имя HTTP-заголовка, содержащего IP-адрес клиента защищаемого приложения (например, `X-Forwarded-For`).

14. Если нужно изменять заголовки HTTP-запросов для веб-приложения, выберите действия с заголовками. Вы можете добавить новое действие с заголовками (см. раздел 8.2.8) по кнопке **Добавить**.

    Примечание. Вы можете добавить веб-приложению несколько действий, связанных с разными HTTP-заголовками.

15. Нажмите **Создать**.

8.2.9.2. Создание веб-приложения на основе существующего

- Чтобы создать веб-приложение на основе существующего:

  1. В раскрывающемся блоке **Веб-приложения** в строке веб-приложения нажмите →.
  2. Нажмите **Действия** → **Копировать**.

     Откроется окно создания веб-приложения. Поля будут заполнены значениями параметров веб-приложения, на основе которого создается новое веб-приложение.
  3. Измените название веб-приложения, а также его узел, расположение или профиль трафика и внесите другие необходимые изменения.

     Примечание. Название веб-приложения, а также сочетание узла, расположения, IP-адреса и порта для прослушивания клиентских запросов для веб-приложения должно быть уникальным в рамках изолированного пространства.
  4. Нажмите **Создать**.

8.2.10. Настройка конфигураций SSL

В PT AF предусмотрены несколько стандартных конфигураций SSL с наборами шифров. Параметры этих конфигураций недоступны для изменения.

При обработке трафика на nginx доступны следующие стандартные конфигурации:

- **TLS 1.2 GOST** — конфигурация для протокола TLS версии 1.2 с поддержкой алгоритмов ГОСТ. По умолчанию для конфигурации включена функция **Отдавать предпочтение серверным шифрам**. Алгоритм ГОСТ Р 34.10-2001 не поддерживается. Используемый набор шифров:
  `GOST2012-KUZNYECHIK-KUZNYECHIKOMAC:GOST2012-MAGMA-MAGMAOMAC:LEGACY-GOST2012-GOST8912-GOST8912:IANA-GOST2012-GOST8912-GOST8912:GOST2001-GOST89-GOST89`
- **TLS 1.2 or earlier** — конфигурация для протоколов TLS версий 1.0, 1.1 и 1.2. По умолчанию для конфигурации включена функция **Отдавать предпочтение серверным шифрам**. Используемый набор шифров:
  `ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS`
- **TLS 1.2 RSA + GOST** — конфигурация для протокола TLS версии 1.2 с поддержкой алгоритмов RSA и ГОСТ. По умолчанию для конфигурации включена функция **Отдавать предпочтение серверным шифрам**. Алгоритм ГОСТ Р 34.10-2001 не поддерживается. Используемый набор шифров:

```
GOST2012-KUZNYECHIK-KUZNYECHIKOMAC:GOST2012-MAGMA-MAGMAOMAC:LEGACY-GOST2012-
GOST8912-GOST8912:IANA-GOST2012-GOST8912-GOST8912:GOST2001-GOST89-
GOST89:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-
AES128-GCM-SHA256:!aNULL:!MD5:!DSS
```

— **TLS 1.3 + 1.2 strong** — конфигурация для протоколов TLS версий 1.2 и 1.3 с набором шифров для TLS 1.2:

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-
POLY1305:ECDHE-RSA-AES128-GCM-SHA256:!aNULL:!MD5:!DSS
```

При обработке трафика на Envoy доступна одна стандартная конфигурация **TLS 1.3 + 1.2 strong** для протоколов TLS версий 1.2 и 1.3 с набором шифров для TLS 1.2:

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-
GCM-SHA256:!aNULL:!MD5:!DSS
```

Вы можете добавить собственную конфигурацию SSL при создании или изменении веб-приложения в изолированном пространстве на странице **Схема конфигурации** → **Веб-приложения**.

Добавление конфигурации SSL

► Чтобы добавить конфигурацию SSL:

1. В раскрывающемся списке **Веб-приложения** нажмите + или →.
2. Выберите цепочку сертификатов SSL.
3. В списке **Конфигурация SSL** нажмите **Добавить**.
4. Введите название конфигурации.
5. Выберите протокол.
6. Если вы выбрали протокол TLS версии 1.0, 1.1 или 1.2:
   - Укажите набор шифров для обеспечения безопасного сетевого соединения в порядке приоритета.
   - Если требуется, отключите использование серверного порядка наборов шифров вместо клиентского.

     Примечание. Для протокола TLS 1.3 недоступен выбор шифров, поскольку по умолчанию на сервере уже установлен актуальный набор.

Изменение конфигурации SSL

► Чтобы изменить конфигурацию SSL:

1. В раскрывающемся блоке **Веб-приложения** в строке веб-приложения нажмите →.
2. В списке **Конфигурация SSL** в строке с названием конфигурации нажмите →.

3. Внесите изменения.
4. Нажмите **Сохранить**.

Удаление конфигурации SSL

- Чтобы удалить конфигурацию SSL:

  1. В раскрывающемся блоке **Веб-приложения** в строке веб-приложения нажмите →.
  2. В списке **Конфигурация SSL** в строке с названием конфигурации нажмите →.
  3. Нажмите **Удалить** и подтвердите удаление.

Наборы шифров

Наборы шифров указываются в соответствии со стандартами OpenSSL (при обработке трафика на nginx) или BoringSSL (при обработке трафика на Envoy) в виде строк, разделенных двоеточием, пробелом или запятой. В конце списка шифров допускается использование точки с запятой.

Строка шифров может быть указана в виде набора шифров (например, `ECDHE-RSA-AES256-GCM-SHA384`) или группы наборов шифров, соответствующих протоколу или типу (например, `RSA` или `SSLv3`). Строки шифров могут объединяться с помощью символа `+` (например, `DH+AES`), группы — с помощью логического оператора `И`.

Подробнее о работе с наборами шифров в nginx см. на сайте docs.nginx.com, в Envoy — на сайте envoyproxy.io/docs.

8.3. Настройка защиты веб-приложения в изолированном пространстве с типом Агент

Часть действий, необходимых для настройки защиты веб-приложения в изолированном пространстве с типом **Агент**, выполняются непосредственно при установке и первоначальной настройке агента. Для завершения настройки необходимо создать веб-приложение в PT AF.

> **Внимание!** В изолированном пространстве с типом **Агент** конфигурация веб-приложений, настроенная в веб-интерфейсе, не синхронизируется автоматически с конфигурацией веб-приложений, настроенной в nginx. Нужно «вручную» следить за тем, чтобы эти конфигурации совпадали.

Вы можете создавать веб-приложения на странице **Схема конфигурации** → **Веб-приложения**.

Создание нового веб-приложения

- Чтобы создать веб-приложение:

  1. В раскрывающемся блоке **Веб-приложения** нажмите +.
  2. Введите название веб-приложения.
  3. В раскрывающемся списке **Шаблон политики безопасности** выберите шаблон политики безопасности.

     Если в списке нет нужного шаблона, вы можете добавить его (см. раздел 9.2) по кнопке **Добавить**.
  4. Выберите режим защиты (см. раздел 8.1).
  5. В блоке параметров **Узлы** нажмите кнопку **Добавить** и в появившемся поле введите IP-адрес или доменное имя защищаемого приложения.

     Вы можете использовать символ звездочки (*) для подстановки любого количества символов в начале или в конце имени (например, `*.example.com` или `example.*`).
  6. Если вы хотите защитить только некоторые части веб-приложения, в поле **Расположение** введите пути к ним.

     Вы можете добавить несколько путей по кнопке **Добавить**. Можно использовать символы ^ (начало пути), $ (конец пути) и * (любое количество произвольных символов).

     Внимание! Использование любого из символов ^ (начало пути), $ (конец пути) и * (любое количество произвольных символов) в поле **Расположение** приводит к поиску совпадений по указанной подстроке. Если перечисленные символы не используются, поиск выполняется по указанному префиксу (по началу строки).
  7. Нажмите **Создать**.

Создание веб-приложения на основе существующего

- Чтобы создать веб-приложение на основе существующего:

  1. В раскрывающемся блоке **Веб-приложения** в строке веб-приложения нажмите →.
  2. Нажмите **Действия** → **Копировать**.

     Откроется окно создания веб-приложения. Поля будут заполнены значениями параметров веб-приложения, на основе которого создается новое веб-приложение.
  3. Измените название веб-приложения, а также его узел, расположение и внесите другие необходимые изменения.

     Примечание. Название веб-приложения, а также сочетание узла и расположения должно быть уникальным в рамках изолированного пространства.
  4. Нажмите **Создать**.

См. также

Алгоритм выбора веб-приложения для обработки и проксирования запроса (см. раздел 8.4)

8.4. Алгоритм выбора веб-приложения для обработки и проксирования запроса

После получения запроса PT AF сопоставляет параметры запроса (заголовок `Host` и URI) с параметрами веб-приложений в два этапа.

> **Примечание.** В изолированном пространстве с типом **PT AF** сопоставляются параметры только тех веб-приложений, профиль трафика которых содержит прослушиваемые IP-адрес и порт, через которые поступил запрос. В изолированном пространстве с типом **Агент** сопоставляются параметры всех веб-приложений.

Первый этап. PT AF сравнивает заголовок `Host` (содержащий доменное имя или IP-адрес сервера защищаемого приложения) со значениями, указанными в карточках веб-приложений в поле **Узлы**, и ищет подходящее веб-приложение в указанном ниже порядке по следующим признакам:

1. **По точному совпадению значений.** Например, если заголовок `Host` имеет значение `www.example.com`, будут отобраны все веб-приложения со значением `www.example.com` в поле **Узлы**.
2. **По самому длинному имени с символом звездочки (*) в начале.** Например, если заголовок `Host` имеет значение `www.example.com`, из двух веб-приложений со значениями `*.example.com` и `*.com` в поле **Узлы** будет отобрано веб-приложение со значением `*.example.com`.
3. **По самому длинному имени с символом звездочки (*) в конце.** Например, если заголовок `Host` имеет значение `www.example.com`, из двух веб-приложений со значениями `www.example.*` и `www.*` в поле **Узлы** будет отобрано веб-приложение со значением `www.example.*`.
4. **По отсутствию узла в веб-приложении.** Например, если заголовок `Host` имеет значение `www.example.com`, будут отобраны веб-приложения, в карточке которых не указаны значения в поле **Узлы**.

Если PT AF находит веб-приложения по одному из признаков, поиск веб-приложений на первом этапе останавливается. Поиск подходящего веб-приложения на втором этапе будет выполняться среди веб-приложений, найденных на первом.

Если PT AF не находит подходящее веб-приложение ни по одному из признаков, дальнейшие действия с запросом зависят от типа изолированного пространства:

— Если запрос был получен узлом PT AF, запрос блокируется (возвращается ответ с кодом 404).

— Если запрос был получен агентом, запрос поступает серверу nginx без обработки агентом и затем направляется защищаемому приложению согласно конфигурации nginx.

> **Примечание.** В каждом изолированном пространстве доступно веб-приложение по умолчанию — **Default Application**. Это веб-приложение настроено на обработку любого трафика: в его параметрах указан самый общий путь к ресурсам `/` и не указан ни один узел. В изолированном пространстве с типом «Агент» не рекомендуется удалять это веб-приложение или указывать в нем узлы и изменять путь к ресурсам, поскольку в этом случае агент может не обрабатывать часть трафика.

Второй этап. PT AF сравнивает URI запроса (содержащий путь к ресурсу) со значениями, указанными в карточках веб-приложений в поле **Расположение**, и ищет подходящее веб-приложение в указанном ниже порядке по следующим признакам:

1. **Совпадающие с регулярными выражением.** Регулярное выражение для указания пути к ресурсу в карточке веб-приложения может содержать только символы `^` (начало пути), `$` (конец пути) и `*` (любое количество произвольных символов). Например, если URI запроса содержит путь `/shop/catalog?page=2&items=15`, будет отобрано веб-приложение с выражением `catalog$`.
2. **По самому длинному префиксу пути.** Например, если URI запроса содержит путь `/shop/catalog?page=2&items=15`, из двух веб-приложений со значениями `/` и `/shop` будет отобрано веб-приложение со значением `/shop`.

Если PT AF находит веб-приложение по одному из признаков, поиск завершается. Запрос будет обработан согласно режиму защиты и шаблону политики безопасности этого веб-приложения. После обработки запрос направляется защищаемому приложению.

> **Внимание!** В изолированном пространстве с типом **Агент** конфигурация веб-приложений, настроенная в веб-интерфейсе, не синхронизируется автоматически с конфигурацией веб-приложений, настроенной в nginx. Нужно «вручную» следить за тем, чтобы эти конфигурации совпадали.

Если PT AF не находит подходящее веб-приложение ни по одному из признаков, дальнейшие действия с запросом зависят от типа изолированного пространства:

— Если запрос был получен узлом PT AF, запрос блокируется (возвращается ответ с кодом 404).

— Если запрос был получен агентом, запрос поступает серверу nginx без обработки агентом и затем направляется защищаемому приложению согласно конфигурации nginx.

9. Работа с политиками и шаблонами политик безопасности

Параметры безопасности веб-приложения в PT AF определяются политикой безопасности.

В этом разделе приведена основная информация о политиках безопасности веб-приложений и шаблонах политик безопасности, а также даны инструкции по работе с ними.

В этом разделе

О политиках и шаблонах политик безопасности (см. раздел 9.1)

Создание шаблона политики безопасности веб-приложений (см. раздел 9.2)

Изменение политик безопасности нескольких веб-приложений (см. раздел 9.3)

Изменение политики безопасности одного веб-приложения (см. раздел 9.4)

См. также

Работа с правилами обработки трафика (см. раздел 10)

9.1. О политиках и шаблонах политик безопасности

Шаблон политики безопасности представляет из себя набор правил обработки трафика (см. раздел 10), значения параметров и выражения которых могут быть переопределены пользователем. На основе шаблонов строятся политики безопасности веб-приложений. Политики безопасности содержат набор правил из шаблонов, при этом значения параметров и выражения этих правил для политики могут быть тоже переопределены. Шаблоны могут применяться для защиты сразу нескольких веб-приложений.

При создании шаблонов и при настройке политики безопасности срабатывает механизм наследования параметров и их значений. Наследование происходит по цепочке: набор правил → шаблон политики безопасности → политика безопасности веб-приложения. Например, если вы настроили защиту нескольких веб-приложений так, что для них используется общий родительский шаблон, вы можете изменить политики безопасности сразу для всех этих приложений только за счет изменения этого шаблона.

Вы можете:

— изменить шаблон политики безопасности;

— создать шаблон политики безопасности на основе существующих наборов правил;

— к каждому приложению или набору приложений применить любой шаблон политики безопасности;

— для любого веб-приложения настроить собственную политику безопасности.

9.2. Создание шаблона политики безопасности веб-приложений

Шаблон позволяет переопределить значения параметров правил системного набора, отключить правила, а также использовать набор пользовательских правил. Вы можете создать собственный шаблон политики безопасности, если предустановленные шаблоны вам не подходят.

- Чтобы создать шаблон политики безопасности:

  1. В главном меню выберите **Схема конфигурации**.
  2. В раскрывающемся блоке **Шаблоны политик безопасности** нажмите +.
  3. В поле **Название** введите имя шаблона.
  4. В раскрывающемся списке **На основе** выберите родительский шаблон.
  5. При необходимости включите функцию использования набора пользовательских правил.
  6. Нажмите **Создать**.

9.3. Изменение политик безопасности нескольких веб-приложений

Вы можете одновременно изменить политики безопасности нескольких веб-приложений за счет изменения шаблона политики безопасности. Такая функция доступна только для тех политик веб-приложений, которые построены на основе общего шаблона. Необходимо учитывать, что параметры, переопределенные в политике безопасности веб-приложения, не будут наследовать последующие изменения соответствующих параметров в шаблоне. При отсутствии пользовательских изменений в политике все изменения шаблона этой политики безопасности отразятся в самой политике.

- Чтобы изменить политики безопасности нескольких веб-приложений:

  1. В главном меню выберите **Схема конфигурации**.
  2. В раскрывающемся блоке **Шаблоны политик безопасности** нажмите → в строке шаблона политики безопасности.

     Откроется карточка шаблона политики безопасности.
  3. Внесите необходимые изменения в шаблон и нажмите **Сохранить**.

9.4. Изменение политики безопасности одного веб-приложения

Вы можете изменить политику безопасности для одного веб-приложения, при этом не меняя параметры общего шаблона политики безопасности.

- Чтобы изменить политику безопасности веб-приложения:

  1. В главном меню выберите **Схема конфигурации**.
  2. В раскрывающемся блоке **Веб-приложения** в строке защищаемого веб-приложения нажмите  .
  3. Внесите изменения и нажмите **Сохранить**.

10. Работа с правилами обработки трафика

Правило — проверка, которая срабатывает при соблюдении определенного условия в контексте защищаемого веб-приложения и используется для обнаружения угрозы безопасности.

Правило может сработать на клиентский запрос или соответствующий ему ответ от сервера, которые удовлетворяют условию, заданному в выражении этого правила. Если в результате проверки PT AF обнаруживает угрозу безопасности, результатом работы правила будет выполнение назначенных действий (см. раздел 11).

В этом разделе

О наборах правил (см. раздел 10.1)

Группы правил обработки трафика (см. раздел 10.2)

Параметры правил обработки трафика (см. раздел 10.3)

Группировка правил (см. раздел 10.4)

Изменение правила политики безопасности веб-приложения (см. раздел 10.5)

Отключение правила обработки трафика (см. раздел 10.6)

Исключение ложных срабатываний правила (см. раздел 10.7)

Изменение ответа защищаемого сервера (см. раздел 10.8)

Создание правила и добавление его в пользовательский набор (см. раздел 10.9)

10.1. О наборах правил

Наборы правил необходимы для создания шаблонов, с помощью которых настраивается политика безопасности. Наборы правил в PT AF бывают системными (не могут быть изменены) и пользовательскими (необходимы для создания коллекции пользовательских правил). Каждый набор может одновременно применяться для нескольких шаблонов. Правила из пользовательского набора срабатывают после всех системных правил, добавленных в политику безопасности.

> **Примечание.** Правила, включенные в системные наборы, предварительно настроены на защиту ресурсов на базе указанных в названии набора технологий.

По умолчанию в системе настроены следующие наборы правил:

- ASP.NET — включает только те правила, которые предназначены для защиты веб-приложений, созданных на платформе ASP.NET;
- Apache Struts — включает только те правила, которые предназначены для защиты веб-приложений, разработанных на фреймворке Apache Struts;

— Bitrix — включает правила, которые предназначены для защиты веб-приложений, разработанных на фреймворке Bitrix Framework;

— Default Template — включает правила всех остальных системных наборов;

— Java — включает только те правила, которые предназначены для защиты веб-приложений, разработанных на языке Java;

— Joomla CMS — включает только те правила, которые предназначены для защиты веб-приложений, основанных на CMS Joomla;

— LAMP (PHP, Apache, MySQL) — включает только те правила, которые предназначены для защиты веб-приложений, разработанных при помощи инструментов PHP, Apache или MySQL;

— Microsoft Exchange — включает те правила, которые предназначены для защиты сервера Microsoft Exchange;

— Node.js — включает только те правила, которые предназначены для защиты веб-приложений, созданных на платформе Node.js;

— PHP — включает только те правила, которые предназначены для защиты веб-приложений, разработанных на языке PHP.

На основе каждого системного набора правил преднастроен одноименный пользовательский шаблон политик безопасности.

10.2. Группы правил обработки трафика

Правила из системного набора сформированы и сгруппированы на основе исследований аналитиков Positive Technologies и распространенных классификаций сетевых атак.

Далее в таблице указаны все группы правил PT AF и дано их краткое описание.

Таблица 12. Группы правил обработки трафика

Группа правил	Описание группы
Контроль доступа	Используется для отслеживания попыток аутентификации пользователя
Боты	Используется для обнаружения запросов от автоматизированных систем
Политики браузера	Реализует механизмы защиты, поддерживаемые браузерами
CSRF	Предназначена для защиты от CSRF-атак
Эксплуатация уязвимостей из списка CVE	Предназначена для защиты от атак, направленных на известные уязвимости в приложениях, которые построены на базе конкретных систем управления содержимым
Загрузка файлов	Реализует механизмы защиты путем проверки загружаемых файлов

Группа правил	Описание группы
Безопасность HTML-форм	Используется для предотвращения изменения веб-форм
Нарушение HTTP	Реализует механизмы защиты от попыток взлома посредством: — обнаружения запросов с нарушениями HTTP-стандартов; — ограничения вариативности для корректных HTTP-запросов с целью уменьшения возможностей для атак
ImageMagick	Предназначена для защиты от эксплуатации уязвимостей, связанных с обработкой изображений в ImageMagick
Внедрение	Реализует механизмы защиты от эксплуатации уязвимостей, основанных на внедрении небезопасного кода
Репутация IP-адреса	Реализует механизмы проверок пользователя по IP-адресу
J2EE	Предназначена для закрытия уязвимостей, которым могут быть подвержены веб-приложения, работающие на платформе Java 2 Enterprise Edition (J2EE)
Безопасность JWT	Предназначена для защиты от атак, направленных на JSON Web Tokens
Исполнение вредоносных файлов	Предназначена для защиты от исполнения вредоносных файлов
Предварительная обработка	Предназначена для выполнения проверок или преобразований в запросе перед выполнением остальных правил в транзакции
Доступность важных файлов	Предназначена для защиты от утечек важных данных
Сессии	Реализует механизмы управления пользовательскими сессиями и обнаружения атак на сессии
Внедрение SQL-кода	Предназначена для защиты от внедрения SQL-кода. Механизм направлен на детектирование атаки как по запросу, так и по ответу
SSRF	Предназначена для защиты от SSRF-атак
Безопасность XML	Предназначена для защиты от XML-атак
XSS	Реализует механизмы защиты от атак, в которых используется межсайтовое выполнение сценариев (XSS). XSS позволяет злоумышленнику получить доступ к любым файлам куки, токенам сеансов или другой конфиденциальной информации, хранящейся в браузере и используемой на сайте, а также переписать содержимое HTML-страницы

10.3. Параметры правил обработки трафика

Правило обработки трафика в PT AF определяется следующими параметрами:

- **Имя** — имя правила;
- **Активно** — статус активности правила;
- **Происхождение** (в правилах из системного набора) — шаблон политики безопасности, в который включено правило;
- **Действия при срабатывании** — действия над трафиком, которые выполняет PT AF в результате срабатывания правила;
- **Группа правил** (в правилах из системного набора) — название группы, в которую входит правило;
- **Точность** (в правилах из системного набора) — точность определения атаки правилом (от 0 до 10), основанная на оценке экспертов Positive Technologies. Оценка 10 означает, что правило не допускает ложных срабатываний;
- **Фаза** — фаза срабатывания (например, **На ответе**, **На запросе**);
- **Теги** — одна или несколько меток атак, обнаруженных в результате срабатывания правила;
- **Классификация** — классификация атак, обнаруженных в результате срабатывания правила;
- **Тип** — тип угрозы безопасности, обнаруженной в результате срабатывания правила;
- **Уровень опасности** — уровень опасности события безопасности, зарегистрированного в результате срабатывания правила;
- **Ревизия** — версия правила.

10.4. Группировка правил

Правила в списке могут быть представлены в сгруппированном виде. Группировка позволяет сворачивать в одну строку несколько правил на основе одного или нескольких атрибутов.

- Чтобы сгруппировать правила,

  над списком правил нажмите  и в раскрывшемся меню выберите один или несколько пунктов, соответствующих атрибутам для группировки.

  Правила в списке отображаются в сгруппированном виде. Одновременно с группировкой вы можете использовать фильтры.

- Чтобы отменить группировку,

  над списком правил нажмите  и в раскрывшемся меню выберите пункт **Отменить группировку**.

10.5. Изменение правила политики безопасности веб-приложения

Вы можете изменять параметры правил политик безопасности или пользовательских шаблонов политик безопасности, а также включать и отключать правила.

- Чтобы изменить правило политики безопасности веб-приложения:

  1. В главном меню выберите **Схема конфигурации**.
  2. В раскрывающемся блоке **Веб-приложения** в строке защищаемого веб-приложения нажмите .
  3. В строке правила нажмите .
  4. Внесите изменения и нажмите **Сохранить**.

См. также

Настройка пользовательского правила с использованием глобального списка (см. раздел 12.10)

10.6. Отключение правила обработки трафика

Вы можете отключить правило, если, например, оно работает неправильно или вызывает большое количество ложных срабатываний для защищаемого веб-приложения. При отключении правила необходимо учитывать, что оно не будет задействовано для обработки HTTP-пакетов.

- Чтобы отключить правило обработки трафика политики безопасности веб-приложения:

  1. В главном меню выберите **Схема конфигурации**.
  2. В раскрывающемся блоке **Веб-приложения** в строке защищаемого веб-приложения нажмите .
  3. В строке правила отключите функцию **Активно**.

Вы также можете отключать правила в пользовательских шаблонах политик безопасности.

10.7. Исключение ложных срабатываний правила

По умолчанию проверка правилом выполняется всегда, если правило включено. Вы можете задать условия для отмены проверки. Условия запуска проверки позволяют исключить ложные срабатывания. Если условия исключения выполнены, проверка не запускается.

Вы можете настроить исключения ложных срабатываний правил двумя способами:

— через политику безопасности веб-приложения; (см. раздел 10.7)

— через событие безопасности (см. раздел 10.7).

Исключение ложных срабатываний правил через политику безопасности

Вы можете перейти к настройке исключений ложных срабатываний правила из политики безопасности веб-приложения. В этом случае исключение будет настроено для конкретного веб-приложения.

► Чтобы исключить ложные срабатывания правил:

1. В главном меню выберите **Схема конфигурации**.
2. В раскрывающемся блоке **Веб-приложения** в строке защищаемого веб-приложения нажмите .
3. В строке правила нажмите .
4. Нажмите .
5. Нажмите **Добавить группу условий** и выберите параметр для настройки исключений (см. приложение В).
6. Для выбранного параметра укажите условие, при котором правило игнорируется.
7. Если требуется добавить еще одно условие, нажмите **Добавить условие**.

   Примечание. Несколько условий из одной группы объединяются с помощью конъюнкции (логического И).
8. Если требуется добавить еще одну группу условий, нажмите **Добавить группу условий**.

   Примечание. Несколько групп условий объединяются с помощью дизъюнкции (логического ИЛИ).
9. Нажмите **Сохранить**.

Исключение ложных срабатываний правила для политики безопасности настроено.

Исключение ложных срабатываний правила через событие безопасности

Вы можете перейти к настройке исключений ложных срабатываний правила из таблицы событий безопасности. Таким образом вы можете настроить исключение для конкретной политики безопасности или для шаблона политики безопасности.

Примечание. Исключения, настроенные для шаблона политики безопасности, будут работать для всех политик безопасности, которые созданы на основе этого шаблона.

► Чтобы исключить ложные срабатывания правил:

1. В главном меню выберите раздел **События безопасности**.
2. В строке события нажмите ▶|.

   Примечание. Вы также можете перейти к настройке исключений из карточки события безопасности. Для этого откройте карточку события и нажмите ▶|.
3. Выберите, куда будет добавлено исключение ложных срабатываний правила: в шаблон политики безопасности или в политику безопасности веб-приложения.
4. Нажмите **Добавить группу условий** и выберите параметр для настройки исключений (см. приложение В).
5. Для выбранного параметра укажите условие, при котором правило игнорируется.
6. Если требуется добавить еще одно условие, нажмите **Добавить условие**.

   Примечание. Несколько условий из одной группы объединяются с помощью конъюнкции (логического И).
7. Если требуется добавить еще одну группу условий, нажмите **Добавить группу условий**.

   Примечание. Несколько групп условий объединяются с помощью дизъюнкции (логического ИЛИ).
8. Нажмите **Сохранить**.

Исключение ложных срабатываний правила настроено в зависимости от выбранного на шаге 3 варианта: для политики безопасности или для шаблона политики безопасности.

10.8. Изменение ответа защищаемого сервера

Если при срабатывании правила необходимо изменить ответ защищаемого сервера, вы можете применить в правиле действие с типом **Отправлять свой ответ**. В теле ответа вы можете указать собственный текст HTML-страницы или переменную (см. раздел 11.6), значение которой будет содержаться в ответе. Признаком начала имени переменной является символ «%».

Примечание. В правиле не может быть установлено несколько действий с типом **Отправлять свой ответ** и одинаковым кодом ответа.

► Чтобы изменить ответ защищаемого сервера:

1. В главном меню выберите **Схема конфигурации**.
2. В раскрывающемся блоке **Действия** нажмите +.

3. В поле **Название** укажите название действия (максимальная длина — 64 символа; допустимо использование букв русского и латинского алфавита, а также спецсимволов).
4. Выберите тип **Отправлять свой ответ**.
5. В поле **Код** введите код того ответа, текст которого требуется изменить.
6. Выберите MIME-тип контента сообщения (**Заголовок Content-Type**).
7. Если требуется добавить в ответ дополнительный заголовок, нажмите **Добавить** и введите название заголовка и его значение.

   Примечание. Заголовки Date, Server, Transfer-Encoding, Content-Type, Content-Length и Connection добавляются в ответ по умолчанию.
8. В поле **Тело ответа** введите текст HTML-страницы для отображения или переменную (см. раздел 11.6), значение которой будет содержаться в ответе.
9. Нажмите **Создать**.
10. Откройте карточку правила (см. раздел 10.5), в поле **Действия при срабатывании** выберите созданное действие и нажмите **Сохранить**.

В случае срабатывания правила, к которому применено созданное действие, ответ от защищаемого сервера будет изменен.

10.9. Создание правила и добавление его в пользовательский набор

Если правил из системного набора вам недостаточно, вы можете создать собственное правило, добавив его в пользовательский набор.

Внимание! Пользовательские правила срабатывают после всех системных правил, добавленных в политику безопасности.

Вы можете создавать пользовательские правила в разделе **Схема конфигурации** → **Набор пользовательских правил**.

Создание нового пользовательского правила

► Чтобы создать правило и добавить его в пользовательский набор:

1. В раскрывающемся блоке **Набор пользовательских правил** нажмите →.
2. Нажмите +.
3. Введите название правила.
4. Введите теги для облегчения поиска на дашборде похожих событий безопасности, которые будут зарегистрированы в результате срабатывания правила.

5. Выберите тип события безопасности, которое будет зарегистрировано в случае срабатывания правила.
6. Выберите уровень опасности события безопасности, которое будет зарегистрировано в результате срабатывания правила.
7. Если для кода проверки трафика требуется ввести пользовательский параметр:
   - В строке **Параметры** нажмите **Добавить**.
   - Введите название пользовательского параметра.
   - В поле **Отображаемое название** введите то название параметра, которое будет отображаться на вкладке **Конфигурация правила** при редактировании пользовательского правила в шаблоне политики веб-приложения или в политике веб-приложения.
   - Выберите тип данных параметра.
   - В поле **Значение по умолчанию** введите значение параметра, которое будет предустановленным.
8. Введите код правила, используя синтаксис языка пользовательских правил (см. приложение Б).
9. Выберите действия над трафиком, которые необходимо выполнить PT AF в результате срабатывания правила.
10. Нажмите **Создать**.

Создание пользовательского правила на основе существующего

Чтобы создать пользовательское правило на основе существующего:

1. В раскрывающемся блоке **Набор пользовательских правил** нажмите →.
2. В строке правила нажмите →.
3. Нажмите **Действия** → **Копировать**.

   Откроется окно создания пользовательского правила. Поля будут заполнены значениями параметров правила, на основе которого создается новое правило.
4. Измените название правила и внесите другие необходимые изменения.

   Примечание. Название пользовательского правила должно быть уникальным в рамках изолированного пространства.
5. Нажмите **Создать**.

11. Работа с действиями

Действие — это реакция системы на срабатывание правила. В зависимости от типа действия (см. раздел 11.4) при срабатывании правила PT AF может:

- добавить IP-адрес в динамический список;
- добавить IP-адрес в список подозрительных адресов, которым будет показываться CAPTCHA.
- зарегистрировать событие в базе данных;
- добавить, изменить или удалить заголовок запроса или ответа;
- заблокировать запрос и отправить ответ;
- отправить данные о событии на удаленный сервер;
- остановить дальнейшую проверку запроса;
- закрыть соединение без отправки ответа клиенту.

Действия делятся на системные и пользовательские. По умолчанию доступны системные действия **Block**, **CAPTCHA**, **Close connection without response**, **Log to db** и **Skip rules**. Вы можете создавать пользовательские действия и управлять ими на странице **Схема конфигурации** → **Действия**.

В этом разделе

Создание действия (см. раздел 11.1)

Изменение действия (см. раздел 11.2)

Удаление действия (см. раздел 11.3)

Типы действий (см. раздел 11.4)

Ограничения на использование действий в правилах обработки трафика (см. раздел 11.5)

Переменные для создания действий (см. раздел 11.6)

11.1. Создание действия

Создание нового действия

- Чтобы создать действие:

  1. В раскрывающемся блоке **Действия** нажмите +.
  2. Введите название действия.

Примечание. Название должно быть уникальным в рамках изолированного пространства и может содержать до 64 символов. Допустимые символы — буквы русского и латинского алфавитов, цифры, специальные символы.

3. Выберите тип действия (см. раздел 11.4).
4. Укажите параметры действия.

   Примечание. После создания действия параметр **Тип** будет недоступен для изменения. Вы сможете изменить только название действия и параметры, привязанные к его типу.
5. Нажмите **Создать**.

Создание действия на основе существующего

Вы можете создавать новые действия на основе ранее созданных пользовательских действий.

- Чтобы создать действие на основе существующего:

1. В раскрывающемся блоке **Действия** строке с названием действия нажмите →.
2. Нажмите **Действия** → **Копировать**.

   Откроется окно создания пользовательского действия. Поля будут заполнены значениями параметров действия, на основе которого создается новое действие.
3. Измените название действия и внесите другие необходимые изменения.

   Примечание. Название пользовательского действия должно быть уникальным в рамках изолированного пространства. После создания действия параметр **Тип** будет недоступен для изменения.
4. Нажмите **Создать**.

11.2. Изменение действия

Вы можете изменять только пользовательские действия. Системные действия недоступны для изменения. Также невозможно изменить тип действия.

- Чтобы изменить действие:

1. В раскрывающемся блоке **Действия** строке с названием действия нажмите →.

   Откроется карточка действия.
2. Внесите изменения.
3. Нажмите **Сохранить**.

11.3. Удаление действия

Вы можете удалить только те действия, которые не используются в правилах. Также для удаления недоступны системные действия.

- Чтобы удалить действие:

  1. В раскрывающемся блоке **Действия** строке с названием действия нажмите →.

     Откроется карточка действия.

  2. Нажмите **Удалить действие** и подтвердите удаление.

Информация об удаленном действии сохранится в записях о событиях безопасности, но ссылка на действие будет удалена.

11.4. Типы действий

При создании пользовательского действия нужно выбрать его тип. Ниже описаны возможные типы действий и их параметры.

Добавлять IP-адрес клиента в глобальный динамический список

При срабатывании правила система добавляет IP-адрес в динамический список.

Параметры действия:

— **Название** — название действия, должно быть уникальным в пределах изолированного пространства.

— **Время жизни (TTL)** — период в минутах, на который IP-адреса добавляются в список (не более 10 080 минут).

— **Глобальный динамический список** — динамический список, в который будет добавлен IP-адрес при срабатывании правила.

Записывать событие в базу данных

При срабатывании правила система регистрирует событие в базе данных.

Параметры действия:

— **Название** — название действия, должно быть уникальным в пределах изолированного пространства.

— **Сохранять необработанные данные** — при включении параметра система сохраняет необработанные данные (параметр включен по умолчанию).

Примечание. В карточке атаки будут отображаться первые 100 КБ необработанного запроса и ответа. В базе данных сохраняется 1 МБ запроса и 2 МБ ответа.

— **Маскировать совпадения** — при включении параметра в разделе **Совпадения** в карточках событий будут маскироваться совпавшие значения полей, названия которых указаны в параметре **Маскируемые поля**.

— **Маскируемые поля** — список названий полей, значения которых будут маскироваться (список по умолчанию — `api`, `token`, `key`, `secret`, `private`, `pass`, `password`, `authorization`, `access_token`, `private_token`, `private-token`). Названия полей для маскирования проверяются без учета регистра.

— **Заменять значение на** — значение, которое будет подставляться вместо значения поля при маскировании.

— **Максимальная длина совпавшего параметра** — максимальный размер значения совпавшего ключа (в байтах), записываемого в базу данных.

Изменять заголовки запроса

При срабатывании правила система добавляет, изменяет или удаляет заголовок запроса.

> **Внимание!** Действия типа **Изменять заголовки запроса,** добавленные в правила, срабатывают при обнаружении правилами подозрительного трафика и позволяют пометить его. В PT AF вы также можете создавать действия с заголовками для веб-приложений (см. раздел 8.2.8). Такие действия позволяют изменять заголовки запросов, например для передачи защищаемому серверу атрибутов сертификатов или IP-адресов клиентов. Таким образом, действия в правилах и в веб-приложениях срабатывают на разных этапах обработки трафика. Не рекомендуется использовать для одного заголовка два действия одновременно: действие типа **Изменять заголовки запроса** в правилах обработки трафика и действие с заголовком для веб-приложения. Это может привести к нежелательным последствиям.

Параметры действия:

— **Название** — название действия, должно быть уникальным в пределах изолированного пространства.

— **Действия** — варианты действий с заголовком:

- **Добавить заголовок.** Действие добавляет заголовок с указанным названием, если заголовка нет или допускается его дублирование. Если заголовок есть и его дублирование не допускается, действие не выполняется.
- **Изменить заголовок.** Действие изменяет заголовок с указанным названием, если он один. Если заголовка нет или есть несколько заголовков с таким названием, действие не выполняется.
- **Удалить заголовок.** Действие удаляет все заголовки с указанным названием.

— **Заголовок** — название заголовка (не более 200 символов).

— **Значение заголовка** — значение заголовка (не более 6000 символов).

> **Примечание.** Вы можете добавлять переменные (см. раздел 11.6) в значение заголовка. Формат — %<Название переменной>.

Также в карточке действия приведены неизменяемые и уникальные заголовки. Значение неизменяемого заголовка устанавливается системой, а уникальный заголовок не может повторяться в запросе.

Изменять заголовки ответа

При срабатывании правила система добавляет, изменяет или удаляет заголовок ответа на запрос.

Параметры действия:

— **Название** — название действия, должно быть уникальным в пределах изолированного пространства.

— **Действия** — варианты действий с заголовком:

- **Добавить заголовок.** Действие добавляет заголовок с указанным названием, если заголовка нет или допускается его дублирование. Если заголовок есть и его дублирование не допускается, действие не выполняется.
- **Изменить заголовок.** Действие изменяет заголовок с указанным названием, если он один. Если заголовка нет или есть несколько заголовков с таким названием, действие не выполняется.
- **Удалить заголовок.** Действие удаляет все заголовки с указанным названием.

— **Заголовок** — название заголовка (не более 200 символов).

— **Значение заголовка** — значение заголовка (не более 6000 символов).

Примечание. Вы можете добавлять переменные (см. раздел 11.6) в значение заголовка. Формат — %<Название переменной>.

Также в карточке действия приведены неизменяемые заголовки. Их значения устанавливаются системой.

Отправлять свой ответ

При срабатывании правила система блокирует запрос и отправляет ответ.

Параметры действия:

— **Название** — название действия, должно быть уникальным в пределах изолированного пространства.

— **Код** — код ответа.

— **Заголовок Content-Type** — MIME-тип тела ответа.

— **Дополнительные заголовки** — дополнительные заголовки, которые будут добавлены в ответ. Поля для ввода названия заголовка и его значения отображаются по кнопке **Добавить заголовок**.

— **Тело ответа** — тело ответа от PT AF.

Примечание. Вы можете добавлять переменные (см. раздел 11.6) в значение заголовка и в тело ответа. Формат — %<Название переменной>.

Также в карточке действия приведены неизменяемые заголовки. Их значения устанавливаются системой.

Отправлять событие на syslog-сервер

При срабатывании правила система отправляет данные о событии на удаленный syslog-сервер.

Параметры действия:

- **Название** — название действия, должно быть уникальным в пределах изолированного пространства.
- **IP-адрес или имя узла** — IP-адрес или имя узла syslog-сервера.
- **Протокол** — протокол для отправки syslog-сообщений (UDP или TCP).
- **Порт** — порт, прослушиваемый syslog-сервером.
- **Максимальный размер сообщения** — максимальный размер отправляемого syslog-сообщения (для протокола UDP не более 65 507 байт, для TCP — 1 048 576 байт). При использовании шаблона **Custom** сообщение сокращается[8], если его размер превышает максимальный.
- **Шаблон** — шаблон события безопасности для отправки на syslog-сервер. В зависимости от выбранного шаблона меняется формат передачи данных.

При выборе шаблона, отличного от **Custom**, действие содержит следующие параметры:

- **Формат** (параметр недоступен для изменения) — стандарт syslog-сообщений.
- **Основные сведения** (параметр недоступен для изменения) — данные о событии безопасности, устанавливаемые системой, которые будут переданы в syslog-сообщении.
- **Содержимое** — данные о событии безопасности, доступные для выбора пользователем, которые будут переданы в syslog-сообщении.

8 При сокращении сообщения сначала обрезаются подставленные в шаблон значения переменных, начиная с последнего. Каждое значение сокращается до тех пор, пока размер сообщения не станет допустимым или пока значение не достигнет лимита **Минимальный размер сокращенного значения**. Если после сокращения всех значений переменных размер сообщения превышает лимит, сообщение обрезается по краю максимального размера. Если при сокращении была обрезана часть многобайтового символа, оставшиеся байты этого символа удаляются.

При выборе шаблона **Custom** действие содержит следующие параметры:

- **Формат** — пользовательский формат передаваемого syslog-сообщения, для его задания вы можете использовать переменные (см. раздел 11.6). Максимальная длина значения — 10 000 символов. Примеры пользовательского формата сообщений приведены ниже.
- **Экранируемые символы** — символы, которые будут экранироваться в syslog-сообщении в подставляемых на место переменных значениях. Максимальная длина значения — 100 символов.

  Примечание. При подстановке переменных `EVENT_TAGS`, `ACTION_IDS`, `ACTION_NAMES`, `ACTION_TYPES`, `MATCHED_VARIABLES`, `MATCHED_KEYS`, `MATCHED_VALUES`, `REQUEST_GET`, `REQUEST_POST`, `REQUEST_COOKIES`, `REQUEST_HEADERS`, `RESPONSE_HEADERS` обрамляющие и разделительные символы (двойные кавычки, запятые и двоеточия) не экранируются.
- **Экранировать управляющие символы** — параметр отвечает за экранирование управляющих символов U+0000 — U+001F в соответствии с RFC 8259.
- **Передавать BOM-символы** — параметр отвечает за передачу в syslog-сообщениях служебных BOM-символов, указывающих на кодировку юникода и порядок байтов. По умолчанию выключен.
- **Минимальный размер сокращенного значения** — минимальный размер каждого значения переменной после сокращения.

Для проверки связи с syslog-сервером карточка действия содержит кнопку **Отправить тестовое сообщение**.

Далее приведены примеры пользовательских форматов syslog-сообщений.

Примечание. Переносы строк и отступы добавлены в примеры для наглядности, формат syslog-сообщения необходимо указывать в одну строку.

Пример пользовательского шаблона сообщения в формате CEF:

```
CEF:0|Positive Technologies|Application Firewall|4.5.0|%EVENT_ID|%RULE_NAME|
%EVENT_INT_SEVERITY|src=%CLIENT_IP msg=Application: %APPLICATION_NAME, ApplicationId:
%APPLICATION_ID, Path: %REQUEST_PATH, Parameter: %MATCHED_VARIABLES
```

Пример пользовательского шаблона сообщения в формате JSON:

```
{
    "timestamp": "%TIMESTAMP",
    "event_id": "%EVENT_ID",
    "rule_name": "%RULE_NAME",
    "severity": "%EVENT_SEVERITY",
    "actions": {%ACTION_NAMES},
    "tags": {%EVENT_TAGS},
    "client_ip": "%CLIENT_IP",
    "client_useragent": "%CLIENT_USERAGENT",
    "application_name": "%APPLICATION_NAME",
    "application_id": "%APPLICATION_ID",
    "request_method": "%REQUEST_METHOD",
```

```
    "request_path": "%REQUEST_PATH",
    "request_headers": {%REQUEST_HEADERS},
    "matched_variables": {%MATCHED_VARIABLES},
    "matched_keys": {%MATCHED_KEYS},
    "matched_values": {%MATCHED_VALUES}
}
```

Не проверять событие правилами

При срабатывании правила дальнейшая проверка запроса не выполняется. Этот тип установлен только для системного действия **Skip rules**, которое по умолчанию используется в правиле **Не проверять статические ресурсы**, и не может быть установлен для пользовательского действия.

Закрывать соединение

При срабатывании правила PT AF закрывает соединение без отправки ответа клиенту. Этот тип установлен только для системного действия **Close connection without response**, которое по умолчанию используется в правиле **Сканер уязвимостей**, и не может быть установлен для пользовательского действия.

CAPTCHA

При срабатывании правила PT AF добавляет IP-адрес, с которого был отправлен запрос, в список подозрительных IP-адресов. При отправке запроса с подозрительного IP-адреса будет необходимо решить CAPTCHA.

Если CAPTCHA была решена до добавления IP-адреса в список подозрительных, и запросы с этого IP-адреса продолжают поступать с ранее выданным токеном доступа, PT AF извлечет из токена доступа идентификатор сессии и добавит его в список отозванных сессий. В связи с этим необходимо будет повторно решить CAPTCHA.

Этот тип установлен только для системного действия **CAPTCHA** и не может быть установлен для пользовательского действия.

> **Примечание.** Действие **CAPTCHA** работает в связке с правилом Использовать CAPTCHA, с помощью которого можно настроить параметры CAPTCHA.

11.5. Ограничения на использование действий в правилах обработки трафика

При использовании действий в правилах необходимо учитывать ряд ограничений:

— В параметрах правила можно выбрать только одно действие с типом **Отправлять свой ответ** и уникальным кодом ответа.

— В одном правиле не могут быть одновременно выбраны действия с типами:

- **Отправлять свой ответ** и **Не проверять событие правилами**;
- **Отправлять свой ответ** и **Изменять заголовки запроса**;
- **Закрывать соединение** и **Не проверять событие правилами**;
- **Закрывать соединение** и **Отправлять свой ответ**.
- **CAPTCHA** и действия с типами, отличными от **Добавлять IP-адрес клиента в глобальный динамический список**, **Записывать событие в базу данных**, **Отправлять событие на syslog-сервер**.

— Для каждого правила может быть выбрано только одно действие с типом **Записывать событие в базу данных**.

— При выборе действия с типом **Отправлять событие на syslog-сервер** также необходимо выбрать действие с типом **Записывать событие в базу данных**.

— Выполнение действия с типом **Отправлять свой ответ** блокирует выполнение действия с типом **Изменять заголовки ответа** (при их наличии в одном правиле).

— В одном правиле можно выбрать несколько действий с типом **Изменять заголовки запроса** или **Изменять заголовки ответа**, в которых указано одно и то же название заголовка (без учета регистра), только если действия добавляют этот заголовок.

11.6. Переменные для создания действий

Действия с типами **Изменять заголовки запроса**, **Изменять заголовки ответа**, **Отправлять свой ответ** и **Отправлять событие на syslog-сервер** поддерживают переменные. Формат добавления переменной — `%<Название переменной>`.

Таблица 13. Переменные для создания действий с типами «Изменять заголовки запроса», «Изменять заголовки ответа» и «Отправлять свой ответ»

Название	Описание
APPLICATION_ID	Идентификатор веб-приложения
APPLICATION_NAME	Название веб-приложения
CLIENT_AUTH_TYPE	Тип аутентификации (базовая, на основе HTML-форм или структуры JSON)

Название	Описание
CLIENT_BROWSER_NAME	Название браузера клиента
CLIENT_BROWSER_VERSION	Версия браузера клиента
CLIENT_CITY	Название города клиента
CLIENT_COUNTRY	Двухбуквенный код страны клиента
CLIENT_GEO	Набор геоданных
CLIENT_IP	IP-адрес клиента
CLIENT_OS_NAME	Семейство операционной системы рабочей станции клиента
CLIENT_PROTO	Протокол соединения
CLIENT_REGION	Регион клиента внутри страны
CLIENT_USERNAME	Логин пользователя
MATCHED	Данные из запроса или ответа, которые привели к срабатыванию правила
NODE_LISTEN_ADDRESS	IP-адрес для прослушивания запросов
PROCESSING_TIME	Время обработки HTTP-транзакции
REQUEST_BODY	Тело запроса
REQUEST_COOKIES	Сессионные куки запроса
REQUEST_FILES	Файлы, передаваемые в запросе
REQUEST_GET	Параметры запроса, передаваемые в URI (GET-параметры запроса)
REQUEST_HEADERS	Заголовки запроса
REQUEST_HTTP_VERSION	Версия HTTP
REQUEST_METHOD	Метод запроса
REQUEST_PATH	Путь к ресурсу
REQUEST_POST	Параметры запроса в теле (POST-параметры)
REQUEST_QUERY	Строка с параметрами запроса
REQUEST_SIZE	Размер запроса в байтах
REQUEST_URI	URI запроса
RESPONSE_BODY	Тело ответа
RESPONSE_HEADERS	Заголовки ответа
RESPONSE_SIZE	Размер ответа в байтах
RESPONSE_STATUS_CODE	Код ответа

Название	Описание
RULE_ID	Идентификатор правила
TIMESTAMP	Время срабатывания правила
TRANSACTION_ID	Идентификатор HTTP-транзакции
WEBSOCKET_DOWNSTREAM	Сообщение от веб-приложения, передаваемое клиенту по протоколу WebSocket
WEBSOCKET_UPSTREAM	Сообщение от клиента, передаваемое веб-приложению по протоколу WebSocket

Таблица 14. Переменные для создания действий с типом «Отправлять событие на syslog-сервер»

Название	Описание
ACTION_IDS	Идентификаторы[9] действий
ACTION_NAMES	Названия[9] действий
ACTION_TYPES	Типы[9] действий
APPLICATION_ID	Идентификатор веб-приложения
APPLICATION_NAME	Название веб-приложения
CLIENT_BROWSER_NAME	Название браузера клиента
CLIENT_BROWSER_VERSION	Версия браузера клиента
CLIENT_CITY	Название города клиента
CLIENT_COUNTRY	Двухбуквенный код страны клиента
CLIENT_IP	IP-адрес клиента
CLIENT_OS_NAME	Семейство операционной системы рабочей станции клиента
CLIENT_PORT	Порт клиента
CLIENT_REGION	Регион клиента внутри страны
CLIENT_USERAGENT	User-Agent клиента
CLIENT_USERNAME	Логин пользователя
EVENT_DESCRIPTION	Описание сработавшего правила
EVENT_ID	Идентификатор события безопасности
EVENT_INT_SEVERITY	Уровень опасности[10] события

9 Значения заключаются в двойные кавычки и разделяются запятой. Пример: `"value1","value2","value3"`.

10 Числовое значение от 0 до 4.

Название	Описание
EVENT_SEVERITY	Название уровня опасности[11] события
EVENT_TAGS	Теги[12] события безопасности
HOSTNAME	Имя узла кластера PT AF, на который поступил запрос
MATCHED_KEYS	Ключи[12] переменных, на которых сработало правило
MATCHED_NOTES	Описание совпавших значений
MATCHED_VALUES	Значения[12] переменных, на которых сработало правило
MATCHED_VARIABLES	Названия[13] переменных, на которых сработало правило
REQUEST_COOKIES	Сессионные куки[14] запроса
REQUEST_GET	Параметры[14] запроса, передаваемые в URI (GET-параметры запроса)
REQUEST_HEADERS	Заголовки[14] запроса
REQUEST_HOST	Значение заголовка `Host` из запроса
REQUEST_METHOD	Метод запроса
REQUEST_PATH	Путь к ресурсу
REQUEST_POST	Параметры[14] запроса в теле (POST-параметры)
REQUEST_QUERY	Строка с параметрами запроса
REQUEST_SIZE	Размер запроса в байтах
REQUEST_URI	URI запроса
RESPONSE_HEADERS	Заголовки[14] ответа
RESPONSE_SIZE	Размер ответа в байтах
RESPONSE_STATUS_CODE	Код ответа
RULE_ID	Идентификатор правила
RULE_NAME	Название правила

11 Название: `unset`, `none`, `low`, `medium`, `high`.

12 Значения заключаются в двойные кавычки и разделяются запятой. Пример: `"value1","value2","value3"`.

13 Значения заключаются в двойные кавычки и разделяются запятой. Пример: `"REQUEST_PATH","REQUEST_HEADERS","REQUEST_BODY"`.

14 Каждый ключ и каждое значение заключаются в двойные кавычки. Ключи и значения разделяются двоеточием, пары ключ-значение разделяются запятой. Пример: `"key1":"value1","key2":"value2","key3":"value3"`.

Название	Описание
RULE_PHASE	Фаза [15], на которой сработало правило
TENANT_ID	Идентификатор изолированного пространства
TIMESTAMP	Время [16] срабатывания правила
TRANSACTION_ID	Идентификатор HTTP-транзакции

15 Название фазы: `undefined`, `on_script_engine_init`, `on_transaction_start`, `on_request`, `on_response`, `on_transaction_complete`, `on_transaction_process`, `on_websocket_upstream`, `on_websocket_downstream`, `on_icap_check`.

16 Формат значения — ISO 8601 (с точностью до микросекунд). Пример: `2026-04-08T13:03:04.123456Z`.

12. Работа с глобальными списками

Глобальный список — это список IP-адресов в нотации CIDR, доступный в рамках изолированного пространства для настройки защиты веб-приложений. На основе данных из глобальных списков вы можете гибко настраивать условия срабатывания правил. Например, правило может срабатывать при получении запросов от IP-адресов, как входящих в список, так и отсутствующих в нем.

Глобальные списки делятся на статические и динамические. Данные статических списков загружаются из текстового файла и не изменяются при работе системы. Динамические списки заполняются при срабатывании правил и хранят записи не более одной недели. Также вы можете вручную добавлять записи в динамический список.

Вы можете использовать глобальные списки:

- в системных правилах для блокировки запроса по IP-адресу;
- в пользовательских правилах (см. раздел 12.10);
- для исключения ложных срабатываний правила (см. раздел 12.11);
- для настройки агрегации событий (см. раздел 14.5) (только динамические списки);
- для создания действия типа **Добавлять IP-адрес клиента в глобальный динамический список** (только динамические списки).

Вы можете создавать глобальные списки и управлять ими на странице **Схема конфигурации → Глобальные списки**. По умолчанию в системе доступен динамический список **Aggregation blacklist**.

В этом разделе

Создание статического списка (см. раздел 12.1)

Создание динамического списка (см. раздел 12.2)

Изменение статического списка (см. раздел 12.3)

Удаление глобального списка (см. раздел 12.4)

Применение изменений в статических списках (см. раздел 12.5)

Поиск IP-адреса в глобальных списках (см. раздел 12.6)

Добавление IP-адресов в динамический список вручную (см. раздел 12.7)

Удаление IP-адреса из динамического списка (см. раздел 12.8)

Экспорт данных глобального списка (см. раздел 12.9)

Настройка пользовательского правила с использованием глобального списка (см. раздел 12.10)

Настройка исключений с использованием глобального списка (см. раздел 12.11)

12.1. Создание статического списка

Для создания статического списка вам потребуется текстовый файл, каждая строка которого может содержать IP-адрес в нотации CIDR, являться комментарием или быть пустой строкой. Единичный IP-адрес допускается указывать без маски /32. Строки с комментариями должны начинаться с символа #.

Например:

```
# C&C list
192.0.2.7
198.51.100.0/32

203.0.113.0/27
```

- Чтобы создать статический список:

1. В раскрывающемся блоке **Глобальные списки** нажмите +.
2. Выберите тип списка **Статический**.
3. Введите название списка.
4. Нажмите **Выберите файл** и укажите файл со списком IP-адресов.
5. Нажмите **Добавить**.

Для использования списка в правилах необходимо применить изменения в конфигурации статических списков (см. раздел 12.5).

12.2. Создание динамического списка

- Чтобы создать динамический список:

1. В раскрывающемся блоке **Глобальные списки** нажмите +.
2. Выберите тип списка **Динамический**.
3. Введите название списка.
4. Нажмите **Добавить**.

12.3. Изменение статического списка

Вы можете изменить название и описание статического списка, а также входящие в него IP-адреса. Для изменения IP-адресов вам потребуется скачать текстовый файл (см. раздел 12.9) для последующего изменения или создать такой файл заново. Каждая строка файла может содержать IP-адрес в нотации CIDR или комментарий или быть пустой строкой. Единичный IP-адрес допускается указывать без маски /32. Комментарий должен начинаться с символа #.

- Чтобы изменить статический список:

  1. В строке с названием списка нажмите →.
  2. Измените название и описание списка.
  3. Нажмите **Выберите файл** и укажите файл со списком IP-адресов.
  4. Нажмите **Сохранить**.

После изменения списка IP-адресов необходимо применить изменения в конфигурации статических списков (см. раздел 12.5). Если были изменены только название и описание списка, применение изменений в конфигурации не требуется.

12.4. Удаление глобального списка

Вы можете удалить только те списки, которые не используются в правилах и в действиях типа **Добавлять IP-адрес клиента в глобальный динамический список**.

- Чтобы удалить глобальный список:

  1. В строке с названием списка нажмите →.
  2. В карточке списка нажмите **Действия**.
  3. В раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

  Система пометит список к удалению.

Отмеченный к удалению список невозможно изменить или использовать в правилах. Вы можете только сохранить его в текстовый файл (см. раздел 12.9). Список будет полностью удален после применения изменений в конфигурации (см. раздел 12.5).

12.5. Применение изменений в статических списках

Создание статического списка, его удаление, а также обновление текстового файла для ранее созданного списка вносят изменения в конфигурацию статических списков. Эти изменения не применяются автоматически, их необходимо применять вручную для использования новой конфигурации в правилах обработки трафика.

Для снижения нагрузки на систему при наличии нескольких текстовых файлов, подготовленных к загрузке в списки, рекомендуется сначала загрузить все файлы, а затем применить изменения.

- Чтобы применить изменения,

  в раскрывающемся блоке **Глобальные списки** нажмите ✓.

12.6. Поиск IP-адреса в глобальных списках

- Чтобы найти IP-адрес в глобальных списках:

  1. В раскрывающемся блоке **Глобальные списки** нажмите .
  2. Введите IP-адрес и нажмите **Найти**.

  Если IP-адрес содержится в глобальных списках, в карточке поиска появится их перечень.

12.7. Добавление IP-адресов в динамический список вручную

- Чтобы добавить IP-адреса:

  1. В строке с названием списка нажмите .
  2. В карточке списка нажмите .
  3. Добавьте IP-адреса.

     Примечание. В одну строку можно добавить только один IP-адрес.
  4. В поле **Время жизни (TTL)** укажите период в минутах, на который IP-адреса будут добавлены в список (1—10080 или 0 — бессрочно).
  5. Нажмите **Добавить**.

12.8. Удаление IP-адреса из динамического списка

- Чтобы удалить IP-адрес:

  1. В раскрывающемся блоке **Глобальные списки** нажмите .
  2. Введите IP-адрес и нажмите **Найти**.
  3. Удалите IP-адрес:

     - Если необходимо удалить IP-адрес (точное совпадение) из всех динамических списков, нажмите **Удалить из этих списков**.
     - Если из одного списка — нажмите в строке с названием списка.

12.9. Экспорт данных глобального списка

Вы можете сохранить IP-адреса, содержащиеся в глобальном списке, в текстовый файл.

- Чтобы сохранить IP-адреса глобального списка,

  в строке с названием списка нажмите .

  Браузер сохранит текстовый файл `<Название глобального списка>.txt` в папке загрузки.

12.10. Настройка пользовательского правила с использованием глобального списка

- Чтобы настроить пользовательское правило с использованием глобального списка:

  1. Создайте правило (см. раздел 10.9) или выберите созданное ранее.
  2. В главном меню выберите **Схема конфигурации**.

     Откроется страница **Схема конфигурации**.
  3. В раскрывающемся блоке **Набор пользовательских правил** нажмите .

     Откроется карточка со списком пользовательских правил.
  4. В строке правила нажмите .

     Откроется карточка правила.
  5. В блоке **Параметры** нажмите **Добавить параметр**.
  6. Введите название пользовательского параметра.
  7. В поле **Отображаемое название** введите название параметра, которое будет отображаться в записях об обнаруженных событиях безопасности.
  8. Выберите тип данных **Списки CIDR**.
  9. Выберите значение по умолчанию — глобальный список, который будет использоваться для работы правила.
  10. Введите код правила, используя синтаксис языка пользовательских правил (см. приложение Б).
  11. Выберите действия с трафиком, которые необходимо выполнить PT AF в результате срабатывания правила.
  12. Сохраните изменения.

  Пользовательское правило с использованием глобального списка настроено. После этого вам необходимо включить правило и подключить набор пользовательских правил к пользовательскому шаблону.

12.11. Настройка исключений с использованием глобального списка

Вы можете задать условия для отмены проверки правилом с использованием глобального списка. Условия запуска проверки позволяют исключить ложные срабатывания. Если условия исключения выполнены, проверка не запускается.

- Чтобы настроить исключение из правила с использованием глобального списка:

  1. В главном меню выберите **Схема конфигурации**.

     Откроется страница **Схема конфигурации**.

  2. В раскрывающемся блоке **Веб-приложения** в строке защищаемого веб-приложения нажмите .

     Откроется список правил политики безопасности веб-приложения.

  3. В строке правила нажмите .

     Откроется карточка правила.

  4. Нажмите .

     Откроется конструктор исключений для запуска правила.

  5. Нажмите **Добавить группу условий**.

     В конструкторе будет добавлена группа условий отмены проверки.

  6. Нажмите **Добавить условие**.

  7. В раскрывающемся списке параметров выберите **IP-адрес**.

  8. Выберите действие **входит в список**.

  9. В раскрывающемся списке выберите глобальный список для настройки исключения.

  10. Нажмите **Сохранить**.

  Исключение ложных срабатываний для правила настроено.

См. также

Создание правила и добавление его в пользовательский набор (см. раздел 10.9)

Справочник по языку пользовательских правил (см. приложение Б)

13. Работа с событиями безопасности

PT AF может регистрировать события безопасности в базе данных. Записи о зарегистрированных событиях отображаются в таблице на дашборде **События безопасности**. В таблице указаны основные параметры событий. Количество отображаемых параметров зависит от размеров вашего экрана.

Ниже приведен полный список параметров событий, отображаемый в карточке события на вкладке детальной информации.

Таблица 15. Параметры события безопасности

Блок параметров	Параметр	Описание
Общие сведения и **Подробности**	Описание	Подробное описание события безопасности
	Правило	Название правила политики безопасности веб-приложения, позволившее зарегистрировать событие безопасности
	Веб-приложение	Название атакуемого веб-приложения
	Узел	Доменное имя защищаемого приложения
	URI	URI запроса
	Дата	Дата и время регистрации события безопасности, отображаемые в локальном часовом поясе
	Действия	Список действий, примененных к запросу по результатам срабатывания правила
	Уровень опасности	Уровень опасности события безопасности: — **Высокий**. Атаки такого уровня могут свидетельствовать о нарушении информационной безопасности и проникновении злоумышленника в защищаемое веб-приложение. Атаки высокого уровня опасности обозначаются красным цветом. — **Средний**. Атаки такого уровня могут свидетельствовать о нарушении информационной безопасности и являться признаком того, что злоумышленник проводит подготовительные действия для проникновения в защищаемое веб-приложение. Например, к таким атакам относится несанкционированное получение конфигурации веб-приложения. Атаки среднего уровня опасности обозначаются желтым цветом.

Блок параметров	Параметр	Описание
		— **Низкий**. Атаки такого уровня опасности свидетельствуют о нарушении информационной безопасности защищаемого веб-приложения и могут являться признаком того, что злоумышленник пытается получить начальный доступ к защищаемому веб-приложению. Например, к таким атакам относится внедрение в запрос произвольного SQL-кода. Атаки низкого уровня опасности обозначаются голубым цветом. — **Нет** (информационный). События такого уровня информируют о нормальной работе веб-приложения и не являются признаком нарушения информационной безопасности. Например, к таким событиям относится запрос на прохождение аутентификации. События информационного уровня опасности обозначаются серым цветом
	Точность	Точность определения атаки правилом, основанная на оценке экспертов Positive Technologies. Возможные значения: от 1 до 10. Оценка 10 означает, что правило не допускает ложных срабатываний
	Тип	Тип события безопасности. Возможные значения: — **Атака**; — **Инфо**; — **Уязвимость**
	Классификация	Уязвимость CVE, группа или класс атаки в базах знаний Securelist, MITRE ATT&CK и других
	Теги	Метка атаки, представляющая собой ключевые слова для поиска информации об атаке. Каждой новой записи об атаке автоматически присваивается метка при наступлении события, определенного в правиле, и выполнении условий, заданных в правиле
	Фаза	Фаза, на которой выполнилось правило (например, **На ответе**, **На запросе**)
	Время обработки	Время обработки запроса системой PT AF, указанное в секундах
	Ревизия	Версия правила, позволившего обнаружить атаку.

Блок параметров	Параметр	Описание
		Примечание. База знаний в PT AF постоянно обновляется. Чтобы предоставить более полную информацию о событии безопасности, PT AF фиксирует версию правила, позволившего зарегистрировать событие безопасности
	IP-адрес	IP-адрес атакующего
	Транзакция	Идентификатор HTTP-транзакции (запроса и ответа), который необходим для поиска атак в пределах одной HTTP-транзакции
	Событие безопасности	Название события безопасности
	ID события безопасности	Идентификатор записи о событии безопасности в базе PT AF
	ID правила	Идентификатор правила политики безопасности веб-приложения
Совпадение	Имя	Имя переменной, на которой сработало правило
	Значение	Значение переменной, на которой сработало правило
	Описание	Описание параметра, на основании которого зарегистрировано событие безопасности
	Ключ	Ключ переменной, на которой сработало правило
Сервер	IP-адрес	IP-адрес, на котором система PT AF принимала запрос
	Имя узла	Имя узла кластера PT AF, на который поступил запрос
	Порт	Номер порта, на который поступил запрос на PT AF
	Веб-приложение	Название атакуемого веб-приложения
Клиент	Браузер	Название браузера атакующего
	Версия браузера	Версия браузера атакующего
	Город	Название города, из которого ведется предполагаемая атака. Город указан только в том случае, если его удалось определить по базе GeoIP2
	Тип аутентификации клиента	Тип аутентификации атакующего
	Имя клиента	Имя учетной записи атакующего, если определено

Блок параметров	Параметр	Описание
	Страна	Название страны атакующего, если ее удалось определить по базе GeoIP2
	Координаты	Координаты, определенные по IP-адресу
	IP-адрес	IP-адрес атакующего и флаг страны, если ее удалось определить по базе GeoIP2
	Регион	Название региона атакующего
	ОС	Семейство операционной системы атакующего
Запрос	Протокол	Протокол передачи данных (HTTP или HTTPS)
	Метод	HTTP-метод
	Размер	Размер запроса, в байтах
	URL	Относительный адрес ресурса, на который отправлялся запрос
	Аргументы запроса	Куки, GET-параметры, заголовки HTTP-запроса, POST-параметры
Ответ	Код ответа	HTTP-код ответа
	Размер ответа	Размер ответа, в байтах
	Заголовки ответа	Заголовки ответа

В этом разделе

Работа со списком событий безопасности (см. раздел 13.1)

Фильтрация событий безопасности (см. раздел 13.2)

Работа с личными фильтрами (см. раздел 13.3)

Просмотр карточки события безопасности (см. раздел 13.4)

Запись информации о событии безопасности в БД системы (см. раздел 13.5)

Работа с отчетами о событиях безопасности (см. раздел 13.6)

13.1. Работа со списком событий безопасности

На странице **События безопасности** вы можете настраивать отображение списка событий безопасности, а также просматривать статистику по событиям.

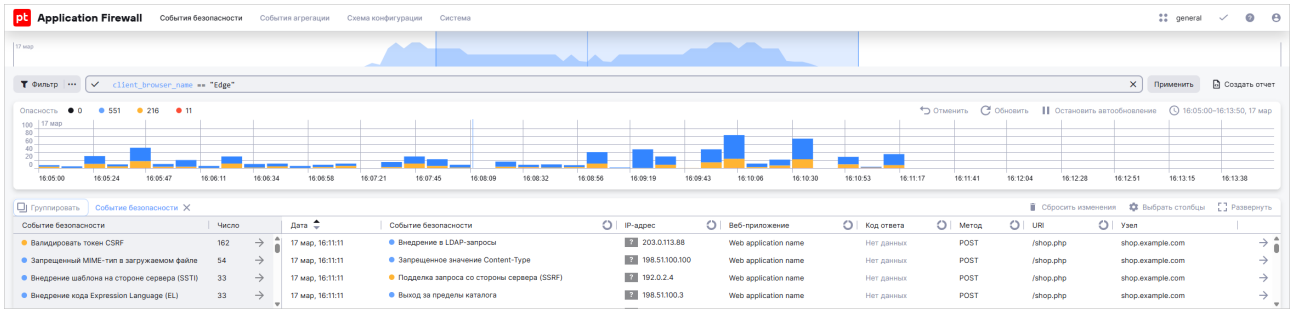


Рисунок 12. Таблица событий безопасности

Вы можете управлять списком событий безопасности следующими способами:

— группировка событий безопасности. Для группировки событий безопасности по определенным критериям необходимо их выбрать, а затем в таблице критериев в строке с набором нужных значений нажать .

/ — сортировка событий безопасности по значению параметра. Одно нажатие — сортировка по возрастанию, два нажатия — сортировка по убыванию, три нажатия — отмена сортировки.

— обновление списка событий безопасности. Список обновляется автоматически раз в 10 секунд. Для остановки обновления необходимо нажать .

— увеличение размера таблицы. Для возврата размера таблицы по умолчанию нужно нажать .

— изменение списка параметров, отображающихся в таблице событий безопасности.

— статистика по параметру. Показывает пять наиболее частых значений параметра и количество событий безопасности, имеющих такие значения.

13.2. Фильтрация событий безопасности

На странице **События безопасности** вы можете фильтровать события на основе одного или нескольких критериев различными способами.

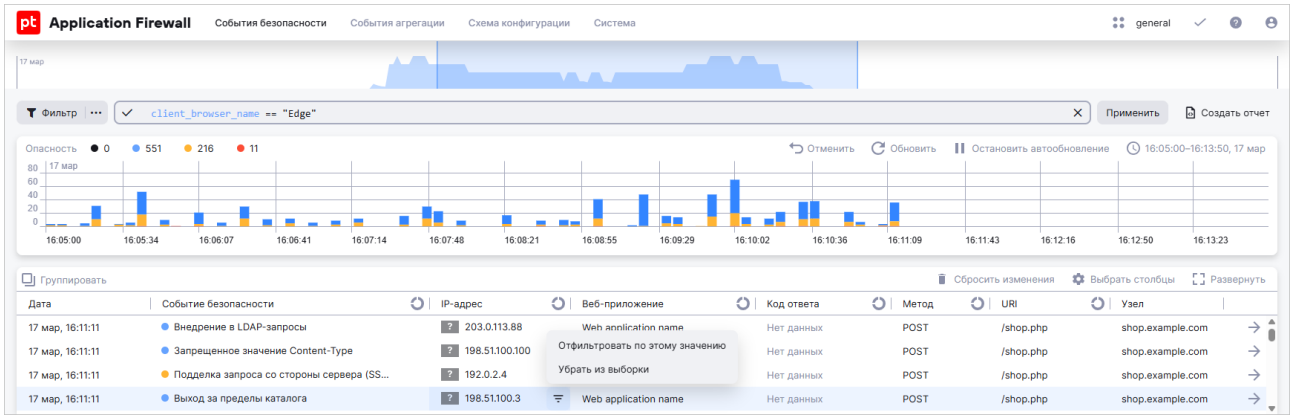


Рисунок 13. Фильтрация событий безопасности

Способы фильтрации событий безопасности:

— **Фильтрация по значениям параметров.** В строку фильтрации введите условие на языке фильтрации (см. приложение Г). Кроме того, вы можете использовать сохраненный ранее личный фильтр (см. раздел 13.3).

  Примечание. Вы можете просмотреть полный список параметров, используемых в условиях фильтрации, нажав Ctrl+Space в строке фильтрации. Чтобы сбросить условия, в строке фильтрации нажмите ✕.

— **Фильтрация по времени.** Необходимо нажать и выбрать период фильтрации либо выделить необходимый период на диаграмме интенсивности трафика (см. раздел 7.2) или на диаграмме событий безопасности (см. раздел 7.2).

— **Фильтрация по уровню опасности событий.** Осуществляется по нажатию на индикатор, соответствующий уровню опасности.

— **Быстрая фильтрация.** В таблице событий нужно навести курсор на значение параметра, нажать и выбрать, включить ли значение в выборку. Для быстрой фильтрации из карточки события (см. раздел 13.4) необходимо нажать на строку параметра и выбрать, включить ли его значение в выборку.

  Примечание. Параметры, для которых доступна быстрая фильтрация, помечены значком , который отображается при наведении курсора на строку параметра.

13.3. Работа с личными фильтрами

Вы можете сохранять условия фильтрации для дальнейшего использования. Сохраненные фильтры доступны только вам, другие пользователи не могут их просматривать, изменять или удалять.

Вы можете работать с личными фильтрами на странице **События безопасности** в панели фильтрации.

Создание личного фильтра

Вы можете создать личный фильтр с нуля или на основе другого ранее созданного личного фильтра.

- Чтобы создать личный фильтр с нуля:
  1. Введите условие фильтрации.
  2. Нажмите ••• → **Сохранить**.
  3. Введите название личного фильтра.
  4. Нажмите **Сохранить**.
- Чтобы создать личный фильтр на основе другого фильтра:
  1. Нажмите и выберите фильтр в списке.

     Условия фильтра будут добавлены в строку фильтрации.
  2. Измените условия фильтрации.
  3. Нажмите ••• → **Сохранить как новый**.
  4. Введите название личного фильтра.
  5. Нажмите **Сохранить**.

Изменение личного фильтра

- Чтобы изменить личный фильтр:
  1. Нажмите и выберите фильтр в списке.

     Условия фильтра будут добавлены в строку фильтрации.
  2. Измените условия фильтрации.
  3. Нажмите ••• → **Сохранить изменения**.

Переименование личного фильтра

- Чтобы переименовать личный фильтр:
  1. Нажмите и выберите фильтр в списке.
  2. Нажмите ••• → **Переименовать**.
  3. Измените название фильтра.
  4. Нажмите **Сохранить**.

Удаление личного фильтра

- Чтобы удалить личный фильтр:

  1. Нажмите и выберите фильтр в списке.
  2. Нажмите → **Удалить**.

13.4. Просмотр карточки события безопасности

Вы можете просмотреть подробную информацию о событии, открыв его карточку на странице **События безопасности**.

В этом разделе

Просмотр информации о событии безопасности (см. раздел 13.4.1)

Просмотр данных запроса и ответа в необработанном виде (см. раздел 13.4.2)

13.4.1. Просмотр информации о событии безопасности

- Чтобы просмотреть информацию о событии безопасности:

  1. В таблице событий нажмите на строку события или .

     Примечание. Для совместной работы с таблицей событий и карточкой события вы можете закрепить карточку по кнопке .

  2. Если требуется просмотреть подробную информацию о событии, нажмите .

     Примечание. В значении параметра **Действия** отображается список действий, которые были выполнены при срабатывании правила в рамках просматриваемого события безопасности.

13.4.2. Просмотр данных запроса и ответа в необработанном виде

Для расследования событий безопасности могут потребоваться данные запросов и ответов в необработанном виде (до их нормализации в PT AF). Вы можете просмотреть эти данные в карточке события безопасности.

- Чтобы просмотреть данные в необработанном виде:

  1. В таблице событий нажмите на строку события или .
  2. Нажмите .

В карточке события отобразятся данные запроса и ответа (при их наличии) в необработанном виде.

Примечание. Максимальный объем отображаемых данных — не более 100 КБ. Для отображения используется кодировка ASCII, последовательность символов `\r\n` и символ `\n` отображаются как перенос строки. Вы можете включать и отключать переносы строк по кнопке .

Примечание. По умолчанию nginx игнорирует заголовки с недопустимыми названиями[17], поэтому они не отображаются в данных запроса. Для отображения таких заголовков нужно изменить значение директивы nginx — `ignore_invalid_headers off`.

3. Если запрос (или ответ) был подвергнут сжатию и его нужно декодировать, включите функцию декодирования.
4. Если нужно сохранить все необработанные данные запроса (или ответа), нажмите .

   Браузер сохранит файл с данными в папку по умолчанию.
5. Если нужно скопировать все необработанные данные запроса (или ответа), нажмите .

Необработанные данные в PT AF хранятся отдельно от событий безопасности. Максимальный размер файла с необработанными данными для каждого запроса — 1 МБ, для ответа — 2 МБ. Общий размер данных запроса и ответа не может превышать 2 МБ. При переполнении раздела с необработанными данными старые данные будут удалены.

13.5. Запись информации о событии безопасности в БД системы

Когда PT AF регистрирует событие, связанное с отправкой одного запроса от клиента к серверу, может оказаться, что событию соответствует несколько разных типов событий, которые система PT AF обнаруживает, используя разные правила обработки трафика. Если в правиле применено действие с типом **Записывать событие в базу данных**, то PT AF запишет информацию об обнаруженном событии безопасности в базу данных. Записи отображаются на странице **События безопасности**. Для каждого события добавляется один или несколько тегов, поясняющих суть произошедшего.

По умолчанию во всех правилах, кроме правил группы **Предварительная обработка**, применено системное действие **Log to db** с типом **Записывать событие в базу данных**. Это действие позволяет сохранять необработанные данные события безопасности и маскировать значения полейс названиями: `api`, `token`, `key`, `secret`, `private`, `pass`, `password`, `authorization`, `access_token`, `private_token`, `private-token`. При необходимости вы можете создать пользовательское действие с типом **Записывать событие в базу данных** и применить его в правиле вместо системного.

17 Допустимы латинские буквы, цифры, дефис, а также в зависимости от значения директивы `underscores_in_headers` — знак подчеркивания.

Примечание. Пользовательское действие с типом **Записывать событие в базу данных** не будет срабатывать, если оно добавлено в правила, связанные с предварительной обработкой запросов (**Предварительно декодировать параметры HTTP**, **Нормализовать параметры**, **Не проверять статические ресурсы**).

Включить запись информации о событии безопасности с помощью пользовательского действия можно в разделе **Схема конфигурации** → **Действия**.

► Чтобы включить запись информации о событии безопасности при срабатывании правила:

1. В поле **Название** укажите название действия (максимальная длина — 64 символа; допустимо использование букв русского и латинского алфавита, а также спецсимволов).
2. Выберите тип **Записывать событие в базу данных**.
3. Если для расследования события безопасности вам могут потребоваться необработанные данные, включите функцию **Сохранять необработанные данные**.
4. Если необходимо маскировать совпавшие переменные в событии безопасности, включите функцию **Маскировать совпавшие переменные**.
5. Если требуется маскировать какое-либо поле, нажмите кнопку **Добавить** и в пустое поле введите название маскируемого поля.

   Примечание. Названия полей для маскирования проверяются без учета регистра. Например, если вам нужно маскировать поля `token`, `Token` и `TOKEN`, достаточно добавить в список только значение `token`.
6. Укажите значение, на которое будут заменяться данные при маскировании.
7. Если требуется, измените значение в поле **Максимальная длина совпавшего параметра**.
8. Нажмите **Создать**.
9. Откройте карточку правила (см. раздел 10.5), в поле **Действия при срабатывании** выберите созданное действие и нажмите **Сохранить**.

При срабатывании правила, к которому применено созданное действие, в базу данных будет записана информация о событии безопасности.

13.6. Работа с отчетами о событиях безопасности

Вы можете создавать отчеты о событиях безопасности в форматах PDF и CSV. Отчет формируется на странице **События безопасности** с учетом указанных на ней условий фильтрации. Отчет в формате PDF содержит распределение событий безопасности за выбранный период по времени (события с уровнем опасности «Нет» не отображаются на диаграммах) и по IP-адресам (показывается топ-10 IP-адресов, с которых осуществляются атаки). Отчет в формате CSV содержит подробную информацию о событиях в виде таблицы.

Создание отчета

- Чтобы создать отчет о событиях безопасности,

  на странице **События безопасности** нажмите **Создать отчет** и в раскрывшемся списке выберите формат отчета.

  Начнется создание отчета (это может занять несколько минут). Информация об отчете отобразится на странице **Система** → **Отчеты**.

Скачивание и удаление отчетов

Вы можете скачивать и удалять отчеты на странице **Система** → **Отчеты**.

- Чтобы скачать отчет,

  в строке отчета нажмите  .

  Браузер сохранит файл с отчетом в папку по умолчанию.

- Чтобы удалить отчет,

  в строке отчета нажмите  и подтвердите удаление.

14. Работа с событиями агрегации

Агрегация — объединение единичных событий безопасности, зарегистрированных одним правилом для одного IP-адреса в рамках веб-приложения. В результате агрегации система регистрирует событие агрегации и добавляет IP-адрес в динамический список, который может быть использован для обработки трафика (например, для блокировки IP-адресов).

По умолчанию агрегация включена для следующих правил:

- **User-Agent бота** — обнаруживает использование ботов;
- **Сканер уязвимостей** — обнаруживает активность сканера уязвимостей;
- **Чтение глобальной адресной книги (GAB) в Skype for Business** — обнаруживает попытки получения доступа к глобальной адресной книге в Skype for Business.

В этом разделе

О событиях агрегации (см. раздел 14.1)

Работа со списком событий агрегации (см. раздел 14.2)

Фильтрация событий агрегации (см. раздел 14.3)

Просмотр карточки события агрегации (см. раздел 14.4)

Настройка агрегации (см. раздел 14.5)

14.1. О событиях агрегации

Записи о зарегистрированных событиях отображаются в таблице на странице **События агрегации**. В таблице указаны основные параметры событий. Количество отображаемых параметров зависит от размеров вашего экрана. Вы также можете просмотреть подробную информацию о событии и разблокировать IP-адрес клиента из события агрегации в карточке события.

Таблица 16. Параметры события агрегации

Параметр	Описание
Дата начала	Дата возникновения первого вошедшего в событие агрегации события безопасности
Дата окончания	Дата возникновения последнего вошедшего в событие агрегации события безопасности
Правило	Название правила, срабатывания которого привели к созданию события агрегации
Срабатываний	Количество срабатываний правила, вошедших в событие агрегации

Параметр	Описание
Продолжительность	Время, за которое фактически было собрано событие агрегации
IP-адрес	IP-адрес отправителя запросов, вызвавших срабатывания правила и сборку события агрегации
Окончание блокировки	Дата, до которой IP-адрес отправителя будет находиться в черном списке
Блокирующее правило	Правило, осуществляющее фактическую блокировку адресов, находящихся в списке заблокированных
Веб-приложение	Название веб-приложения, в рамках которого создано событие агрегации

14.2. Работа со списком событий агрегации

На странице **События агрегации** вы можете управлять списком событий агрегации: группировать, сортировать, а также вручную обновлять список событий.

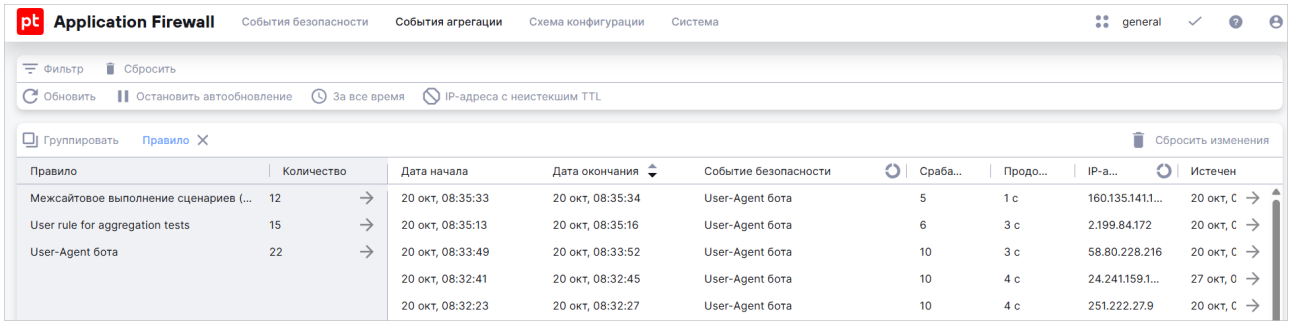


Рисунок 14. Таблица событий агрегации

— группировка событий агрегации. Для группировки необходимо выбрать критерии, а затем в таблице критериев в строке с набором нужных значений нажать .

/ — сортировка событий агрегации по значению параметра. Одно нажатие — сортировка по возрастанию, два нажатия — сортировка по убыванию, три нажатия — отмена сортировки.

— обновление списка событий агрегации. Список обновляется автоматически раз в 10 секунд. Для остановки обновления необходимо нажать .

— статистика по параметру. Показывает пять наиболее частых значений параметра и количество событий агрегации, имеющих такие значения.

14.3. Фильтрация событий агрегации

На странице **События агрегации** вы можете фильтровать события на основе одного или нескольких критериев различными способами.

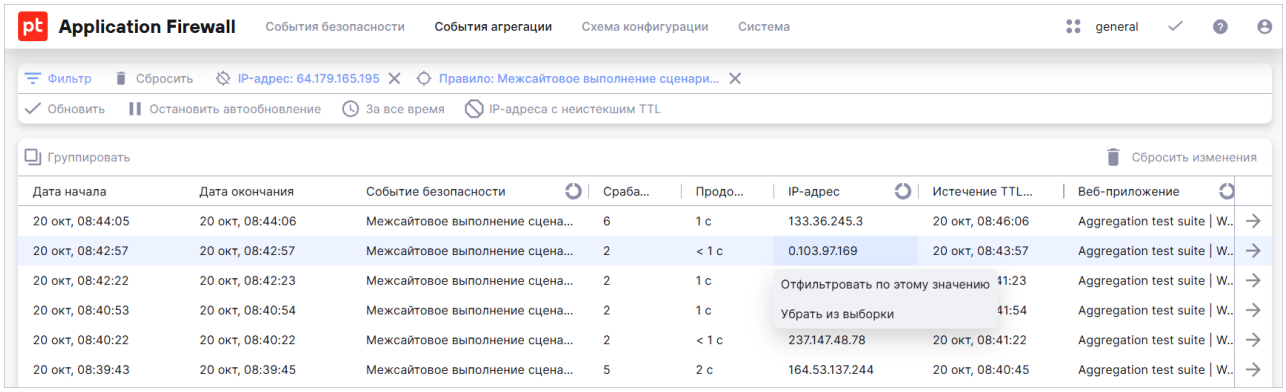


Рисунок 15. Фильтрация событий агрегации

Способы фильтрации событий агрегации:

- **Фильтрация по значениям параметров.** Необходимо нажать , выбрать параметры событий агрегации и ввести их значения. Для исключения параметра из фильтрации нужно нажать .
- **Фильтрация по IP-адресам с неистекшим TTL.** Необходимо нажать . В списке отобразятся только события агрегации, связанные с IP-адресами с неистекшим временем жизни.
- **Фильтрация по времени.** Необходимо нажать и выбрать период фильтрации.
- **Быстрая фильтрация.** В таблице событий агрегации нужно нажать на значение параметра и выбрать, включить ли его в выборку.

  Примечание. Выполнить быструю фильтрацию можно по значениям параметров **Событие безопасности**, **IP-адрес** и **Веб-приложение**.

- Чтобы сбросить фильтрацию по одному параметру,

  в строке фильтрации нажмите рядом с этим параметром.

- Чтобы сбросить все фильтры,

  нажмите **Сбросить**.

14.4. Просмотр карточки события агрегации

- Чтобы просмотреть карточку события агрегации:

  1. Выберите вкладку **События агрегации**.

     На экране отобразится таблица со всеми событиями агрегации, зарегистрированными в системе.

  2. В строке с событием агрегации, в карточку которого нужно перейти, нажмите →.

     Откроется карточка события агрегации.

  3. Если требуется посмотреть список событий безопасности, сформировавших агрегацию, нажмите **Посмотреть цепочку событий**.

     Откроется страница с таблицей событий безопасности, объединенных в событие агрегации.

     Примечание. Время для событий безопасности хранится с точностью до миллисекунд, а для событий агрегации — до секунд. Из-за этого при фильтрации в выборку могут попасть более поздние события безопасности, произошедшие в ту же секунду, что и последнее событие в агрегации.

  4. Если требуется разблокировать IP-адрес, соответствующий событию агрегации, нажмите **Разблокировать**.

     Примечание. Кнопка **Разблокировать** отображается на карточке, если время блокировки IP-адреса не истекло.

     IP-адрес исключается из списка блокировки для соответствующего приложения.

14.5. Настройка агрегации

- Чтобы настроить агрегацию:

  1. Откройте карточку правила:

     - Если необходимо настроить агрегацию в правиле шаблона, на странице **Схема конфигурации** в раскрывающемся блоке **Шаблоны политик безопасности** в строке с названием шаблона нажмите →.
     - Если необходимо настроить агрегацию в правиле веб-приложения, в раскрывающемся блоке **Веб-приложения** в строке с названием веб-приложения нажмите .

  2. В строке с названием правила нажмите →.

  3. Если в раскрывающемся списке **Действия при срабатывании** не выбрано действие с типом **Записывать событие в базу данных**, выберите это действие.

  4. В карточке правила нажмите .

5. Включите агрегацию.
6. Если необходимо, измените временные параметры агрегации.
7. В раскрывающемся списке **Глобальный динамический список** выберите динамический список для добавления IP-адресов.

   Примечание. Также вы можете создать динамический список по кнопке **Добавить** в раскрывающемся списке.
8. Нажмите **Применить**.

15. Администрирование PT AF

В этом разделе содержатся инструкции по администрированию PT AF.

В этом разделе

Управление учетными записями (см. раздел 15.1)

Смена своего пароля (см. раздел 15.2)

Настройка LDAP-подключений (см. раздел 15.3)

Настройка OAuth-подключений (см. раздел 15.4)

Управление ролями (см. раздел 15.5)

Управление изолированными пространствами (см. раздел 15.6)

Тонкая настройка обработки трафика в изолированных пространствах (см. раздел 15.7)

Управление ICAP-серверами (см. раздел 15.8)

Управление кластером Kubernetes (см. раздел 15.9)

Мониторинг состояния PT AF (см. раздел 15.10)

Установка доверенного сертификата для веб-интерфейса PT AF (см. раздел 15.11)

Обновление базы знаний (см. раздел 15.12)

Работа с лицензией (см. раздел 15.13)

Об архивации журнала событий (см. раздел 15.14)

Настройка взаимной TLS-аутентификации клиента с агентом PT AF (см. раздел 15.15)

Настройка отправки сообщений о событиях аудита на удаленный syslog-сервер (см. раздел 15.16)

Резервное копирование и восстановление данных PT AF (см. раздел 15.17)

Экспорт и импорт параметров защиты приложений (см. раздел 15.18)

Синхронизация объектов между экземплярами PT AF (см. раздел 15.19)

Настройка декодирования запросов и ответов (см. раздел 15.20)

Тонкая настройка применения конфигурации (см. раздел 15.21)

Настройка журналирования работы агента (см. раздел 15.22)

Настройка отправки данных из журналов access.log и error.log во внешние SIEM-системы (см. раздел 15.23)

Отправка событий от агентов в SIEM-системы (см. раздел 15.24)

Обновление базы GeoIP для агента (см. раздел 15.25)

Изменение списка NTP-серверов (см. раздел 15.26)

Скрытие информации о версии nginx из сообщения об ошибке (см. раздел 15.27)

15.1. Управление учетными записями

В зависимости от типа аутентификации пользователей в PT AF предусмотрены три типа учетных записей: локальные, доменные и учетные записи, созданные в результате входа в PT AF с помощью OAuth-подключения.

Локальные учетные записи в общем случае используются для работы в определенном изолированном пространстве (см. раздел 15.6). Вместе с тем вы можете пригласить пользователя одного изолированного пространства в другое. Локальные учетные записи создаются, изменяются и удаляются вручную.

Доменные учетные записи добавляются в PT AF автоматически после создания LDAP-подключения (см. раздел 15.3.1) и предоставления прав доступа (см. раздел 15.3.4). Вы не можете добавлять, изменять или удалять доменные учетные записи вручную. В PT AF доступен только просмотр их параметров.

При первом успешном входе пользователя в PT AF с помощью OAuth-подключения создается новая учетная запись. При создании учетной записи ей назначается роль, указанная в параметрах OAuth-подключения (см. раздел 15.4). Вы не можете добавлять и удалять такие учетные записи вручную. Учетные записи, связанные с OAuth-подключением, удаляются только при удалении этого OAuth-подключения.

При развертывании PT AF автоматически создается учетная запись администратора (логин — `admin`, пароль — `positive`), имеющая все возможные привилегии (см. раздел 15.5). Эту учетную запись невозможно заблокировать. При первом входе нужно сменить пароль учетной записи администратора на более сложный.

Вы можете управлять учетными записями на странице **Система** → **Пользователи**.

В этом разделе

Создание локальной учетной записи (см. раздел 15.1.1)

Приглашение пользователя другого изолированного пространства (см. раздел 15.1.2)

Изменение локальной учетной записи (см. раздел 15.1.3)

Удаление локальной учетной записи (см. раздел 15.1.4)

Настройка параметров безопасности учетных записей (см. раздел 15.1.5)

15.1.1. Создание локальной учетной записи

Изолированное пространство, в котором создается учетная запись пользователя, является домашним изолированным пространством для этого пользователя.

- Чтобы создать локальную учетную запись:

  1. В таблице учетных записей нажмите +.
  2. Введите логин.

     Примечание. Логин должен быть уникальным и может содержать только латинские буквы, цифры и специальные символы. В качестве логина можно указать адрес электронной почты.
  3. Введите адрес электронной почты пользователя.
  4. Введите и подтвердите пароль.

     Примечание. Пароль должен отвечать требованиям парольной политики (см. раздел 15.1.5).
  5. Выберите роль пользователя.

     Примечание. Если в списке нет нужной роли, вы можете создать ее (см. раздел 15.5.1) по кнопке **Добавить**.
  6. Если после первого входа в PT AF пользователю нужно сменить пароль, включите принудительную смену пароля.
  7. Если требуется, включите признак сервисной учетной записи.

     Примечание. Сервисные учетные записи не блокируются, если не был изменен временный пароль и при превышении пороговых значений параметров безопасности (см. раздел 15.1.5): времени жизни неактивной учетной записи и максимального количества неуспешных попыток входа. Учетные записи администраторов изолированных пространств по умолчанию являются сервисными.
  8. Нажмите **Добавить пользователя**.

15.1.2. Приглашение пользователя другого изолированного пространства

Вы можете пригласить пользователей, учетные записи которых были созданы в других изолированных пространствах, в свое изолированное пространство.

- Чтобы пригласить пользователя:

  1. В таблице учетных записей нажмите +.
  2. Нажмите .
  3. Введите логин.
  4. Выберите роль приглашаемого пользователя в своем изолированном пространстве.

Примечание. Если в списке нет нужной роли, вы можете создать ее (см. раздел 15.5.1) по кнопке **Добавить**.

5. Нажмите кнопку **Пригласить пользователя**.

Учетная запись приглашенного пользователя появится в таблице учетных записей. В строке с параметрами учетной записи приглашенного пользователя отобразится значок .

После приглашения пользователь может переключаться между изолированными пространствами в главном меню (см. раздел 7.1) по кнопке .

15.1.3. Изменение локальной учетной записи

- Чтобы изменить локальную учетную запись:

1. В строке с параметрами учетной записи нажмите .
2. Внесите изменения.
3. Нажмите **Сохранить**.

15.1.4. Удаление локальной учетной записи

Если учетная запись удаляется из изолированного пространства, в которое пользователь был приглашен, она не будет удалена из остальных изолированных пространств. Если учетная запись удаляется из домашнего изолированного пространства, она будет удалена из всех изолированных пространств.

Примечание. Вы не можете удалить учетную запись администратора изолированного пространства. Она удалится автоматически при удалении изолированного пространства.

- Чтобы удалить локальную учетную запись:

1. В строке с параметрами учетной записи нажмите .
2. Нажмите **Удалить** и подтвердите удаление.

15.1.5. Настройка параметров безопасности учетных записей

PT AF позволяет настраивать параметры безопасности учетных записей.

Параметры безопасностей учетных записей разделены на группы:

— **Парольная политика.** Требования к длине и составу пароля, а также время его жизни. Время жизни пароля — это срок действия пароля в днях с момента создания учетной записи или смены пароля пользователем или администратором системы. По истечении срока пользователю требуется сменить пароль для продолжения работы в PT AF.

Внимание! Парольная политика применяется только к локальным учетным записям. Пароли доменных учетных записей и сроки их действия настраиваются в Microsoft Active Directory.

Примечание. Пользователям не нужно менять пароль после изменения требований к длине и составу пароля.

- **Политика временной блокировки.** Требования к блокировке учетных записей на заданный период после заданного количества неуспешных попыток входа в PT AF.
- **Политика постоянной блокировки.** Требования к постоянной блокировке учетных записей с временным паролем, который не был изменен за заданный промежуток времени, и (или) учетных записей после заданного количества неуспешных попыток входа.

  Примечание. Если настроены временная и постоянная блокировка учетных записей при неуспешных попытках входа, сработает блокировка с меньшим количеством допустимых неуспешных попыток. При одинаковом количестве неуспешных попыток сработает постоянная блокировка.
- **Сессия.** Определяет время жизни сессии в часах. Время жизни сессии устанавливается для всех пользователей системы. По умолчанию сессия действует бессрочно.

  Внимание! Сессия может быть завершена до истечения времени ее жизни — если пользователь закрывает вкладку браузера, не установив флажок **Запомнить меня**, или в течение 15 минут бездействует.

► Чтобы настроить параметры безопасности учетных записей:

1. В главном меню выберите **Система**.
2. Выберите вкладку **Безопасность учетных записей**.
3. Настройте параметры безопасности учетных записей.

   Примечание. Блок параметров **Обязательные символы** позволяет сделать обязательным использование в пароле хотя бы одной цифры, заглавной латинской буквы, строчной латинской буквы и хотя бы одного специального символа из набора специальных символов.
4. Нажмите кнопку **Сохранить**.

15.2. Смена своего пароля

Смена пароля доступна только для локальных учетных записей.

► Чтобы сменить свой пароль:

1. В главном меню нажмите и в раскрывшемся меню выберите **Сменить пароль**.
2. Введите старый пароль.

3. Дважды введите новый пароль.
4. Нажмите **Сменить пароль**.

Ваш пароль изменен. Необходимо заново войти в PT AF на всех устройствах.

15.3. Настройка LDAP-подключений

Вы можете управлять LDAP-подключениями и правами доступа доменных пользователей на странице **Система** → **LDAP-подключения**.

Внимание! К доменным учетным записям не применяются требования парольной политики (см. раздел 15.1.5).

В этом разделе

Создание LDAP-подключения (см. раздел 15.3.1)

Изменение LDAP-подключения (см. раздел 15.3.2)

Удаление LDAP-подключения (см. раздел 15.3.3)

Настройка соответствия ролей PT AF и групп Microsoft Active Directory (см. раздел 15.3.4)

Изменение соответствия ролей PT AF и групп Microsoft Active Directory (см. раздел 15.3.5)

Удаление соответствия ролей PT AF и групп Microsoft Active Directory (см. раздел 15.3.6)

Запуск синхронизации с Microsoft Active Directory вручную (см. раздел 15.3.7)

15.3.1. Создание LDAP-подключения

Создание нового LDAP-подключения

- Чтобы создать LDAP-подключение:

1. В таблице LDAP-подключений нажмите +.
2. Введите название LDAP-подключения.
3. Введите IP-адрес или полное доменное имя LDAP-сервера.
4. Введите номер порта.
5. Если требуется, включите защищенное соединение с LDAP-сервером.
6. В поле **База поиска пользователей** введите имя записи каталога, начиная с которой выполняется поиск учетных записей пользователей.
7. В поле **Фильтр для поиска пользователей** введите условие для поиска.

Примечание. Не поддерживается постраничное получение результатов поиска. Для уменьшения количества получаемых записей уточняйте условия поиска (например, ищите пользователей по их группе).

8. Введите логин и пароль пользователя, который обладает правами на чтение объектов из каталога.
9. Если требуется, включите автоматическую синхронизацию пользователей и укажите ее интервал.
10. Введите названия атрибутов логина и электронной почты для поиска пользователей.
11. Нажмите **Создать**.

LDAP-подключение создано. Теперь нужно настроить права доступа (см. раздел 15.3.4) для доменных пользователей.

Создание LDAP-подключения на основе существующего

- Чтобы создать LDAP-подключение на основе существующего:

1. В строке с параметрами LDAP-подключения нажмите →.
2. Нажмите **Действия** → **Копировать**.

   Откроется окно создания LDAP-подключения. Поля будут заполнены значениями параметров LDAP-подключения, на основе которого создается новое LDAP-подключение.
3. Измените название LDAP-подключения и внесите другие необходимые изменения.

   Примечание. Название LDAP-подключения должно быть уникальным в рамках изолированного пространства.
4. Введите пароль пользователя, который обладает правами на чтение объектов из каталога.
5. Нажмите **Создать**.

15.3.2. Изменение LDAP-подключения

- Чтобы изменить LDAP-подключение:

1. В строке с параметрами LDAP-подключения нажмите →.
2. Внесите изменения.

3. Если требуется проверить LDAP-подключение после изменения, нажмите **Синхронизировать**.
4. Нажмите **Сохранить**.

LDAP-подключение изменено. Права доступа доменных пользователей обновятся согласно интервалу синхронизации.

15.3.3. Удаление LDAP-подключения

Удаление LDAP-подключения доступно только администраторам базового изолированного пространства `general`. LDAP-подключение удалится из всех изолированных пространств. Также удалятся ранее настроенные права доступа для доменных пользователей, связанных с этим LDAP-подключением. Вместе с тем сессии доменных пользователей останутся активными до истечения времени их жизни.

- Чтобы удалить LDAP-подключение:

1. В строке с параметрами LDAP-подключения нажмите →.
2. Нажмите **Удалить** и подтвердите удаление.

15.3.4. Настройка соответствия ролей PT AF и групп Microsoft Active Directory

Права доменных пользователей в изолированном пространстве определяются соответствием групп Microsoft Active Directory и ролей PT AF. Рекомендуется настраивать соответствия таким образом, чтобы каждому доменному пользователю были доступны только одно изолированное пространство и одна роль в нем.

В ином случае при первом входе в PT AF пользователь будет авторизован только в одном из доступных ему изолированных пространств согласно внутреннему алгоритму. Это изолированное пространство будет назначено как единственное доступное пространство для пользователя (пространство по умолчанию). Также согласно алгоритму из нескольких подходящих ролей пользователю будет назначена только одна роль.

- Чтобы настроить соответствие ролей и групп:

1. В таблице соответствий нажмите +.
2. Выберите LDAP-подключение к каталогу, с которым требуется настроить соответствие.
3. Введите название атрибута, который содержит список групп пользователя в каталоге.
4. Введите условие для фильтрации групп.

5. Выберите соответствующую группам роль.
6. Нажмите **Создать**.

Соответствие настроено. Права доступа доменных пользователей обновятся согласно интервалу синхронизации.

15.3.5. Изменение соответствия ролей PT AF и групп Microsoft Active Directory

- Чтобы изменить соответствие ролей и групп:

1. В строке соответствия нажмите →.
2. Внесите изменения.
3. Нажмите **Сохранить**.

Соответствие изменено. Права доступа доменных пользователей обновятся согласно интервалу синхронизации.

15.3.6. Удаление соответствия ролей PT AF и групп Microsoft Active Directory

Авторизация доменного пользователя после удаления соответствия зависит от наличия других настроенных соответствий для этого пользователя, а также от факта авторизации в PT AF до удаления соответствия.

Если для пользователя настроены другие соответствия, он сможет авторизоваться в том же изолированном пространстве с другой ролью или в другом пространстве согласно соответствию, выбранному внутренним алгоритмом (сменится пространство по умолчанию). Права доступа обновятся после синхронизации с Microsoft Active Directory (запланированной или запущенной вручную).

Если других соответствий нет и пользователь ранее был авторизован в PT AF, он сможет продолжить работать в PT AF с прежней ролью. Если других соответствий нет и пользователь ранее не авторизовывался в PT AF, он не сможет авторизоваться.

- Чтобы удалить соответствие ролей и групп:

1. В строке соответствия нажмите →.
2. Нажмите **Удалить** и подтвердите удаление.

15.3.7. Запуск синхронизации с Microsoft Active Directory вручную

Запуск синхронизации доступен только администраторам базового изолированного пространства `general`.

- Чтобы вручную запустить синхронизацию с Microsoft Active Directory:

  1. В строке с параметрами LDAP-подключения нажмите →.
  2. Нажмите **Синхронизировать**.

     В строке **Последняя синхронизация** отобразятся значок ◌ и ход выполнения синхронизации (в процентах).

15.4. Настройка OAuth-подключений

OAuth-подключения позволяют пользователям входить в PT AF с помощью внешних сервисов аутентификации. PT AF поддерживает работу с сервисами аутентификации по протоколу OAuth 2.0.

Вы можете управлять OAuth-подключениями на странице **Система** → **OAuth-подключения**.

Подготовка к настройке OAuth-подключений

Перед настройкой OAuth-подключений необходимо добавить переменную окружения, отвечающую за формирование URL для перенаправления на страницу веб-интерфейса PT AF при аутентификации с помощью внешнего сервиса.

- Чтобы подготовиться к настройке OAuth-подключений,

  задайте значение переменной окружения `FRONTEND_ADDRESS`:

  ```
  sudo kubectl -n ptaf-backend set env deployment ptaf-auth-mgr FRONTEND_ADDRESS='<адрес веб-интерфейса PT AF>'
  ```

  Примечание. Адрес веб-интерфейса PT AF необходимо задать в формате: `https://адрес_WebUI`.

Создание нового OAuth-подключения

Перед созданием OAuth-подключения в PT AF необходимо зарегистрировать ваш PT AF во внешнем сервисе аутентификации. Вы получите значения следующих параметров, необходимые для создания OAuth-подключения в PT AF:

— Идентификатор клиента — публичный идентификатора PT AF во внешнем сервисе аутентификации.

— Секрет PT AF — закрытый идентификатор для подключения PT AF к сервису аутентификации.

— URL конфигурации — URL внешнего сервиса, по которому доступно описание конфигурации для аутентификации в PT AF.

— Атрибуты логина и электронной почты — названия атрибутов логина и электронной почты пользователей во внешнем сервисе аутентификации.

► Чтобы создать OAuth-подключение:

1. В таблице OAuth-подключений нажмите +.
2. Введите название OAuth-подключения.
3. Активируйте OAuth-подключение.
4. Введите идентификатор клиента.
5. Введите секрет PT AF.
6. Введите URL конфигурации.
7. Выберите роль, которая будет назначена пользователю при создании учетной записи после первого успешного входа с помощью OAuth-подключения.
8. Добавьте SSL-сертификат.

   Примечание. Вы можете включить пропуск проверки SSL-сертификата.
9. Введите названия атрибутов логина и электронной почты для поиска пользователей.

   Примечание. При первом успешном входе пользователя в PT AF с помощью OAuth-подключения создается новая учетная запись с логином и адресом электронной почты из указанных атрибутов.
10. Нажмите **Добавить**.

OAuth-подключение создано. Пользователи могут входить (см. раздел 6) в PT AF с помощью этого OAuth-подключения.

Создание OAuth-подключения на основе существующего

► Чтобы создать OAuth-подключение на основе существующего:

1. В строке с параметрами OAuth-подключения нажмите →.
2. Нажмите **Действия** → **Копировать**.

   Откроется окно создания OAuth-подключения. Поля будут заполнены значениями параметров OAuth-подключения, на основе которого создается новое подключения.
3. Измените название OAuth-подключения и внесите другие необходимые изменения.

   Примечание. Название OAuth-подключения должно быть уникальным в рамках изолированного пространства.

4. Введите секрет PT AF.
5. Нажмите **Добавить**.

Изменение OAuth-подключения

- Чтобы изменить OAuth-подключение:

1. В строке с параметрами OAuth-подключения нажмите →.
2. Внесите изменения.
3. Нажмите **Сохранить**.

Удаление OAuth-подключения

- Чтобы удалить OAuth-подключение:

1. В строке с параметрами OAuth-подключения нажмите →.
2. Нажмите **Удалить** и подтвердите удаление.

15.5. Управление ролями

В PT AF реализована ролевая модель управления доступом. Роль содержит набор привилегий, которые определяют доступные для пользователя разделы интерфейса и операции.

В каждом изолированном пространстве можно создать собственный набор ролей. Эти роли можно назначать пользователям как своего пространства, так и других пространств (приглашенным пользователям). Создаваемые роли можно изменять и удалять.

По умолчанию система содержит стандартные роли `Administrator`, `Operator` и `Guest`. Эти роли невозможно изменить или удалить.

Вы можете управлять ролями на странице **Система** → **Роли**.

В этом разделе

Создание роли (см. раздел 15.5.1)

Изменение роли (см. раздел 15.5.2)

Удаление роли (см. раздел 15.5.3)

15.5.1. Создание роли

Создание новой роли

- Чтобы создать роль:

  1. В таблице ролей нажмите +.
  2. Введите название роли.
  3. Укажите привилегии для новой роли, нажимая на их значки.

     Примечание. По нажатию значок меняет свой цвет. В светлой теме значок выданной привилегии — черный, в темной теме — белый.

  4. Нажмите **Создать**.

Создание роли на основе существующей

- Чтобы создать роль на основе существующей:

  1. В строке с названием роли нажмите →.
  2. Нажмите **Копировать**.

     Откроется окно создания роли. Поля будут заполнены значениями параметров роли, на основе которого создается новая роль.

  3. Измените название роли и внесите другие необходимые изменения.

     Примечание. Название роли должно быть уникальным в рамках изолированного пространства.

  4. Нажмите **Создать**.

15.5.2. Изменение роли

- Чтобы изменить роль:

  1. В строке с названием роли нажмите →.
  2. Внесите изменения.
  3. Нажмите **Сохранить**.

15.5.3. Удаление роли

- Чтобы удалить роль:

  1. В строке с названием роли нажмите →.
  2. Нажмите **Удалить** и подтвердите удаление.

     Примечание. Если удаляемая роль уже назначена пользователям, в карточке роли отобразится их список. Чтобы удалить такую роль, нужно сначала выбрать другие роли для этих пользователей.

15.6. Управление изолированными пространствами

Изолированное пространство — это изолированная рабочая среда, доступная только тем пользователям, которые имеют в ней учетные записи. Изолированные пространства обеспечивают независимую работу разных групп пользователей в рамках одного экземпляра PT AF. Объекты изолированного пространства делятся на частные и общие. Частные объекты (например, события безопасности и веб-приложения) доступны только пользователям изолированного пространства. Общие объекты (например, стандартные действия и шаблоны политик безопасности) доступны всем пользователям PT AF.

При развертывании PT AF автоматически создается базовое изолированное пространство `general`. Только его администраторы могут создавать другие изолированные пространства, управлять лицензией, работать с резервными копиями и просматривать данные расширенного мониторинга PT AF (загруженность серверов и баз данных).

Трафик изолированного пространства может обрабатываться на узлах PT AF или на агенте. Если планируется обрабатывать трафик на узлах PT AF, при создании пространства потребуется выбрать зону доступности. Она определяет узлы кластера, на которых будет выполняться обработка. После создания пространства тип обработки трафика и зону доступности сменить невозможно.

Вы можете изменять количество и мощность подов, обрабатывающих трафик изолированного пространства. Поды с меньшей мощностью более эффективно используют ресурсы. Увеличение мощности позволяет избежать частого масштабирования и выделить больше ресурсов для анализа трафика.

Таблица 17. Мощность подов

Уровень вычислительной мощности пода	ОЗУ	Количество ЦП	Количество процесс-обработчиков	Количество обрабатываемых запросов в секунду[18]
Базовый	4 ГБ	1,5	1	300—750

18 Измерения производительности проводились в лабораторных условиях для различных аппаратных конфигураций PT AF.

Уровень вычислительной мощности пода	ОЗУ	Количество ЦП	Количество процесс-обработчиков	Количество обрабатываемых запросов в секунду[18]
Увеличенный	8 ГБ	2	2	600—1500
Максимальный	16 ГБ	4	4	1100—3000

Вы можете управлять изолированными пространствами на странице **Система** → **Изолированные пространства**.

В этом разделе

Создание изолированного пространства (см. раздел 15.6.1)

Изменение изолированного пространства (см. раздел 15.6.2)

Удаление изолированного пространства (см. раздел 15.6.3)

Особенности применения конфигурации в зависимости от количества подов (см. раздел 15.6.4)

Особенности обработки трафика на сервере Envoy (см. раздел 15.6.5)

Особенности обработки трафика на сервере nginx (см. раздел 15.6.6)

15.6.1. Создание изолированного пространства

При создании изолированного пространства также создается учетная запись его администратора.

► Чтобы создать изолированное пространство:

1. В таблице изолированных пространств нажмите +.
2. Введите название изолированного пространства.
3. Выберите, где будет обрабатываться трафик изолированного пространства: на узлах PT AF или на агенте.
4. Если обработка трафика будет выполняться на узлах PT AF:
   - Выберите зону доступности — группу узлов для обработки трафика веб-приложений создаваемого изолированного пространства.
   - Выберите тип сервера для обработки трафика: nginx или Envoy.

     Примечание. Обработка трафика на сервере Envoy имеет ряд особенностей (см. раздел 15.6.5).
   - Если необходимо, измените минимальное и максимальное количество подов (см. раздел 15.6.4) и их мощность.

     Примечание. Изменение мощности подов доступно только при выборе сервера nginx.

5. Введите логин и пароль администратора создаваемого изолированного пространства.

   Примечание. Логин администратора должен быть уникальным и может содержать только латинские буквы, цифры и специальные символы. В качестве логина можно указать адрес электронной почты. Пароль должен отвечать требованиям парольной политики (см. раздел 15.1.5).

6. Введите адрес электронной почты администратора.
7. Если после первого входа в PT AF администратору нужно сменить пароль, включите принудительную смену пароля.
8. Если необходимо предоставить доступ текущему пользователю к создаваемому изолированному пространству, включите функцию приглашения пользователя в изолированное пространство.

   Примечание. При включении функции приглашения пользователя в изолированное пространство ему будет назначена роль администратора этого изолированного пространства.

9. Нажмите **Создать**.

После создания изолированного пространства, трафик которого будет обрабатывать агент, формируется строка, которая потребуется для настройки агента после установки. Строка отображается в карточке изолированного пространства в поле **Строка для соединения с PT AF** и доступна только администратору пространства.

15.6.2. Изменение изолированного пространства

- Чтобы изменить изолированное пространство:

  1. В строке с названием изолированного пространства нажмите →.
  2. Внесите изменения.

     Примечание. Тип сервера для обработки трафика могут сменить только администраторы базового изолированного пространства `general`.

  3. Нажмите **Сохранить**.

15.6.3. Удаление изолированного пространства

- Чтобы удалить изолированное пространство:

  1. В строке с названием изолированного пространства нажмите →.
  2. Нажмите **Удалить** и подтвердите удаление.

15.6.4. Особенности применения конфигурации в зависимости от количества подов

С версии 4.3.0 при изменении параметров PT AF новая конфигурация по умолчанию применяется поэтапно, без прерывания трафика. Однако, при недостаточном минимальном количестве подов возможны небольшие потери трафика: запросы, поступившие в момент перезапуска единственного пода на узле, будут отброшены. Чтобы избежать потерь трафика, рекомендуется указывать следующие минимальные значения:

— Для статических подов — не менее двух подов на узел.

— Для динамических подов:

  - При отсутствии в изолированном пространстве профилей трафика с внешней балансировкой без контроля IP-адресов — не менее двух подов.
  - При наличии профилей трафика с внешней балансировкой без контроля IP-адресов — не менее `2×<Количество узлов-обработчиков>` подов.

15.6.5. Особенности обработки трафика на сервере Envoy

Обработка трафика на сервере Envoy имеет ряд особенностей:

— Доступна только базовая мощность для пода (1 процесс-обработчик).

— При смене типа сервера (с nginx на Envoy или наоборот) будет прерываться обработка трафика.

— Не поддерживаются NTLM-аутентификация, балансировка нагрузки между серверами по хеш-суммам IP-адресов, а также алгоритмы шифрования ГОСТ.

— Не поддерживается антивирусная проверка файлов с помощью сторонних ICAP-серверов.

— Не поддерживаются TLS-сертификаты без Subject Alternative Names (SAN) или Common Name (CN).

— Не поддерживается добавление и выбор сертификатов (см. раздел 8.2.4) удостоверяющего центра для проверки подлинности сертификатов приложения.

— Для обеспечения безопасной передачи данных между клиентом и PT AF поддерживается только одна стандартная конфигурация SSL (см. раздел 8.2.10). Недоступно создание собственных конфигураций SSL. При смене типа сервера с nginx на Envoy для всех приложений будет выбрана стандартная конфигурация.

— Если в профиле трафика для расширения SNI выбран вариант **Отправлять имя из запроса**, защищаемому серверу будет отправляться имя узла, указанное в заголовке `Host`.

— Перенаправление клиентских запросов на HTTPS-порт поддерживается только с одного HTTP-порта.

— Не поддерживается обработка трафика по протоколу HTTP 1.0.

— Не поддерживается механизм плавного завершения сессии (см. раздел 15.21.3).

— Не поддерживаются HTTP-заголовки, имена которых содержат символы в кодировке, отличной от ASCII. Соединения с такими заголовками автоматически разрываются на уровне протокола.

— При обработке запросов, пересылаемых частями (chunked-запросов), некоторые заголовки могут быть удалены сервером (в частности, `Transfer-Encoding`).

— Если для веб-приложения настроено получение реального IP-адреса клиента из HTTP-заголовка[19], возможно появление ошибок при больших нагрузках (когда под начинает потреблять 100 процентов ресурсов центрального процессора).

— Не срабатывает правило **Одинаковые заголовки в запросе** для заголовков `Accept`, `Accept-Encoding`, `Cache-Control`. Envoy объединяет эти заголовки в один, перечисляя значения через запятую, в результате чего запрос к приложению содержит только один заголовок данного типа.

— Не поддерживается управление HTTP-заголовками (см. раздел 8.2.8) путем создания действий с заголовками.

— Не поддерживается аутентификация клиентов в защищаемых приложениях по клиентским сертификатам и проверка сертификатов клиентов по спискам отозванных сертификатов (см. раздел 8.2.7.1).

15.6.6. Особенности обработки трафика на сервере nginx

При использовании сервера nginx по умолчанию действует ограничение в 1 ГБ для загрузки больших файлов. Вы можете увеличить это значение в рамках изолированного пространства с помощью утилиты traffic_setting.py (см. раздел 15.7) (параметр `core_nginx_client_max_body_size`).

> **Примечание.** Рекомендуем выносить в отдельные изолированные пространства веб-приложения, для которых характерна загрузка больших файлов, чтобы исключить их влияние на другие веб-приложения.

15.7. Тонкая настройка обработки трафика в изолированных пространствах

Внимание! Значения параметров по умолчанию являются оптимальными для стабильной работы PT AF и защищаемых приложений. Изменение значений параметров может привести к нарушению работы системы.

19 Доступно, когда перед PT AF находится внешний балансировщик или прокси-сервер.

Вы можете настроить параметры обработки трафика (см. раздел 15.7.3) отдельно для каждого изолированного пространства с помощью утилиты `traffic_settings.py`. Настройка повлияет на работу всех веб-приложений изолированного пространства. Если для работы веб-приложений нужны разные значения параметров, необходимо создавать веб-приложения в разных изолированных пространствах.

При использовании кластерной конфигурации PT AF утилиту traffic_settins.py можно запускать на любом базовом узле с ролью `master`. Утилита находится в каталоге `/var/pt/ptaf-deploy/current/scripts/` и требует предварительной настройки (см. раздел 15.7.1).

В этом разделе

Настройка утилиты traffic_settings.py (см. раздел 15.7.1)

Определение значения параметра base_url (см. раздел 15.7.2)

Изменение параметров изолированного пространства с помощью утилиты (см. раздел 15.7.3)

Настройка отображения информации о неуспешных попытках аутентификации по сертификатам (см. раздел 15.7.4)

15.7.1. Настройка утилиты traffic_settings.py

- Чтобы настроить утилиту:

  1. Перейдите в каталог `/var/pt/ptaf-deploy/current/scripts/`:
     ```
     cd /var/pt/ptaf-deploy/current/scripts/
     ```
  2. В файле `ptaf_settings.json` укажите следующие данные:
     - `base_url` — URL сервиса API PT AF.

       Примечание. Значение параметра `base_url` зависит от конфигурации (см. раздел 15.7.2) PT AF.
     - `username` — логин администратора изолированного пространства.

15.7.2. Определение значения параметра base_url

Значение параметра `base_url` зависит от конфигурации PT AF:

— В минимальной конфигурации — в качестве значения `base_url` нужно указать URL веб-интерфейса PT AF в формате `http[s]://<Адрес веб-интерфейса>`.

— В кластерной конфигурации:

- при совпадении VIP-адресов, назначенных сервису ptaf-border, веб-интерфейсу PT AF и веб-интерфейсу Grafana — в качестве значения `base_url` нужно указать строку `https://voyager-backend-ingress-1.ptaf-backend.svc.cluster.local`.
- при несовпадении VIP-адресов, назначенных сервису ptaf-border, веб-интерфейсу PT AF и веб-интерфейсу Grafana — значение `base_url` необходимо определять по инструкции ниже.

► Чтобы определить значение `base_url`:

1. Выведите и скопируйте VIP-адрес веб-интерфейса PT AF:
   ```
   wsc -c "vip list" | grep manage
   ```
2. Выполните команду, вставив в нее VIP-адрес веб-интерфейса PT AF из предыдущего шага:
   ```
   sudo kubectl get svc -n ptaf-backend | grep <VIP-адрес веб-интерфейса PT AF>
   ```
   В командной строке отобразится название сервиса Ingress для Voyager в формате `voyager-backend-ingress-N`.
3. Скопируйте название сервиса Ingress для Voyager в формате `voyager-backend-ingress-N`.
4. Вставьте скопированное на предыдущем шаге значение в строку `https://<Название сервиса Ingress для Voyager>.ptaf-backend.svc.cluster.local`.

   Например: `https://voyager-backend-ingress-1.ptaf-backend.svc.cluster.local`.

15.7.3. Изменение параметров изолированного пространства с помощью утилиты

► Чтобы изменить параметры изолированного пространства с помощью утилиты `traffic_settings.py`:

1. Перейдите в каталог `/var/pt/ptaf-deploy/current/scripts/`:
   ```
   cd /var/pt/ptaf-deploy/current/scripts/
   ```
2. Получите текущие параметры изолированного пространства:
   ```
   /var/pt/infra/current/ansible_virtualenv/bin/python3 /var/pt/ptaf-deploy/current/scripts/
   traffic_settings.py get > traffic_settings.json
   ```
3. Введите пароль администратора изолированного пространства.

4. Сделайте резервную копию текущих параметров изолированного пространства:
   ```
   cp traffic_settings.json traffic_settings.json.bak
   ```
5. Внесите необходимые изменения в файл `traffic_settings.json` и сохраните их:
   ```
   /var/pt/infra/current/ansible_virtualenv/bin/python3 /var/pt/ptaf-deploy/current/scripts/traffic_settings.py set < traffic_settings.json
   ```
6. Введите пароль администратора изолированного пространства.
7. Дождитесь применения конфигурации (см. раздел 7.6).

Таблица 18. Параметры изолированного пространства, настраиваемые с помощью утилиты traffic_settings.py

Параметр	Описание параметра	Тип данных	Значение по умолчанию
Управление веб-приложениями			
`max_applications_count`	Максимальное количество веб-приложений в изолированном пространстве. Максимальное значение — 30	Integer	`10`
`core_nginx_client_max_body_size`	Максимальный размер тела запроса	String	`1g`
Управление трафиком			
`core_nginx_host_header_mode`	Переопределение заголовка запроса Host или добавление к нему значений. Возможные значения: — host_listen_port[20]; — only_host[21];	Enum	`origin_host` — для пространств, созданных в PT AF версии 4.2.1 или выше; `legacy` — для изолированных пространств, созданных в PT AF версии ниже 4.2.1

20 Передача в заголовке Host имени сервера и порта проксируемого сервера. Соответствует значению директивы nginx `proxy_set_header Host $host:<port>`.

21 Передача в заголовке Host имени сервера. Соответствует значению директивы nginx `proxy_set_header Host $host`.

Параметр	Описание параметра	Тип данных	Значение по умолчанию
	— origin_host[22]; — legacy[23]		
envoy_preserve_headers_case	Сохранять ли регистр[24] для названий заголовков запросов, получаемых от клиента. Возможные значения: — true — сохранять регистр; — false — приводить к нижнему регистру	Boolean	true
Настройка буферов (сервер nginx)			
core_nginx_proxy_buffers	Количество и размер буферов, используемых для считывания ответа от проксируемого сервера для одного подключения. Количество буферов должно быть 2 или больше	String	8 8k
core_nginx_proxy_buffer_size	Максимальный размер буфера для чтения заголовков ответа от проксируемого сервера	String	8k

22 Позволяет передать неизмененный заголовок Host. Соответствует значению директивы nginx proxy_set_header Host $http_host.

23 Позволяет использовать в заголовке Host разные значения в зависимости от портов: для портов 80 и 443 будет использоваться значение only_host, для остальных портов — значение host_listen_port.

24 Параметр влияет на все профили трафика, для которых в качестве сервера для обработки трафика выбран Envoy, и на профили трафика с типом балансировщика **Внешний с контролем IP-адресов**, для которых в качестве сервера обработки трафика выбран nginx. При использовании механизма плавного завершения сессии (см. раздел 15.21.3) заголовки запросов всегда приводятся к нижнему регистру, параметр envoy_preserve_headers_case не влияет на регистр заголовков.

Параметр	Описание параметра	Тип данных	Значение по умолчанию
core_nginx_proxy_busy_buffers_size	Размер буферов[25], которые могут быть заняты для отправки ответа клиенту, пока ответ еще не прочитан целиком	String	16k
core_nginx_client_body_buffer_size	Размер буфера для чтения тела запроса клиента в ядре nginx (ptaf-core)	String	null
core_nginx_client_header_buffer_size	Максимальный размер буфера для чтения заголовка запроса клиента в ядре nginx (ptaf-core)	String	1k
core_nginx_large_client_header_buffers	Максимальное число и размер буферов для чтения большого заголовка запроса клиента в ядре nginx (ptaf-core)	String	4 8k
Настройка тайм-аутов (сервер nginx)			
core_nginx_proxy_read_timeout	Тайм-аут при чтении ответа проксированного сервера	String	60s
core_nginx_proxy_send_timeout	Тайм-аут при передаче запроса проксированному серверу	String	60s
core_nginx_send_timeout	Тайм-аут при передаче ответа клиенту	String	60s
core_nginx_keepalive_timeout	Время, в течение которого поддерживаемое клиентское соединение будет	String	75s

25 Минимальное значение должно быть больше или равно большему из значений: `core_nginx_proxy_buffer_size` или `core_nginx_proxy_buffers`. Максимальное значение должно быть меньше, чем значение, рассчитанное по формуле: `(core_nginx_proxy_buffers.num - 1) * core_nginx_proxy_buffers.size`

Параметр	Описание параметра	Тип данных	Значение по умолчанию
	оставаться открытым на стороне сервера		
core_nginx_proxy_connect_timeout	Тайм-аут для установления соединения с прокси-сервером	String	60s
core_nginx_worker_shutdown_timeout	Тайм-аут в секундах для плавного завершения рабочих процессов	String	30s
core_nginx_client_body_timeout	Тайм-аут при чтении тела запроса клиента	String	60s
core_nginx_client_header_timeout	Тайм-аут при чтении заголовка запроса клиента	String	60s
core_nginx_resolver_timeout	Тайм-аут для преобразования имени в адрес в ptaf-core	String	30s
Настройка тайм-аутов (сервер Envoy)			
core_envoy_listener_route_idle_timeout	Время, в течение которого соединение может существовать без активности в восходящем или нисходящем направлении. Переопределяет тайм-аут core_envoy_listener_stream_idle_timeout	String	60s
core_envoy_listener_stream_idle_timeout	Время, в течение которого соединение может существовать без активности в восходящем или нисходящем направлении	String	60s

Параметр	Описание параметра	Тип данных	Значение по умолчанию
core_envoy_listener_idle_timeout	Время существования соединения без активных запросов. По истечении этого времени соединение будет закрыто	String	75s
core_envoy_cluster_connect_timeout	Время ожидания для новых сетевых подключений к узлам в кластере	String	60s
core_envoy_cluster_query_timeout_seconds	Время в секундах, которое дается каждому серверу для ответа на запрос с первой попытки	Integer	30
core_envoy_listener_request_headers_timeout	Время ожидания получения заголовков запроса	String	60s
core_envoy_listener_route_timeout	Тайм-аут ожидания ответа от ядра Envoy (ptaf-envoy)	String	0s
Настройка записи событий в журналы access.log и error.log (сервер nginx)			
core_nginx_access_log	Записывать ли события в журнал access.log	Boolean	false
core_nginx_access_log_format	Формат записи данных в журнал access.log	String	"$remote_addr - $remote_user [$time_local] \"$request\" $status $body_bytes_sent \"$http_referer\" \"$http_user_agent\""
core_nginx_access_log_path	Расположение журнала access.log	String	syslog:server=unix:/opt/shared/log.sock,facility=local7,tag=nginx,severity=info
core_nginx_error_log_enabled	Записывать ли события в журнал error.log	Boolean	false

Параметр	Описание параметра	Тип данных	Значение по умолчанию
core_nginx_error_log_endpoints	Список точек назначения для отправки данных журнала error.log	Array of strings	["syslog:server=unix:/opt/shared/log.sock, facility=local7,tag=nginx error"]
Настройка записи событий в журналы access.log и error.log (сервер Envoy)			
core_envoy_access_log_enabled	Записывать ли события в журнал access.log	Boolean	false
core_envoy_access_log_format	Формат записи данных в журнал access.log	String	"%DOWNSTREAM_REMOTE_ADDRESS_WITHOUT_PORT% - - [%START_TIME(%d/%b/%Y:%T %z)%] \"%REQ(:METHOD)% %REQ(X-ENVOY-ORIGINAL-PATH?:PATH)% %PROTOCOL%\" %RESPONSE_CODE% %BYTES_SENT% \"%REQ(REFERER)%\" \"%REQ(USER-AGENT)%\""
core_envoy_error_log_format	Формат записи данных в журнал error.log	String	"[%Y-%m-%d %T.%e][%t][%l] [%n] [%g:%#] %v"
Настройка уровня журналирования			
core_nginx_log_level	Уровень логирования на сервере nginx. Возможные значения: — error; — info; — debug; — warn	Enum	error
core_envoy_log_level	Уровень логирования на сервере Envoy.	Enum	info

Параметр	Описание параметра	Тип данных	Значение по умолчанию
	Возможные значения: — `trace`; — `debug`; — `info`; — `warn`; — `error`; — `critical`; — `off`		
`core_ptaf_log_level`	Уровень логирования [26] модуля ядра PT AF. Возможные значения: — `trace`; — `debug`; — `info`; — `warning`; — `error`; — `fatal`; — `crit`	Enum	`error`
`envoy_proxy_log_level`	Уровень логирования на сервере Envoy при использовании внешнего балансировщика нагрузки с контролем IP-адресов.	Enum	`info`

26 Для сохранения производительности модуля ядра значение `debug` необходимо присваивать временно для максимальной детализации логирования и выключать, когда вся необходимая информация получена.

Параметр	Описание параметра	Тип данных	Значение по умолчанию
	Возможные значения: — `trace`; — `debug`; — `info`; — `warn`; — `error`; — `critical`; — `off`		

15.7.4. Настройка отображения информации о неуспешных попытках аутентификации по сертификатам

С помощью утилиты traffic_settings.py вы можете настроить отображение в журнале access.log информации о попытках аутентификации пользователей защищаемых приложений без сертификатов и с использованием невалидных клиентских сертификатов.

Примечание. В журнале error.log неуспешные попытки аутентификации по клиентским сертификатам отображаются, если на сервере установлен режим логирования debug.

- Чтобы настроить отображение неуспешных попыток аутентификации по клиентским сертификатам в журнале access.log,

  следуя инструкции (см. раздел 15.7.3), в файле `traffic_settings.json`:

  - включите запись событий в журнал access.log:
    ```
    "core_nginx_access_log": true
    ```
  - измените формат записи событий в журнал, добавив печать заголовка `X-Block-Type` с помощью переменной журнала `$sent_http_x_block_type`, например:
    ```
    "core_nginx_access_log_format": "$remote_addr - $remote_user [$time_local] \"$request\"
    $status $body_bytes_sent \"$sent_http_x_block_type \"$http_referer\" \"$http_user_agent\""
    ```

  При неуспешных попытках аутентификации пользователей по клиентским сертификатам в журнале access.log будут появляться записи со значением `id003` для переменной `$sent_http_x_block_type`. Пример записи в журнале: `10.233.82.81 - - [17-Apr-2026:13:19:17 +0000] "GET / HTTP/1.1" 403 9 "id003 "-" "Mozilla"`.

15.8. Управление ICAP-серверами

PT AF может отправлять извлеченные из запросов файлы на проверку во внешнюю аналитическую систему. Результат проверки возвращается в PT AF и при наличии угроз в файле приводит к срабатыванию правила.

Для настройки интеграции нужно добавить ICAP-сервер и настроить правило **Отправлять файлы на ICAP-серверы** в шаблоне политики безопасности.

Вы можете управлять ICAP-серверами на странице **Система** → **ICAP-серверы**.

> **Внимание!** Не поддерживается антивирусная проверка файлов с помощью сторонних ICAP-серверов при обработке трафика на сервере Envoy (см. раздел 15.6.5).

В этом разделе

Добавление ICAP-сервера (см. раздел 15.8.1)

Изменение параметров ICAP-сервера (см. раздел 15.8.2)

Удаление ICAP-сервера (см. раздел 15.8.3)

15.8.1. Добавление ICAP-сервера

Добавление нового ICAP-сервера

- Чтобы добавить ICAP-сервер:

  1. В таблице ICAP-серверов нажмите +.
  2. Введите название ICAP-сервера.
  3. Введите адрес ICAP-сервера в формате `icap://<Доменное имя или IP-адрес ICAP-сервера>:<Номер порта>`.

     Примечание. В зависимости от режима проверки и режима работы ICAP-сервера адрес может содержать дополнительные параметры. Например, `icap://192.0.2.36:1344/scanrequest?modify=y&block-unwanted=y&timeout=30`.
  4. Если требуется, измените тайм-аут проверки.

     Примечание. Значительное увеличение тайм-аута может привести к нестабильной работе PT AF при обработке запросов с большим количеством файлов.
  5. Если вы добавляете ICAP-сервер в базовом изолированном пространстве `general`, выберите область видимости ICAP-сервера.

     Примечание. Локальный сервер будет доступен только администраторам текущего изолированного пространства, системный сервер — администраторам всех изолированных пространств.

Примечание. Системный сервер можно добавить только в базовом изолированном пространстве `general`. После добавления нельзя сменить область видимости сервера.

6. Если требуется, добавьте дополнительные заголовки запроса к ICAP-серверу.

   Примечание. В значении заголовка можно указывать переменные (см. раздел 11.6) в формате `%<Название переменной>`.

7. Введите название заголовка ответа ICAP-сервера для передачи вердикта о вредоносности проверяемых файлов.

   Примечание. Название заголовка определяет разработчик ICAP-сервера. Например, PT Sandbox в режиме ожидания при обнаружении угрозы отправляет ответ с кодом 204 и добавляет заголовок `X-Virus-ID` с кратким описанием угрозы.

8. Если требуется, проверьте соединение с ICAP-сервером.
9. Нажмите **Добавить**.

Добавление ICAP-сервера на основе существующего

- Чтобы добавить ICAP-сервер на основе существующего:

  1. В строке с параметрами ICAP-сервера нажмите →.
  2. Нажмите **Действия** → **Копировать**.

     Откроется окно добавления ICAP-сервера. Поля будут заполнены значениями параметров ICAP-сервера, на основе которого создается новый сервер.

  3. Измените название ICAP-сервера и внесите другие необходимые изменения.

     Примечание. Название ICAP-сервера должно быть уникальным в рамках изолированного пространства.

  4. Если требуется, проверьте соединение с ICAP-сервером.
  5. Нажмите **Добавить**.

15.8.2. Изменение параметров ICAP-сервера

- Чтобы изменить параметры ICAP-сервера:

  1. В строке с параметрами ICAP-сервера нажмите →.
  2. Внесите изменения.
  3. Если требуется, проверьте соединение с ICAP-сервером.
  4. Нажмите **Сохранить**.

15.8.3. Удаление ICAP-сервера

- Чтобы удалить ICAP-сервер:

  1. В строке с названием ICAP-сервера нажмите →.
  2. Нажмите **Удалить** и подтвердите удаление.

15.9. Управление кластером Kubernetes

В этом разделе приведены инструкции по управлению узлами кластера Kubernetes.

Внимание! Не меняйте IP-адрес сетевого интерфейса eth-cluster, поскольку это действие приводит к потере работоспособности PT AF.

В этом разделе

Подготовка узла к добавлению в кластер (см. раздел 15.9.1)

Добавление узла в кластер (см. раздел 15.9.2)

Изменение имени узла кластера (см. раздел 15.9.3)

Удаление узла из кластера (см. раздел 15.9.4)

См. также

Команды сбора и реконфигурации кластера Kubernetes (см. приложение А.6)

15.9.1. Подготовка узла к добавлению в кластер

Перед добавлением узла в кластер необходимо его подготовить.

- Чтобы подготовить узел к добавлению в кластер:

  1. На узле установите ОС тем способом, который использовали при установке PT AF:
     - Debian из ISO-образа.
     - Debian из OVA-образа.
     - Debian из QCOW2-образа.
     - Astra Linux из репозитория.
  2. Если вы используете ОС Astra Linux, настройте ее.
  3. Проверьте и измените имя узла.
  4. Настройте виртуальные IP-адреса узла.

5. Настройте синхронизацию системного времени узла с NTP-серверами.
6. Настройте сетевые интерфейсы узла.

Далее вы можете добавить узел в кластер.

15.9.2. Добавление узла в кластер

Вы можете добавлять в кластер базовые и дополнительные узлы.

При добавлении узлов необходимо учитывать следующие особенности назначения ролей:

— Количество базовых узлов с ролью `master` должно оставаться нечетным. Таким образом, если необходимы новые узлы с ролью `master`, необходимо добавить два таких узла.

— Должен быть один или четное количество базовых узлов с ролью `clickhouse`. Таким образом, если необходимы новые узлы с ролью `clickhouse`:

- если базовый узел с ролью `clickhouse` один, необходимо добавить один или другое нечетное количество узлов;
- если базовых узлов с ролью `clickhouse` четное количество, необходимо добавить два или другое четное количество таких узлов.

— При добавлении узлов с ролью `minio` необходимо добавлять количество узлов, кратное текущему количеству узлов с этой ролью. Например, если до добавления новых узлов в кластере было три узла с ролью `minio`, можно добавить три, шесть, девять узлов с ролью `minio`.

► Чтобы добавить узел кластера Kubernetes:

1. На базовом узле предварительной настройки кластера в интерфейсе командной строки добавьте новый узел в конфигурацию Kubernetes:

   ```
   sudo wsc -c "inventory node add <Имя узла>"
   ```

   Например:

   ```
   sudo wsc -c "inventory node add node1.af4.example.com"
   ```

2. Добавьте параметры узла:

   ```
   sudo wsc -c "inventory node set <Имя узла> port <Номер порта для доступа к узлу по SSH>
   user_name <Логин для доступа к узлу по SSH> user_password <Пароль для доступа к узлу по
   SSH> cluster_ip <IP-адрес нового узла> sudo_password <Пароль для выполнения команд от
   имени администратора> role <Роли узла>"
   ```

3. Выполните проверку параметров узлов и сервисов:

   ```
   sudo wsc -c "inventory check"
   ```

4. Примените изменения:

   ```
   sudo wsc -c "config commit"
   ```

5. Запустите сценарии установки PT AF:

- Если вы добавляете базовый узел, выполните команду:
  ```
  sudo /var/pt/infra/current/install.sh
  ```
- Если вы добавляете дополнительный узел с ролью `worker-traffic`, выполните команду:
  ```
  sudo /var/pt/infra/current/install.sh --action=add_worker
  ```

6. По завершении установки убедитесь, что узел добавлен в кластер:
   ```
   sudo kubectl get nodes
   ```
7. Запустите установку пакета ptaf-deploy:
   ```
   sudo /var/pt/ptaf-deploy/current/install.sh
   ```
8. Проверьте работоспособность всех подов:
   ```
   sudo kubectl get pods --all-namespaces -o wide
   ```

15.9.3. Изменение имени узла кластера

В разделе приведена инструкция по изменению имени любого узла кластера.

► Чтобы изменить имя узла:

1. На узле с ролью `master` в интерфейсе командной строки выведите параметры конфигурации переименовываемого узла:
   ```
   sudo wsc -c "inventory node list <Старое имя узла>"
   ```
2. Скопируйте и сохраните значения параметров.
3. Выведите пароль для повышения привилегий (sudo password):
   ```
   sudo wsc -c "inventory render type json" | jq '._meta.hostvars."<Старое имя
   узла>".ansible_become_pass'
   ```
4. Скопируйте и сохраните пароль.
5. Удалите переименовываемый узел из конфигурации кластера (inventory):
   ```
   sudo wsc -c "inventory node del <Старое имя узла> force"
   ```
6. Удалите все поды с узла:
   ```
   sudo kubectl get nodes
   sudo kubectl drain <Старое имя узла> --ignore-daemonsets=true --delete-emptydir-data=true
   ```
7. Удалите узел из кластера Kubernetes:
   ```
   sudo kubectl delete node <Старое имя узла>
   ```
8. На переименовываемом узле сбросьте параметры Kubernetes:
   ```
   sudo kubeadm reset
   sudo rm -fr /etc/cni/net.d/
   sudo rm -fr /etc/kubernetes/
   sudo rm -fr ~/.kube/
   ```
9. На всех узлах кластера в файле `/etc/hosts` смените имя переименовываемого узла на новое.

10. На переименовываемом узле смените имя узла:
    ```
    sudo hostnamectl set-hostname <Новое имя узла>
    ```
11. На узле с ролью `master` добавьте новый узел в конфигурацию Kubernetes:
    ```
    sudo wsc -c "inventory node add <Новое имя узла>"
    ```
12. Восстановите параметры:
    ```
    sudo wsc -c "inventory node set <Новое имя узла> cluster_ip CLUSTER_IP port SSH_PORT
    user_name SSH_USER sudo_password SUDO_PASSWORD ssl_key KEY_PATH"
    sudo wsc -c "inventory node set <Новое имя узла> role ROLES"
    ```
    Примечание. Вы можете просмотреть значения параметров после восстановления с помощью команды `sudo wsc -c "inventory node list <Новое имя узла>"` и проверить корректность конфигурации с помощью команды `sudo wsc -c "inventory check"`.
13. Запустите сценарий установки системы:
    ```
    /var/pt/infra/current/install.sh
    ```

Имя узла изменено.

15.9.4. Удаление узла из кластера

Вы можете удалить узлы из кластера.

Удаление базового узла с ролью master

- Чтобы удалить узел из кластера Kubernetes,

  запустите сценарий удаления узла и подтвердите действие:
  ```
  sudo /var/pt/infra/current/install.sh --action=remove_failed_node --nodes <Имя узла>
  ```

Удаление дополнительного узла с ролью worker-traffic

- Чтобы удалить узел из кластера Kubernetes:

  1. Запустите сценарий удаления узла и подтвердите действия:
     ```
     sudo /var/pt/infra/current/install.sh --action=remove_worker --nodes <Имя узла>
     ```
  2. Удалите узел из конфигурации кластера:
     ```
     sudo wsc -c "inventory node del <Имя узла> role worker-traffic"
     sudo wsc -c "inventory node del <Имя узла>"
     ```
  3. Выполните проверку параметров узлов и сервисов:
     ```
     sudo wsc -c "inventory check"
     ```

4. Убедитесь, что узел удален из кластера:
   ```
   sudo kubectl get nodes
   ```
5. Проверьте работоспособность всех подов и убедитесь, что информация об удаленном узле удалена из конфигурации:
   ```
   sudo kubectl get pods --all-namespaces -o wide
   ```

15.10. Мониторинг состояния PT AF

В PT AF доступны встроенные средства для мониторинга работоспособности и целостности системы и ее сервисов. Также предусмотрена возможность интеграции с Grafana.

В этом разделе

Мониторинг встроенными средствами (см. раздел 15.10.1)

Мониторинг состояния в Grafana (см. раздел 15.10.2)

15.10.1. Мониторинг встроенными средствами

Результаты мониторинга отображаются на странице **Система** → **Мониторинг** → **Система**. Если PT AF развернут в кластерной конфигурации, в верхней части рабочей области находится навигационная панель для выбора отображаемых данных — о состоянии всего кластера и о состоянии каждого из его узлов.

На виджетах отображается следующая информация:

— **Бесперебойная работа.** Доля времени с момента установки, в течение которого PT AF был доступен (в процентах). Также в нижней части виджета отображаются дополнительные показатели:

- **Последний перезапуск** — время с последнего перезапуска PT AF;
- **Время простоя** — суммарное время недоступности PT AF с момента установки;
- **Время жизни** — суммарное время работы PT AF с момента установки.

— **Статус сервисов.** Список сервисов узла со статусами:

✓ — сервис работает корректно;

! — сервис перегружен, может возникнуть проблема в его работе;

! — сервис недоступен, произошла неполадка или ошибка в его работе;

! — сервис работает корректно, но произошло системное событие, не нарушающее его работоспособность.

> **Примечание.** Если поды сервиса неработоспособны, отображаются сообщения об ошибках и информация о способе их устранения.

— **ЦПУ.** Утилизация ядер ЦП.

— **ОЗУ.** Утилизация ОЗУ.

— **Средняя нагрузка.** Среднее значение загруженности PT AF. Вычисляется как длина очереди из процессов, ждущих выполнения в операционной системе.

— **Диск I/O (R/W).** Скорость чтения и записи данных.

— **Сеть I/O.** Суммарная скорость входящего и исходящего трафика на всех сетевых интерфейсах.

— **БД событий безопасности.** Скорость выполнения операций с БД событий безопасности.

— **БД конфигурации.** Скорость выполнения операций с БД конфигурации.

15.10.2. Мониторинг состояния в Grafana

Мониторинг состояния PT AF в Grafana доступен на обзорном дашборде **Home** → **Dashboards** → **Infrastructure** → **System Status**. На дашборде отображаются основные индикаторы состояния PT AF, виджеты и фильтры.

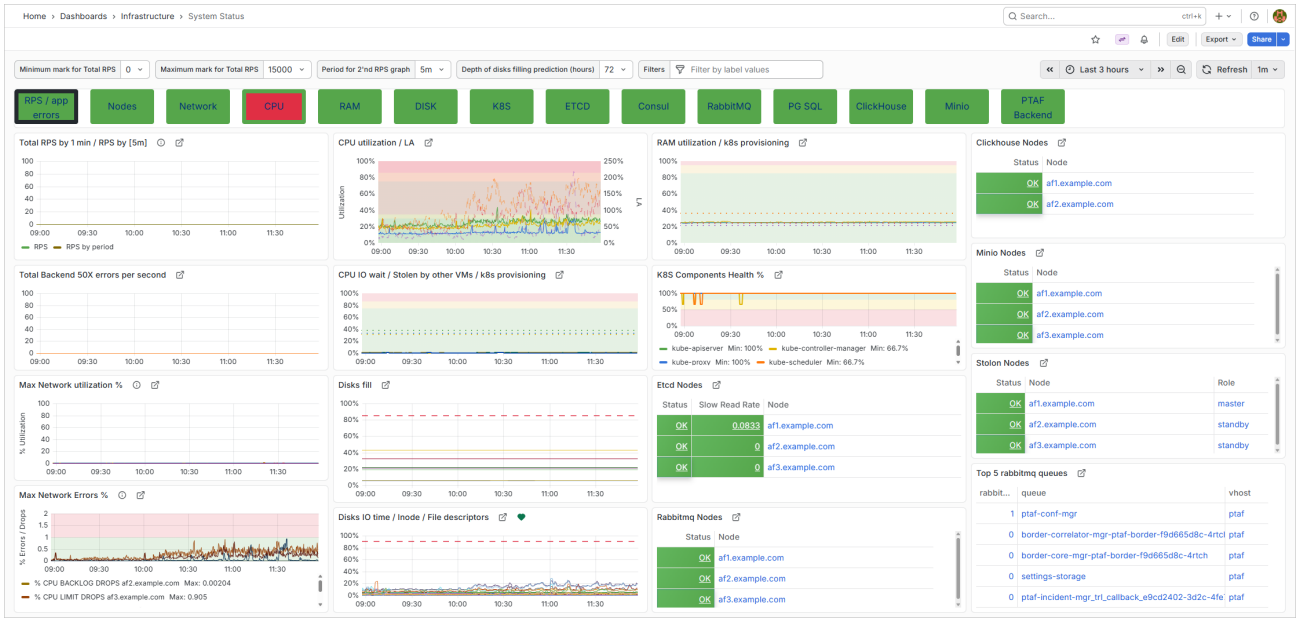


Рисунок 16. Мониторинг состояния PT AF в Grafana

Каждый индикатор окружен рамкой. Цвет индикатора и рамки сигнализирует о состоянии той или иной подсистемы (см. приложение Д) для всего кластера без разделения на зоны, изолированные пространства и веб-приложения.

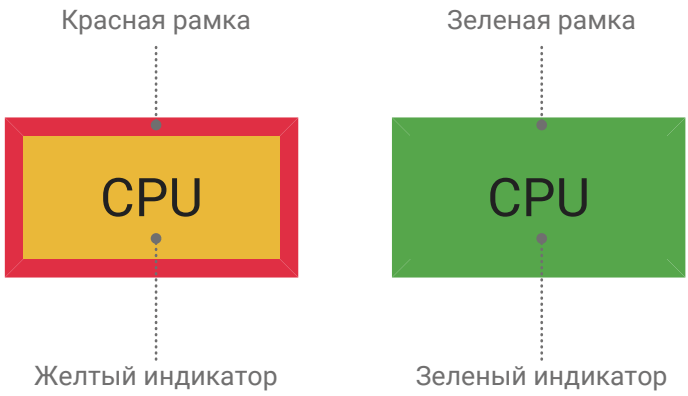


Рисунок 17. Индикатор и рамка

15.11. Установка доверенного сертификата для веб-интерфейса PT AF

При развертывании PT AF для его веб-интерфейса автоматически устанавливается самоподписанный сертификат, поставляемый в составе дистрибутива. Поэтому при попытке подключения к веб-интерфейсу вы получите предупреждение о том, что создаваемое подключение не защищено.

Вы можете установить собственный доверенный сертификат, который должен отвечать следующим требованиям:

- Алгоритмы шифрования сертификата должны поддерживаться библиотекой OpenSSL версии 3.0.11.
- Длина ключа должна быть не менее 2048 бит.
- В расширении Subject Alternative Name (SAN) должны быть указаны все домены, для которых используется сертификат.

► Чтобы установить доверенный сертификат:

1. Разместите файлы сертификата и закрытого ключа на одном из базовых узлов в любом каталоге.
2. Скопируйте файлы:
   ```
   sudo cp <Имя файла сертификата> ptaf-restproxy.crt
   sudo cp <Имя файла закрытого ключа> ptaf-restproxy.pem
   ```
3. Удалите секрет с данными старого сертификата:
   ```
   sudo kubectl delete secret ptaf-restproxy-certs -n ptaf-backend
   ```

4. Создайте секрет с данными нового сертификата:

   ```
   sudo kubectl create secret generic ptaf-restproxy-certs --from-file=./ptaf-restproxy.crt
   --from-file=./ptaf-restproxy.pem -n ptaf-backend
   ```

5. Перезапустите под ptaf-restproxy:

   ```
   sudo kubectl -n ptaf-backend rollout restart deployment ptaf-restproxy
   ```

15.12. Обновление базы знаний

События безопасности защищаемых веб-приложений регистрируются на основании базы знаний, которая содержит информацию о правилах, необходимых для защиты. База регулярно пополняется новыми правилами. Для достижения максимальной безопасности веб-приложений базу знаний необходимо поддерживать в актуальном состоянии.

Механизм обновления базы знаний позволяет получать последние обновления, не дожидаясь выхода новой версии продукта. А в случае возникновения уязвимостей нулевого дня вы своевременно можете получить правила для их блокировки.

В этом разделе

Обновление базы знаний через веб-интерфейс (см. раздел 15.12.1)

Проверка обновления на наличие конфликтов (см. раздел 15.12.2)

Просмотр отчета об обновлении (см. раздел 15.12.3)

15.12.1. Обновление базы знаний через веб-интерфейс

Вы можете выполнить обновление базы знаний PT AF, получив файл обновления в технической поддержке Positive Technologies. Файл обновления необходимо загрузить в систему. Загрузка файла обновления доступна только администратору PT AF.

В случае конфликтов при обновлении предпочтение отдается новой версии. Конфликты могут возникнуть в случае удаления используемых системных правил или сброса переопределенных пользователем значений параметров правил к значениям по умолчанию. До запуска обновления вы можете проверить его на наличие конфликтов (см. раздел 15.12.2).

- Чтобы обновить базу знаний через веб-интерфейс:

  1. В главном меню нажмите ? и в раскрывшемся меню выберите пункт **О продукте**.

     Откроется карточка с информацией об активной лицензии и версиях используемых компонентов.

  2. Нажмите кнопку **Загрузить обновление** и выберите файл для загрузки обновления.

     PT AF выполнит проверку файла. Если файл имеет подходящий формат и содержит более свежую версию базы знаний, то обновление будет разрешено.

Примечание. Во время загрузки файла обновления вы можете продолжить работу с системой, загрузка будет проходить в фоновом режиме.

3. Нажмите кнопку **Обновить базу знаний**.

   Начнется обновление базы знаний PT AF. На время обновления будут заблокированы все действия с объектами системы.

База знаний обновлена. В карточке отображается новая версия базы знаний. При необходимости вы можете просмотреть отчет об обновлении (см. раздел 15.12.3).

См. также

Проверка обновления на наличие конфликтов (см. раздел 15.12.2)

Просмотр отчета об обновлении (см. раздел 15.12.3)

15.12.2. Проверка обновления на наличие конфликтов

До запуска обновления вы можете выполнить проверку обновления на наличие конфликтов, а затем принять решение о необходимости обновления.

- Чтобы проверить обновление на конфликты:

1. В главном меню нажмите ? и в раскрывшемся меню выберите пункт **О продукте**.

   Откроется карточка с информацией об активной лицензии и версиях используемых компонентов.

2. Нажмите кнопку **Загрузить обновление** и выберите файл для загрузки обновления.

   PT AF выполнит проверку файла. Если файл имеет подходящий формат и содержит более свежую версию базы знаний, то обновление будет разрешено.

   Примечание. Во время загрузки файла обновления вы можете продолжить работу с системой, загрузка будет проходить в фоновом режиме.

3. Нажмите кнопку **Проверить на конфликты**.

   Начнется проверка обновления базы знаний PT AF на конфликты. Проверка может занять некоторое время. Если конфликты будут обнаружены, у администратора PT AF и администратора изолированного пространства появятся соответствующие предупреждения.

4. Если конфликты обнаружены и вам требуется просмотреть информацию о конфликтах, нажмите кнопку **Показать конфликты**.

   Откроется карточка с описанием конфликтов обновления базы знаний.

   Примечание. Вы можете просмотреть подробную информацию об изменении параметра по кнопке → в строке записи о конфликте.

Если потеря пользовательской конфигурации правил, для которых возник конфликт, допустима, вы можете запустить обновление по кнопке **Обновить базу знаний**.

15.12.3. Просмотр отчета об обновлении

После загрузки обновления вы можете просмотреть отчет о конфликтах и обновленных правилах.

> **Примечание.** Данные в отчете для администратора PT AF сгруппированы по изолированным пространствам.

- Чтобы просмотреть отчет об обновлении:

  1. В главном меню нажмите ? и в раскрывшемся меню выберите пункт **О продукте**.

     Откроется карточка с информацией об активной лицензии и версиях используемых компонентов.

  2. По ссылке **Отчет** откройте карточку отчета об обновлении базы знаний.

     На вкладке **Изменения без конфликтов** отображается информация о появлении новых правил, удалении правил и изменении уже существующих правил, параметры которых не были переопределены до обновления. На вкладке **Разрешенные конфликты** отображается информация об обновленных правилах, в которых изменены пользовательские значения параметров.

15.13. Работа с лицензией

Порядок работы с лицензией зависит от цели ее приобретения:

- **Продление срока действия лицензии.** Необходимо по истечении срока действия лицензии, чтобы сохранить доступ к защитным функциям и механизмам PT AF, к поставке обновлений и технической поддержке. Для продления лицензии необходимо обратиться в Positive Technologies.
- **Замена лицензии.** Необходима при изменении конфигурации физического сервера с установленной системой PT AF или в случае миграции системы с одного виртуального сервера на другой. Для замены лицензии необходимо обратиться в службу технической поддержки Positive Technologies.

Таблица 19. Порядок работы с лицензией

Этап	Действие	
	Продление лицензии	**Замена лицензии**
1	Получение фингерпринта (см. раздел 15.13.1)	
2	Загрузка лицензии (см. раздел 15.13.2)	
3	—	Активация лицензии (см. раздел 15.13.3)

В этом разделе

Получение фингерпринта (см. раздел 15.13.1)

Загрузка лицензии (см. раздел 15.13.2)

Активация лицензии (см. раздел 15.13.3)

Просмотр информации о лицензии PT AF (см. раздел 15.13.4)

15.13.1. Получение фингерпринта

Для получения фингерпринта вам потребуется предварительно запросить у менеджера Positive Technologies ключ инициализации.

► Чтобы получить фингерпринт:

1. Перейдите на страницу веб-интерфейса PT AF для работы с лицензиями:
   - Если вы продляете лицензию, в главном меню нажмите ? и выберите пункт **Лицензии**.
   - Если вы заменяете лицензию, войдите в веб-интерфейс PT AF и нажмите **Управление лицензиями**.
2. Нажмите +.
3. В поле **Ключ** введите ключ инициализации.
4. Нажмите **Скачать фингерпринт**.

   PT AF создаст файл фингерпринта.

Файл фингерпринта необходимо отправить менеджеру Positive Technologies по электронной почте. Менеджер Positive Technologies на основании фингерпринта создаст файл лицензии и пришлет его вам.

15.13.2. Загрузка лицензии

Полученный файл лицензии вам нужно загрузить в PT AF. Вы можете загружать в PT AF только лицензии, полученные от Positive Technologies.

Для загрузки лицензии вам потребуется принять условия лицензионного соглашения с конечным пользователем программного обеспечения PT AF. С текстом соглашения вы можете ознакомиться на странице загрузки лицензии.

► Чтобы загрузить лицензию:

1. Перейдите на страницу веб-интерфейса PT AF для работы с лицензиями:
   - Если вы продляете лицензию, в главном меню нажмите ? и выберите пункт **Лицензии**.

- Если вы заменяете лицензию, войдите в веб-интерфейс PT AF и нажмите **Управление лицензиями**.

2. Нажмите +.
3. В блоке параметров **Загрузить лицензию** нажмите **Прочесть из файла**.
4. Выберите файл для загрузки ключа лицензии и нажмите **Открыть**.

   В поле **Токен** появится ключ лицензии.

   Примечание. Если файл лицензии загрузить не удается, вы можете ввести ключ лицензии в поле **Токен** вручную.
5. Установите флажок **Я согласен с условиями лицензионного соглашения**.
6. Нажмите **Загрузить лицензию**.

Лицензия загружена. Если вы продляете лицензию, необходимо активировать загруженную лицензию вручную (см. раздел 15.13.3).

15.13.3. Активация лицензии

Для работы в PT AF загруженная лицензия должна быть активирована. При первичной загрузке лицензии активация происходит автоматически. При наличии в системе действующей лицензии следующую загружаемую лицензию нужно активировать вручную. В системе может быть только одна активная лицензия.

► Чтобы активировать лицензию:

1. В главном меню нажмите ? и выберите пункт **Лицензии**.
2. В строке лицензии нажмите →.
3. Нажмите **Активировать лицензию**.

15.13.4. Просмотр информации о лицензии PT AF

Вы можете просмотреть информацию о любой лицензии, загруженной в PT AF.

► Чтобы просмотреть информацию о лицензии PT AF:

1. В главном меню нажмите ? и выберите пункт **Лицензии**.
2. В строке лицензии нажмите →.

См. также

Просмотр информации о системе PT AF (см. раздел 17.1)

15.14. Об архивации журнала событий

PT AF автоматически архивирует файлы журнала событий с помощью стандартной утилиты `logrotate`. Файлы журнала находятся в каталоге `/var/log`, правила ротации файлов — в каталоге `/etc/logrotate.d`.

Утилита `logrotate` автоматически запускается каждый час и архивирует файлы, подпадающие под правила ротации. Архивы размещаются в каталоге с файлами журналов.

15.15. Настройка взаимной TLS-аутентификации клиента с агентом PT AF

- Чтобы настроить взаимную TLS-аутентификацию (mTLS) клиента с агентом:

  1. На сервере агента в файле `/etc/nginx/nginx.conf` в секции `http` → `server` проверьте значения директив:

     ```
     ssl on;
     ssl_certificate <Путь к файлу сертификата>;
     ssl_certificate_key <Путь к файлу закрытого ключа>;
     ```

  2. В секцию `http` → `server` добавьте директивы:

     ```
     ssl_verify_client on;
     ssl_client_certificate <Путь к файлу с доверенными сертификатами удостоверяющего центра (CA), которые используются для проверки подлинности клиентских сертификатов>;
     ```

  3. На стороне клиента импортируйте клиентский сертификат в программное обеспечение, для которого требуется поддержка взаимной TLS-аутентификации с агентом.

15.16. Настройка отправки сообщений о событиях аудита на удаленный syslog-сервер

- Чтобы настроить отправку сообщений о событиях аудита на удаленный syslog-сервер:

  1. В главном меню выберите **Система**.
  2. Выберите вкладку **Отправка событий аудита**.
  3. Если требуется, примените конфигурацию ко всем изолированным пространствам.
  4. Включите отправку событий.
  5. Введите IP-адрес или доменное имя syslog-сервера.
  6. Если требуется, измените протокол и порт для отправки сообщений.
  7. Укажите максимальный размер сообщения: не более 65 507 байт для протокола UPD и не более 104 8576 байт для TCP.
  8. Нажмите **Сохранить**.

15.17. Резервное копирование и восстановление данных PT AF

В резервной копии сохраняются параметры:

- учетных записей и пользовательских ролей;
- веб-приложений и шаблонов политик безопасности;
- наборов системных и пользовательских правил;
- действий;
- глобальных списков;
- профилей трафика, защищаемых серверов и IP-адресов для прослушивания;
- действий с HTTP-заголовками;
- конфигураций SSL и цепочек сертификатов SSL, включая закрытые ключи.

В резервной копии не сохраняются данные о событиях безопасности.

Можно восстановить данные из резервной копии, созданной как на текущей, так и на предыдущей версии системы. Если версия базы знаний в резервной копии ниже текущей версии, PT AF обновит базу знаний, сохраненную в резервной копии.

> **Внимание!** Не поддерживается восстановление резервной копии на другом экземпляре PT AF (в том числе и на заново установленном), если он содержит другое количество узлов (отличное от экземпляра резервной копии), а также другие названия зон доступности.
>
> **Внимание!** В изолированных пространствах с типом обработки трафика **PT AF** и сервером для модулей обработки трафика nginx при восстановлении данных из резервных копий, созданных в версиях ниже 4.4.0, параметры, связанные с поведением HTTP-заголовков, восстановлены не будут. Для управления HTTP-заголовками необходимо создать действия с заголовками (см. раздел 8.2.8) и добавить их в параметры веб-приложений.

Вы можете работать с резервными копиями на странице **Система** → **Резервные копии**.

В этом разделе

Создание резервной копии (см. раздел 15.17.1)

Восстановление данных из резервной копии (см. раздел 15.17.2)

Скачивание резервной копии (см. раздел 15.17.3)

Удаление резервной копии (см. раздел 15.17.4)

15.17.1. Создание резервной копии

- Чтобы создать резервную копию:

  1. Нажмите **Новая копия**.
  2. Введите название копии.
  3. Если требуется зашифровать резервную копию, включите защиту паролем и введите пароль.
  4. Нажмите **Создать**.

     Начнется создание резервной копии. По завершении копирования в описании статуса копии появится информация о дате и времени ее создания.
  5. Нажмите **Закрыть**.

     Примечание. Вы можете закрыть карточку копии до завершения резервного копирования. Это не прервет процесс создания копии. Вы можете узнать о статусе копии в таблице резервных копий.

После создания копии рекомендуется ее скачать (см. раздел 15.17.3) и сохранить на внешний носитель.

15.17.2. Восстановление данных из резервной копии

Во время восстановления веб-интерфейс PT AF будет заблокирован. После начала восстановления отменить его невозможно.

- Чтобы восстановить данные из резервной копии:

  1. В строке с названием копии нажмите →.
  2. Нажмите **Восстановить из копии**.
  3. Введите название копии или пароль (если копия зашифрована).
  4. Нажмите **Восстановить из копии**.

     Начнется восстановление данных из резервной копии. Сессии всех пользователей будут автоматически завершены. Они смогут войти в PT AF только после завершения восстановления.
  5. По завершении восстановления нажмите **Перейти на страницу входа** и войдите в PT AF.

Если названия узлов в резервной копии и в текущем экземпляре PT AF отличаются, после входа в верхней части страницы отобразится уведомление о необходимости проверки соответствия названий. Уведомление содержит ссылку[27] для перехода в карточку настройки соответствия.

6. Если отображается уведомление о необходимости проверки соответствия названий, выполните следующие действия:
   - По ссылке откройте карточку и, если требуется, настройте соответствие узлов.
   - Нажмите **Сохранить**.

15.17.3. Скачивание резервной копии

► Чтобы скачать резервную копию:

1. В строке с названием копии нажмите →.
2. Нажмите **Действия** → **Скачать**.
3. Выберите папку для скачивания архива с резервной копией.
4. Нажмите **Сохранить**.

15.17.4. Удаление резервной копии

► Чтобы удалить резервную копию:

1. В строке с названием копии нажмите →.
2. Нажмите **Действия** → **Удалить**.
3. Введите название копии.
4. Нажмите **Удалить**.

15.18. Экспорт и импорт параметров защиты приложений

К параметрам защиты относятся:

— веб-приложения и их политики безопасности;

— шаблоны политик безопасности;

— пользовательские правила;

— глобальные списки IP-адресов;

— пользовательские действия.

---

27 Доступна только администратору базового изолированного пространства `general`.

Внимание! Глобальные списки экспортируются и импортируются без содержащихся в них IP-адресов.

Экспорт и импорт параметров защиты приложений может понадобиться, например, в следующих случаях:

- для использования одинаковых параметров защиты приложений в нескольких изолированных пространствах;
- резервного копирования перед масштабными изменениями;
- отправки информации в техническую поддержку Positive Technologies;
- автоматизации хранения и резервирования параметров защиты приложений с помощью сторонних инструментов (например, Git).

В этом разделе

Экспорт параметров защиты приложений (см. раздел 15.18.1)

Импорт параметров защиты приложений (см. раздел 15.18.2)

Управление асинхронным импортом параметров защиты (см. раздел 15.18.3)

15.18.1. Экспорт параметров защиты приложений

При экспорте формируется JSON-файл с параметрами защиты приложений (см. раздел 15.18) изолированного пространства.

► Чтобы экспортировать параметры защиты приложений изолированного пространства:

1. В главном меню выберите **Схема конфигурации**.
2. Вверху справа нажмите ↑↓ и выберите **Экспортировать параметры защиты**.
3. Нажмите **Загрузить**.

JSON-файл с параметрами защиты приложений изолированного пространства загружен на ваш компьютер. Вы можете импортировать параметры защиты в другое изолированное пространство.

15.18.2. Импорт параметров защиты приложений

При импорте параметров защиты приложений следует учитывать следующие особенности:

— При импорте выполняется полная замена всех параметров защиты приложений изолированного пространства на импортируемые. Например, если до импорта в изолированное пространство были добавлены пользовательские правила, а в импортируемом JSON-файле их нет, после импорта параметров защиты пользовательские правила будут удалены.

— Если в изолированном пространстве есть объект с таким же названием, как объект в импортируемом файле, при импорте объект не удалится из изолированного пространства, но его параметры будут заменены на те, которые указаны для объекта с таким же названием в файле импорта.

► Чтобы импортировать параметры защиты приложений в изолированное пространство:

1. В главном меню выберите **Схема конфигурации**.
2. Вверху справа нажмите ↑↓ и выберите **Импортировать параметры защиты**.
3. Перетащите JSON-файл с параметрами защиты приложений в область загрузки или выберите файл, нажав ссылку.
4. Нажмите **Импортировать**.

   Начнется импорт параметров защиты. До завершения импорта некоторые объекты PT AF доступны только для просмотра.

После импорта параметров защиты может начаться процесс применения конфигурации. Вы можете отследить статус применения конфигурации по индикатору в главном меню (см. раздел 7.6).

15.18.3. Управление асинхронным импортом параметров защиты

В PT AF реализован механизм асинхронного импорта, который позволяет импортировать большое количество параметров защиты без возникновения ошибок.

Вы можете управлять параметрами асинхронного импорта, задаваемыми с помощью переменных:

— `IMPORT_ASYNC_ENABLED` — включение механизма асинхронного импорта. Значение по умолчанию — true (асинхронный импорт включен).

— `CHECK_STATUS_ATTEMPTS` — количество попыток завершения синхронизации. Значение по умолчанию — 60.

— `CHECK_STATUS_TIMEOUT` — тайм-аут попытки завершения синхронизации в секундах. Значение по умолчанию — 10.

- Чтобы изменить параметры асинхронного импорта,

  задайте новые значения переменных, выполнив команду:

  ```
  sudo kubectl -n ptaf-backend set env deploy/ptaf-dc-syncer IMPORT_ASYNC_ENABLED=true
  CHECK_STATUS_ATTEMPTS=<Количество попыток завершения синхронизации>
  CHECK_STATUS_TIMEOUT=<Тайм-аут попытки завершения синхронизации в секундах>
  ```

  Например:

  ```
  sudo kubectl -n ptaf-backend set env deploy/ptaf-dc-syncer IMPORT_ASYNC_ENABLED=true
  CHECK_STATUS_ATTEMPTS=1000 CHECK_STATUS_TIMEOUT=60
  ```

- Чтобы выключить механизм асинхронного импорта,

  выполните команду:

  ```
  sudo kubectl -n ptaf-backend set env deploy/ptaf-dc-syncer IMPORT_ASYNC_ENABLED=false
  ```

15.19. Синхронизация объектов между экземплярами PT AF

Синхронизация объектов между экземплярами PT AF предполагает копирование объектов экземпляра-источника в экземпляр-приемник. С помощью синхронизации можно привести объекты экземпляров к общему виду, что обеспечивает наиболее эффективную защиту приложений в условиях распределения нагрузки между разными центрами обработки данных.

> **Внимание!** Перед настройкой синхронизации нужно убедиться, что на серверах синхронизируемых экземпляров установлены одинаковые версии PT AF.

К объектам синхронизации относятся:

- веб-приложения и их политики безопасности;
- шаблоны политик безопасности;
- действия с заголовками;
- пользовательские правила;
- пользовательские действия;
- глобальные списки IP-адресов;
- содержимое статических списков IP-адресов;
- конфигурации SSL;
- цепочки SSL-сертификатов УЦ;
- списки отозванных сертификатов;
- защищаемые серверы;
- ICAP-серверы;

— параметры декодирования HTTP-запросов и ответов;

— параметры отправки событий аудита на syslog-серверы.

Внимание! При удалении на стороне экземпляра-источника объекта синхронизации, использующегося в другом объекте на стороне экземпляра-приемника (например, при удалении защищаемого сервера, использующегося в профиле трафика), возникнет ошибка синхронизации.

Для настройки синхронизации объектов между экземплярами PT AF необходимо:

1. Назначить (см. раздел 15.19.1) один из экземпляров источником синхронизации.
2. Активировать (см. раздел 15.19.2) учетную запись синхронизации в веб-интерфейсе экземпляра-приемника.
3. Создать (см. раздел 15.19.1) экземпляр-приемник в веб-интерфейсе экземпляра-источника.
4. Выбрать (см. раздел 15.19.3) экземпляр для синхронизации.
5. Запустить синхронизацию вручную (см. раздел 15.19.4) или включить автоматическую синхронизацию (см. раздел 15.19.5) в веб-интерфейсе экземпляра-источника.

В этом разделе

Настройка экземпляров PT AF для синхронизации (см. раздел 15.19.1)

Управление учетной записью синхронизации (см. раздел 15.19.2)

Выбор экземпляров PT AF для синхронизации (см. раздел 15.19.3)

Управление состоянием синхронизации экземпляров (см. раздел 15.19.4)

Включение автоматической синхронизации (см. раздел 15.19.5)

15.19.1. Настройка экземпляров PT AF для синхронизации

При синхронизации объекты экземпляра-источника копируются в экземпляры-приемники.

Включение механизма синхронизации

► Чтобы включить механизм синхронизации,

выполните команды:

- на сервере экземпляра-источника:

```
kubectl -n ptaf-backend set env deployment/ptaf-conf-mgr-rest deployment/ptaf-auth-mgr
DC_CONFIG_SYNC_ENABLED=true FEATURE_MULTI_DC_ENABLED=true
```

- на сервере экземпляров-приемников:

```
kubectl -n ptaf-backend set env deployment/ptaf-conf-mgr-rest deployment/ptaf-auth-mgr
FEATURE_MULTI_DC_ENABLED=true
```

Создание экземпляра-приемника

Экземпляры-приемники необходимо создавать в веб-интерфейсе экземпляра-источника.

Перед созданием экземпляра-приемника необходимо активировать учетную запись синхронизации (см. раздел 15.19.2).

- Чтобы создать экземпляр-приемник:

  1. В веб-интерфейсе экземпляра-источника перейдите на страницу **Система** → **Экземпляры**.
  2. Нажмите +.
  3. Введите название экземпляра.
  4. Введите краткое название экземпляра (не более пяти символов).
  5. Отключите проверку TLS, если необходимо отказаться от проверки цепочки сертификатов экземпляра.
  6. Вставьте строку подключения, сгенерированную при активации учетной записи синхронизации (см. раздел 15.19.2) на стороне создаваемого экземпляра.

     Примечание. Вы можете проверить подключение создаваемого экземпляра к серверу по кнопке **Проверить соединение с сервером**. В дальнейшем статус подключения экземпляра к серверу будет отображаться в его строке в списке экземпляров.
  7. Нажмите **Создать**.

Изменение экземпляра-приемника

- Чтобы изменить экземпляр-приемник:

  1. В веб-интерфейсе экземпляра-источника перейдите на страницу **Система** → **Экземпляры**.
  2. В строке экземпляра нажмите →.
  3. Внесите изменения.
  4. Нажмите **Сохранить**.

Удаление экземпляра-приемника

- Чтобы удалить экземпляр-приемник:

  1. В веб-интерфейсе экземпляра-источника перейдите на страницу **Система** → **Экземпляры**.
  2. В строке экземпляра нажмите →.
  3. Нажмите **Удалить** и подтвердите удаление.

15.19.2. Управление учетной записью синхронизации

Каждый экземпляр-приемник имеет учетную запись синхронизации. Активация учетной записи включает синхронизацию экземпляра-приемника с экземпляром-источником, деактивация приводит к выключению синхронизации.

Управлять учетной записью синхронизации экземпляра-приемника можно на странице **Система** → **Учетная запись синхронизации**.

В этом разделе

Активация учетной записи (включение синхронизации) (см. раздел 15.19.2.1)

Генерация новой строки подключения (см. раздел 15.19.2.2)

Деактивация учетной записи (выключение синхронизации) (см. раздел 15.19.2.3)

15.19.2.1. Активация учетной записи (включение синхронизации)

Для включения синхронизации между экземплярами PT AF необходимо активировать учетную запись синхронизации в веб-интерфейсе экземпляра-приемника.

► Чтобы активировать учетную запись синхронизации:

1. В веб-интерфейсе экземпляра-приемника перейдите на страницу **Система** → **Учетная запись синхронизации**.
2. Активируйте учетную запись синхронизации.
3. Нажмите **Сгенерировать строку подключения** и подтвердите действие.
4. Нажмите **Скопировать**.

   Строка подключения сгенерирована и скопирована в буфер обмена.

   Внимание! Строку подключения можно скопировать только один раз после генерации. При утере строки подключения нужно будет сгенерировать ее заново.
5. Нажмите **Сохранить** и подтвердите действие.

Далее на стороне экземпляра источника создайте экземпляр-приемник (см. раздел 15.19.1) и в его параметрах укажите скопированную на шаге 4 строку подключения.

15.19.2.2. Генерация новой строки подключения

Вы можете сгенерировать новую строку подключения для синхронизации экземпляров, например, в рамках периодической смены паролей для обеспечения безопасности.

- Чтобы сгенерировать новую строку подключения:

  1. В веб-интерфейсе экземпляра-приемника перейдите на страницу **Система** → **Учетная запись синхронизации**.
  2. Нажмите **Сгенерировать строку подключения** и подтвердите действие.
  3. Нажмите **Скопировать**.

     Строка подключения сгенерирована и скопирована в буфер обмена.

     Внимание! Строку подключения можно скопировать только один раз после генерации. При утере строки подключения нужно будет сгенерировать ее заново.

  Далее на стороне-экземпляра-источника укажите новую строку подключения в параметрах экземпляра-приемника.

15.19.2.3. Деактивация учетной записи (выключение синхронизации)

При необходимости вы можете отключить синхронизацию объектов между экземплярами PT AF, для этого необходимо деактивировать учетную запись синхронизации в веб-интерфейсе экземпляра-приемника.

- Чтобы деактивировать учетную запись синхронизации:

  1. В веб-интерфейсе экземпляра-приемника перейдите на страницу **Система** → **Учетная запись синхронизации**.
  2. Деактивируйте учетную запись.
  3. Нажмите **Сохранить** и подтвердите действие.

  Учетная запись синхронизации деактивирована, синхронизация между текущим экземпляром-приемником и экземпляром-источником выключена.

15.19.3. Выбор экземпляров PT AF для синхронизации

Синхронизация выполняется в рамках одного изолированного пространства. Для настройки синхронизации в параметрах изолированного пространства необходимо выбрать экземпляры-приемники, для которых будет выполняться синхронизация.

- Чтобы выбрать экземпляры-приемники для синхронизации:

  1. В веб-интерфейсе экземпляра-источника в главном меню выберите **Система**.
  2. Выберите вкладку **Изолированные пространства**.
  3. В строке с названием изолированного пространства нажмите →.
  4. Нажмите ⟳.

5. В раскрывающемся списке выберите экземпляры PT AF для синхронизации параметров защиты.

   Если в списке нет нужного экземпляра, вы можете добавить его (см. раздел 15.19.1) по кнопке **Добавить**.

6. Нажмите **Сохранить**.

15.19.4. Управление состоянием синхронизации экземпляров

Вы можете просматривать состояние синхронизации экземпляров, а также управлять синхронизацией в веб-интерфейсе экземпляра-источника.

Запуск синхронизации

Перед запуском синхронизации необходимо учитывать следующее:

— Синхронизация выполняется в рамках изолированного пространства, из которого запускается. Таким образом, во всех экземплярах PT AF, для которых будет выполняться синхронизация, должно быть создано изолированное пространство (см. раздел 15.6) с одинаковым именем.

— При синхронизации выполняется полная замена всех синхронизируемых объектов экземпляра-приемника на объекты экземпляра-источника. Например, если до синхронизации в экземпляр-приемник были добавлены пользовательские правила, а в экземпляре-источнике их нет, после синхронизации пользовательские правила будут удалены.

— Если в экземпляре-приемнике есть синхронизируемый объект с таким же названием, как объект в экземпляре-источнике, при синхронизации объект не удалится, но его параметры будут заменены на те, которые указаны для объекта с таким же названием в экземпляре-источнике.

— При синхронизации глобальные списки копируются без содержащихся в них IP-адресов.

► Чтобы запустить синхронизацию параметров защиты между экземплярами:

1. Войдите в то изолированное пространство экземпляра-источника, в рамках которого необходимо выполнить синхронизацию.
2. Перейдите на страницу **Система** → **Состояние синхронизации**.
3. Выполните одно из действий:
   - Если вы хотите запустить синхронизацию параметров защиты между двумя экземплярами, в строке с названием экземпляра-приемника нажмите и подтвердите действие.

- Если вы хотите запустить синхронизацию параметров защиты между несколькими экземплярами, выберите экземпляры-приемники для синхронизации и нажмите **Синхронизировать**.

Примечание. Для обновления статусов синхронизации нажмите **Обновить статусы**.

Экспорт параметров защиты экземпляра

Если вы хотите посмотреть текущие параметры защиты экземпляра-приемника, вы можете экспортировать их.

- Чтобы экспортировать параметры защиты экземпляра-приемника:

  1. В веб-интерфейсе экземпляра-источника перейдите на страницу **Система** → **Состояние синхронизации**.
  2. В строке с названием экземпляра-приемника нажмите .

  JSON-файл с параметрами защиты экземпляра загружен на ваш компьютер.

15.19.5. Включение автоматической синхронизации

Вы можете включить автоматическую синхронизацию объектов между экземплярами PT AF. Перед этим в параметрах изолированного пространства необходимо выбрать экземпляры (см. раздел 15.19.3) PT AF, для которых будет выполняться синхронизация.

- Чтобы включить автоматическую синхронизацию:

  1. В веб-интерфейсе экземпляра-источника в главном меню выберите **Система**.
  2. Выберите вкладку **Изолированные пространства**.
  3. В строке с названием изолированного пространства нажмите .
  4. Нажмите .
  5. Включите автоматическую синхронизацию.
  6. Выберите единицу измерения для автоматической синхронизации.
  7. Введите период автоматической синхронизации.
  8. Нажмите **Сохранить**.

  Автоматическая синхронизация включена и выполняется с заданной периодичностью в рамках изолированного пространства. При необходимости вы можете запускать синхронизацию вручную (см. раздел 15.19.4).

15.20. Настройка декодирования запросов и ответов

Вы можете включить декодирование данных запросов и ответов. Включение декодирования позволяет записывать данные запросов и ответов в базу данных в декодированном виде, что упрощает работу с ними.

Настраивать декодирование запросов и ответов можно из базового изолированного пространства `general`. Если необходимо, чтобы администраторы других изолированных пространств могли самостоятельно включать и выключать декодирование, можно включить соответствующий параметр в изолированном пространстве `general`.

Вы можете управлять декодированием на странице **Система** → **Декодирование запросов и ответов**.

Включение декодирования

- Чтобы включить декодирование в изолированном пространстве `general`:

  1. Включите декодирование запросов и ответов.
  2. Если необходимо включить декодирование во всех изолированных пространствах, включите применение настраиваемых параметров декодирования для всех изолированных пространств.
  3. Если необходимо, измените возможность редактировать параметры декодирования для каждого изолированного пространства.

     Примечание. При включенном параметре декодирование будет включено во всех изолированных пространствах, но администраторы изолированных пространств смогут его отключить. При выключенном параметре администраторы изолированных пространств не смогут отключить декодирование.
  4. Нажмите **Сохранить**.

  Данные запросов и ответов записываются в базу данных и отображаются в карточках событий безопасности в декодированном виде. Функция декодирования недоступна в карточках событий безопасности.

Выключение декодирования

- Чтобы выключить декодирование в изолированном пространстве `general`:

  1. Выключите декодирование запросов и ответов.
  2. Если необходимо выключить декодирование во всех изолированных пространствах, включите применение настраиваемых параметров декодирования для всех изолированных пространств.
  3. Если необходимо, измените возможность редактировать параметры декодирования для каждого изолированного пространства.

Примечание. При включенном параметре декодирование будет выключено во всех изолированных пространствах, но администраторы изолированных пространств смогут его включить. При выключенном параметре администраторы изолированных пространств не смогут включить декодирование.

4. Нажмите **Сохранить**.

Запросы и ответы записываются в базу данных и отображаются в карточках событий безопасности в сжатом виде. Вы можете просматривать данные запросов и ответов в декодированном виде в веб-интерфейсе, используя функцию декодирования в карточках событий безопасности (см. раздел 13.4.2).

15.21. Тонкая настройка применения конфигурации

В разделе приведены инструкции для тонкой настройки применения конфигурации.

В этом разделе

Настройка механизма поэтапного применения конфигурации (см. раздел 15.21.1)

Настройка разделения подов на виртуальные группы (см. раздел 15.21.2)

Настройка механизма плавного завершения сессии (см. раздел 15.21.3)

15.21.1. Настройка механизма поэтапного применения конфигурации

Конфигурация ядра PT AF делится на следующие типы:

- **Серверная конфигурация.** Содержит параметры, связанные с управлением трафиком: параметры профилей трафика, защищаемых серверов, шифрования.
- **Динамическая конфигурация.** Содержит параметры действий и системных правил, идентификаторы глобальных списков, параметры и код пользовательских правил, общую информацию о приложении (идентификатор, название, режим защиты, защищаемые узлы и пути к их ресурсам, внешние IP-адреса и порты балансировщика).
- **Статическая конфигурация.** Содержит код системных правил и статические глобальные списки.

С версии 4.3.0 при изменении параметров PT AF новая конфигурация по умолчанию применяется поэтапно[28], без прерывания трафика. Система последовательно завершает работу подов с истекшими сессиями и вместо них создает поды с новой конфигурацией для обработки новых сессий. Вместе с тем механизм поэтапного применения конфигурации

28 В прежних версиях PT AF механизм поэтапного применения конфигурации по умолчанию был отключен.

увеличивает время применения конфигурации. Также он не исключает прерывание длительных сессий (например, связанных с загрузкой файлов большого размера) — при применении конфигурации такие сессии могут прерываться по тайм-ауту.

Вы можете изменить параметры механизма или вовсе его отключить. Отключение механизма ускорит применение серверной конфигурации, однако может привести к прерыванию трафика во время ее применения. Вместе с тем применение конфигурации, вызванное изменением системных правил в шаблонах политики безопасности, всегда выполняется бесшовно, «на лету».

> **Внимание!** Настройка механизма повлияет на применение конфигурации в каждом изолированном пространстве. Невозможно настроить механизм только для отдельного изолированного пространства.

Таблица 20. Параметры механизма поэтапного применения конфигурации

Параметр	Описание
`CORE_LIVENESS_INITIAL_DELAY_SECONDS`	Период в секундах между запуском пода и первой пробой работоспособности (Liveness Probe). Значение по умолчанию — `30`
`CORE_LIVENESS_PERIOD_SECONDS`	Период в секундах между пробами работоспособности (Liveness Probe). Значение по умолчанию — `10`
`CORE_READINESS_INITIAL_DELAY_SECONDS`	Период в секундах между запуском пода и первой пробой готовности (Readiness Probe). Значение по умолчанию — `10`
`CORE_READINESS_PERIOD_SECONDS`	Период в секундах между пробами готовности (Readiness Probe). Значение по умолчанию — `10`
`CORE_ROLLING_UPDATE_MAX_SURGE`	Количество дополнительных подов, которые будут запущены при поэтапном применении конфигурации ядра. Можно указать точное число дополнительных подов (например, `CORE_ROLLING_UPDATE_MAX_SURGE="2"`) или их количество в процентах от общего числа подов (например, `CORE_ROLLING_UPDATE_MAX_SURGE="10%"`). Значение по умолчанию — `0`
`CORE_ROLLING_UPDATE_MAX_UNAVAILABLE`	Количество подов, которые будут недоступны при поэтапном применении конфигурации ядра. Можно указать точное число подов (например, `CORE_ROLLING_UPDATE_MAX_UNAVAILABLE="2"`) или их количество в процентах от общего числа подов (например, `CORE_ROLLING_UPDATE_MAX_UNAVAILABLE="10%"`). Значение по умолчанию — `20%`
`DO_ROLLING_UPDATE_TO_APPLY_SERVER_CONFIG`	Выполнять ли поэтапное применение конфигурации ядра при изменении серверной конфигурации. Значение по умолчанию — `true` (выполнять)

Внимание! Значения по умолчанию уже оптимизированы производителем для стабильной работы механизма. Их изменение не рекомендуется, поскольку может привести к сбоям.

Настройка механизма

- Чтобы настроить механизм поэтапного применения конфигурации:

1. Укажите количество дополнительных подов, которые будут запущены при работе механизма, и (или) количество недоступных подов:

```
sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rpc
CORE_ROLLING_UPDATE_MAX_SURGE=<Количество дополнительных подов>
CORE_ROLLING_UPDATE_MAX_UNAVAILABLE=<Количество недоступных подов>
sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rest
CORE_ROLLING_UPDATE_MAX_SURGE=<Количество дополнительных подов>
CORE_ROLLING_UPDATE_MAX_UNAVAILABLE=<Количество недоступных подов>
```

   Внимание! Хотя бы один параметров `CORE_ROLLING_UPDATE_MAX_SURGE` и `CORE_ROLLING_UPDATE_MAX_UNAVAILABLE` должен быть не равен нулю.

2. Укажите периоды между пробами готовности и работоспособности пода:

```
kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rpc
CORE_LIVENESS_INITIAL_DELAY_SECONDS=<Период в секундах>
CORE_LIVENESS_PERIOD_SECONDS=<Период в секундах>
CORE_READINESS_INITIAL_DELAY_SECONDS=<Период в секундах>
CORE_READINESS_PERIOD_SECONDS=<Период в секундах>
kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rest
CORE_LIVENESS_INITIAL_DELAY_SECONDS=<Период в секундах>
CORE_LIVENESS_PERIOD_SECONDS=<Период в секундах>
CORE_READINESS_INITIAL_DELAY_SECONDS=<Период в секундах>
CORE_READINESS_PERIOD_SECONDS=<Период в секундах>
```

3. Проверьте статус развертывания новых подов:

```
sudo kubectl -n ptaf-backend rollout status deployments.apps ptaf-conf-mgr-rpc
sudo kubectl -n ptaf-backend rollout status deployments.apps ptaf-conf-mgr-rest
```

   После развертывания появятся сообщения:

```
deployment "ptaf-conf-mgr-rpc" successfully rolled out
deployment "ptaf-conf-mgr-rest" successfully rolled out
```

Отключение механизма

- Чтобы отключить механизм поэтапного применения конфигурации,

  выполните команды:

```
kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rpc
DO_ROLLING_UPDATE_TO_APPLY_SERVER_CONFIG=false
kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rest
DO_ROLLING_UPDATE_TO_APPLY_SERVER_CONFIG=false
```

При повторном включении механизма рекомендуется повторно указывать значения для всех параметров.

См. также

Особенности применения конфигурации в зависимости от количества подов (см. раздел 15.6.4)

15.21.2. Настройка разделения подов на виртуальные группы

По умолчанию бесшовное применение динамической конфигурация выполняется сразу на всех подах узла. Если конфигурация не может быть применена «на лету» (например, из-за ошибок или исключений), автоматически выполняется полная реконфигурация всех экземпляров ptaf-core, которая может прерывать обработку трафика.

Вы можете разделить поды одного узла на несколько виртуальных групп. В этом случае бесшовное применение выполняется одновременно только на одной группе подов, что всегда обеспечивает наличие работоспособных подов из других групп. Однако вместе с повышением надежности увеличивается и время бесшовного применения конфигурации.

Разделение на виртуальные группы повлияет на поды в каждом изолированном пространстве. Невозможно разделить поды только в отдельном изолированном пространстве.

- Чтобы разделить поды на виртуальные группы,

  выполните команды:

```
sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rpc
CORE_NODE_GROUPS_IN_RESOURCE_GROUP_TOTAL_COUNT=<Количество групп>
sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rest
CORE_NODE_GROUPS_IN_RESOURCE_GROUP_TOTAL_COUNT=<Количество групп>
```

15.21.3. Настройка механизма плавного завершения сессии

При применении конфигурации сервис ptaf-nginx по умолчанию закрывает соединения простым способом: разрывает их на уровне TCP (TCP FIN), предварительно не посылая ответ с HTTP-заголовком `Connection: close`. В некоторых случаях это может привести к проблемам в работе веб-приложений. Чтобы исключить эти проблемы, вы можете включить механизм плавного завершения сессии.

Ограничения механизма:

- Механизм поддерживается только для профилей трафика с внешним балансировщиком и контролем IP-адресов (см. раздел 8.2).
- Не поддерживается плавное завершение сессии на агентах, а также при обработке трафика на сервере Envoy.
- Не поддерживаются протоколы NTLM, SSL и PROXY.
- Не отслеживается статус применения конфигурации в Ingress.

— Если веб-приложения получают трафик через один и тот же прослушиваемый IP-адрес, PT AF добавит в запросы к каждому приложению все заголовки, указанные в карточках приложений в поле **Имя HTTP-заголовка**.

  Примечание. Имя HTTP-заголовка указывается только в тех случаях, когда перед PT AF находится внешний балансировщик или прокси-сервер и реальный IP-адрес клиента нужно получать из HTTP-заголовка.

— При включении, отключении или изменении механизма возможно появление временных проблем в обработке трафика: может прерываться обработка запросов, неверно определяться клиентский IP-адрес, а также некорректно заполняться заголовки, в которых передается клиентский IP-адрес. Вместе с тем корректная работа системы быстро восстанавливается после применения всех изменений. Если важно полностью исключить возможные сбои при обработке трафика, рекомендуется пустить трафик в обход PT AF на время переключения и настройки механизма.

— Не поддерживается сохранение регистра имен заголовков запросов с помощью параметра (см. раздел 15.7) `envoy_preserve_headers_case`: при использовании механизма плавного завершения сессии заголовки приводятся к нижнему регистру.

  Внимание! Настройка механизма повлияет на плавное завершение сессий в каждом изолированном пространстве. Невозможно настроить механизм только для отдельного изолированного пространства.

Таблица 21. Параметры механизма плавного завершения сессии

Параметр	Описание
`CLIENT_IP_HEADER_MODE`	Вариант модификации заголовка `X-Forwarded-For` при включении механизма: — `default` — включение механизма не влияет на модификацию заголовка. Является вариантом по умолчанию и не поддерживает Proxy Protocol. — `complete_address_list` — в заголовке передаются все IP-адреса в цепочке (как доверенные, так и недоверенные). — `trusted_address_list` — если в цепочке после IP-адреса клиента находятся только доверенные IP-адреса, передаются все адреса в цепочке. Если в цепочке находится хотя бы один недоверенный IP-адрес, передается последний недоверенный IP-адрес
`CORE_DELAY_BEFORE_SIGQUIT`	Задержка перед выполнением команды `nginx -s quit` (SIGQUIT) при получении сигнала на завершение процесса (SIGTERM). Значение по умолчанию — `10`
`CORE_GRACEFUL_SHUTDOWN_TIMEOUT`	Период, в течение которого под должен корректно завершить работу. Значение по умолчанию — `30`

Параметр	Описание
core_nginx_worker_shutdown_timeout	Тайм-аут, за который nginx после получения сигнала для завершения работы пода (SIGQUIT) ожидает завершения всех активных сессий. Параметр изменяется с помощью сценария traffic_settings.py (см. первый шаг инструкции по включению механизма) и не должен превышать значение CORE_GRACEFUL_SHUTDOWN_TIMEOUT. Значение по умолчанию — 30s
STATIC_INGRESS_CHECK_INTERVAL	Период между проверками состояния HTTP-соединения с серверами. Значение по умолчанию — 1s
STATIC_INGRESS_CHECK_TIMEOUT	Тайм-аут ожидания ответа от сервера при проверке HTTP-соединения. Значение по умолчанию — 2s
STATIC_INGRESS_GRACEFUL_TIMEOUT	Период, в течение которого HAProxy после получения сигнала выключения или перезагрузки ожидает завершения активных сессий. Значение по умолчанию — 60s
STATIC_INGRESS_HARD_STOP_TIMEOUT	Период, по завершении которого HAProxy после получения сигнала выключения или перезагрузки принудительно завершает работу. По истечении этого периода активные сессии принудительно закрываются. Значение по умолчанию — 70s
STATIC_INGRESS_TIMEOUT_TUNNEL	Тайм-аут для туннельных соединений. Значение по умолчанию — 10m
USE_INGRESS_FOR_STATIC_BALANCERS	Выполнять ли плавное завершение сессий. Значение по умолчанию — false (не выполнять)

Включение механизма

- Чтобы включить механизм плавного завершения сессии:

  1. Выполните команды:

     ```
     sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rpc
     USE_INGRESS_FOR_STATIC_BALANCERS=true CORE_GRACEFUL_SHUTDOWN_TIMEOUT=80
     sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rest
     USE_INGRESS_FOR_STATIC_BALANCERS=true CORE_GRACEFUL_SHUTDOWN_TIMEOUT=80
     sudo echo '{"core_nginx_worker_shutdown_timeout": "60s"}' | python3 /var/pt/ptaf-deploy/
     current/scripts/traffic_settings.py set
     ```

  2. Если требуется, измените другие параметры (см. таблицу 21):

     ```
     sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rpc <Название
     параметра>=<Значение параметра>
     sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rest <Название
     параметра>=<Значение параметра>
     ```

Отключение механизма

- Чтобы отключить механизм плавного завершения сессии,

  выполните команды:

  ```
  sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rpc
  USE_INGRESS_FOR_STATIC_BALANCERS=false
  sudo kubectl -n ptaf-backend set env deploy/ptaf-conf-mgr-rest
  USE_INGRESS_FOR_STATIC_BALANCERS=false
  ```

15.22. Настройка журналирования работы агента

- Чтобы настроить журналирование:

  1. На сервере агента установите утилиту logrotate:

     ```
     sudo apt-get install -y logrotate
     ```

  2. Создайте файл конфигурации `/etc/logrotate/nginx` с параметрами журналирования:

     ```
     /var/log/nginx/*.log {
       size <Максимальный размер файла журнала (G для гигабайтов, M для мегабайтов, k для
     килобайтов)>
       rotate <Максимальное количество сохраняемых файлов журналов>
       missingok
       compress
       delaycompress
       notifempty
       create 0640 nginx nginx
       sharedscripts
       postrotate [ ! -f /run/nginx.pid ] || kill -USR1 `cat /run/nginx.pid` endscript
       endscript
     }
     ```

     Например:

     ```
     sudo vi /etc/logrotate.d/nginx
     /var/log/nginx/*.log {
       size 200M
       rotate 5
       missingok
       compress
       delaycompress
       notifempty
       create 0640 nginx nginx
       sharedscripts
       postrotate [ ! -f /run/nginx.pid ] || kill -USR1 `cat /run/nginx.pid` endscript
     ```

```
    endscript
}
```

3. Запустите журналирование:
   ```
   sudo logrotate /etc/logrotate.d/nginx
   ```

Журналирование настроено.

15.23. Настройка отправки данных из журналов access.log и error.log во внешние SIEM-системы

Вы можете отправлять во внешние SIEM-системы данные о запросах к защищаемому серверу (access.log), а также данные о возникших на сервере ошибках (error.log). Данные собираются со всех узлов кластера и отправляются с помощью инструмента Fluent Bit.

Для сбора данных и отправки во внешнюю систему необходимо:

1. Включить Fluent Bit на всех узлах кластера.
2. Настроить Fluent Bit для подключения к внешней системе SIEM с помощью конфигурационной карты (ConfigMap).
3. Включить журналирование и отправку данных во внешнюю систему.

Включение Fluent Bit

- Чтобы включить Fluent Bit на всех узлах кластера,

  на базовом узле предварительной настройки кластера запустите сценарий установки PT AF со специальным ключом:

  - если PT AF установлен на Debian:
    ```
    sudo /var/pt/ptaf-deploy/current/install.sh --action=add_fluent_bit
    ```
  - если PT AF установлен на Astra Linux:
    ```
    sudo /var/pt/tmp/ptaf-deploy/install.sh --action=add_fluent_bit
    ```

  Fluent Bit включен на всех узлах кластера.

  Примечание. Вы можете изменять параметры Fluent Bit с помощью конфигурационной карты Kubernetes (ConfigMap).

Настройка отправки данных во внешнюю систему

- Чтобы настроить Fluent Bit на отправку данных из журналов access.log и error.log во внешнюю систему:

  1. Откройте ConfigMap для изменения параметров Fluent Bit:
     `sudo KUBE_EDITOR="nano" kubectl edit configmap -n ptaf-infra fluent-bit-cm`
  2. В секции `OUTPUT` укажите параметры подключения к внешней системе (подробное описание параметров см. на сайте docs.fluentbit.io).

     Примечание. Параметры секции `OUTPUT` зависят от используемого типа сервера для обработки трафика — nginx или Envoy. Примеры параметров секции приведены ниже.
  3. Перезапустите каждый под Fluent Bit с помощью команды:
     `sudo kubectl delete pod -n ptaf-infra fluent-bit-<Идентификатор пода Fluent Bit>`

Вы можете получить идентификаторы всех подов Fluent Bit, выполнив команду `sudo kubectl delete pod -n ptaf-infra fluent-bit-` и дважды нажав клавишу Tab. Также вы можете получить список всех существующих подов с помощью команды `kubectl get pods -n ptaf-infra`.

Пример параметров секции `OUTPUT` для отправки данных из журналов access.log или error.log (сервер nginx):

```
[OUTPUT]
    name                syslog
    match               *
    host                192.0.2.255
    port                514
    mode                tcp
    syslog_format       rfc5424
    syslog_maxsize      2048
    syslog_severity_key severity
    syslog_facility_key facility
    syslog_hostname_key hostname
    syslog_appname_key  appname
    syslog_procid_key   procid
    syslog_msgid_key    msgid
    syslog_sd_key       sd
    syslog_message_key  message
```

Пример параметров секции `OUTPUT` для отправки событий из журнала access.log (сервер Envoy):

Внимание! В параметре `match` необходимо указать значение `envoy.access`.

```
[OUTPUT]
    name                syslog
    match               envoy.access
    host                192.0.2.255
```

```
port                514
mode                tcp
syslog_format       rfc5424
syslog_maxsize      2048
syslog_severity_key severity
syslog_facility_key facility
syslog_hostname_key hostname
syslog_appname_key  appname
syslog_procid_key   procid
syslog_msgid_key    msgid
syslog_sd_key       sd
syslog_message_key  message
```

Пример параметров секции `OUTPUT` для отправки ошибок из журнала error.log (сервер Envoy):

Внимание! В параметре `match` необходимо указать значение `envoy.error`.

```
[OUTPUT]
    name                syslog
    match               envoy.error
    host                192.0.2.255
    port                514
    mode                tcp
    syslog_format       rfc5424
    syslog_maxsize      2048
    syslog_severity_key severity
    syslog_facility_key facility
    syslog_hostname_key hostname
    syslog_appname_key  appname
    syslog_procid_key   procid
    syslog_msgid_key    msgid
    syslog_sd_key       sd
    syslog_message_key  message
```

Включение журналирования событий и ошибок

- Чтобы включить запись событий в журнал access.log в изолированном пространстве на сервере nginx,

  выполните запрос к REST API:

```
PATCH <Корневой URL API>/config/traffic_settings
{
  "core_nginx_access_log": true
}
```

- Чтобы включить запись событий в журнал access.log в изолированном пространстве на сервере Envoy,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_envoy_access_log_enabled": true
  }
  ```

- Чтобы включить запись ошибок в журнал error.log в изолированном пространстве на сервере nginx,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_nginx_error_log_enabled": true
  }
  ```

  Примечание. На сервере Envoy запись ошибок в журнал error.log включена по умолчанию.

Изменение формата записи событий в журнал access.log

При необходимости вы можете изменить формат записи событий в журнал access.log с помощью запроса к REST API.

- Чтобы изменить формат записи на сервере nginx,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_nginx_access_log_format": <Формат записи событий>
  }
  ```

  Примечание. По умолчанию формат записи событий в журнал — `"$remote_addr - $remote_user [$time_local] \"$request\" $status $body_bytes_sent \"$http_referer\" \"$http_user_agent\""`. Подробное описание возможных значений см. на сайте nginx.org.

- Чтобы изменить формат записи на сервере Envoy,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_envoy_access_log_format": <Формат записи данных>
  }
  ```

  Примечание. По умолчанию формат записи данных в журнал — `"%DOWNSTREAM_REMOTE_ADDRESS_WITHOUT_PORT% - - [%START_TIME(%d/%b/%Y:%T %z)%] \"%REQ(:METHOD)% %REQ(X-ENVOY-ORIGINAL-PATH?:PATH)% %PROTOCOL%\" %RESPONSE_CODE% %BYTES_SENT% \"%REQ(REFERER)%\" \"%REQ(USER-AGENT)%\""`.

Изменение списка точек назначения для отправки ошибок из журнала error.log (сервер nginx)

При необходимости вы можете изменить список точек назначения для отправки ошибок из журнала error.log с помощью запроса к REST API.

- Чтобы изменить список точек назначения,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_nginx_error_log_endpoints": [<Список точек назначения>]
  }
  ```

  Внимание! По умолчанию для отправки ошибок из журнала error.log настроена точка назначения `"syslog:server=unix:/opt/shared/log.sock,facility=local7,tag=nginx error"`. Не изменяйте адрес сервера: `server=unix:/opt/shared/log.sock`, так как он указывает на точку сбора данных со всех подов ядра и требуется для отправки данных через Fluent Bit. Подробное описание возможных значений см. на сайте nginx.org.

Изменение формата записи ошибок в журнал error.log (сервер Envoy)

При необходимости вы можете изменить формат записи ошибок в журнал error.log на сервере Envoy с помощью запроса к REST API.

- Чтобы изменить формат записи на сервере Envoy,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_envoy_error_log_format": <Формат записи ошибок>
  }
  ```

  Примечание. По умолчанию формат записи ошибок в журнал error.log — `"core_envoy_error_log_format":"[%Y-%m-%d %T.%e][%t][%l][%n] [%g:%#] %v"`.

Отключение журналирования событий и ошибок

- Чтобы отключить запись событий в журнал access.log в изолированном пространстве на сервере nginx,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_nginx_access_log": false
  }
  ```

- Чтобы отключить запись событий в журнал access.log в изолированном пространстве на сервере Envoy,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_envoy_access_log_enabled": false
  }
  ```

- Чтобы отключить запись ошибок в журнал error.log в изолированном пространстве на сервере nginx,

  выполните запрос к REST API:

  ```
  PATCH <Корневой URL API>/config/traffic_settings
  {
    "core_nginx_error_log_enabled": false
  }
  ```

  Примечание. На сервере Envoy нельзя выключить запись ошибок в журнал error.log.

Отключение Fluent Bit

- Чтобы отключить Fluent Bit на всех узлах,

  на базовом узле предварительной настройки кластера запустите сценарий установки PT AF со специальным ключом:

  - если PT AF установлен на Debian:

    ```
    sudo /var/pt/ptaf-deploy/current/install.sh --action=remove_fluent_bit
    ```

  - если PT AF установлен на Astra Linux:

    ```
    sudo /var/pt/tmp/ptaf-deploy/install.sh --action=remove_fluent_bit
    ```

  Fluent Bit отключен на всех узлах кластера.

15.24. Отправка событий от агентов в SIEM-системы

Если для защиты приложений вы используете агенты, вы можете настроить отправку событий от агента PT AF в систему управления событиями информационной безопасности (в SIEM-систему).

Внимание! SIEM-система должна поддерживать прием сообщений от 65 КБ.

- Чтобы настроить отправку событий в SIEM-систему:

  1. Установите внешний сборщик данных Fluent Bit на сервере агента:

     - В виде deb-пакета — если агент установлен из deb-пакета, ISO-образа, Docker-образа или если в качестве агента установлен прокси-сервер envoy;

- В виде Helm Chart (см. раздел 15.24.2) — если агент установлен с помощью Ingress-контроллера.

2. Настройте агент (см. раздел 15.24.3).

В этом разделе

Установка Fluent Bit в виде deb-пакета (см. раздел 15.24.1)

Установка Fluent Bit в виде Helm Chart (см. раздел 15.24.2)

Настройка агента для отправки событий в SIEM-систему (см. раздел 15.24.3)

15.24.1. Установка Fluent Bit в виде deb-пакета

Установите Fluent Bit в виде deb-пакета, если агент установлен из deb-пакета, ISO-образа или Docker-образа.

Документацию по установке Fluent Bit можно найти на сайте производителя. Например, вы можете установить Fluent Bit с помощью скрипта:

```
export FLUENT_BIT_RELEASE_VERSION=2.2.2
curl https://raw.githubusercontent.com/fluent/fluent-bit/master/install.sh | sh
service fluent-bit start
```

После установки необходимо настроить конфигурацию Fluent Bit в файле `/etc/fluent-bit/fluent-bit.conf`. Это можно сделать одним из способов:

— **Без использования Storage.** Если лимит памяти для хранения чанков превышен, Fluent Bit перестанет принимать новые сообщения.

— **С использованием Storage.** Если лимит памяти для хранения чанков превышен, Fluent Bit будет записывать новые чанки на диск. При превышении максимального объема данных на диске будет выполняться ротация.

Настройка конфигурации без использования Storage

► Чтобы настроить конфигурацию Fluent Bit без использования Storage,

в файле `/etc/fluent-bit/fluent-bit.conf` отредактируйте секции `[INPUT]` и `[OUTPUT]`:

```
[INPUT]
    Name syslog
    Parser syslog-rfc5424
    Mode            tcp
    Listen          0.0.0.0
    Port            5140
    Buffer_Max_Size 64KB # Максимальный размер сообщения
    Buffer_Chunk_Size 15MB # Размер чанка с сообщениями (не должен быть меньше
максимального размера сообщения)
```

```
    Mem_Buf_Limit 300MB # Лимит памяти для хранения чанков, при превышении которого Fluent
Bit перестанет принимать новые сообщения
...
[OUTPUT]
    Name syslog
    syslog_format rfc5424
    syslog_maxsize 64KB # Максимальный размер сообщения
    Match *
    host {{ Адрес для отправки сообщений в SIEM-систему }}
    port {{ Порт для отправки сообщений в SIEM-систему }}
    mode {{ Протокол для отправки сообщений в SIEM-систему (tcp или udp)}}
    syslog_severity_preset 6
    syslog_facility_preset 16
    syslog_hostname_key host
    syslog_appname_key ident
    syslog_procid_key pid
    syslog_msgid_key msgid
    syslog_message_key message
    Retry_Limit False # Максимальное количество попыток отправки сообщения при
недоступности SIEM-системы (False — бесконечно)
```

Настройка конфигурации с использованием Storage

- Чтобы настроить конфигурацию Fluent Bit с использованием Storage,

  в файле `/etc/fluent-bit/fluent-bit.conf` отредактируйте секции `[SERVICE]`, `[INPUT]`, `[OUTPUT]`:

```
[SERVICE]
    flush          1
    daemon         Off
    log_level      info
    parsers_file   parsers.conf
    plugins_file   plugins.conf
    http_server    Off
    http_listen    0.0.0.0
    http_port      2020
    storage.metrics off
    storage.max_chunks_up 50 # Количество чанков в оперативной памяти. При его превышении
чанки будут записываться на диск
    storage.path /var/log/flb-storage/ # Путь, по которому будут сохраняться чанки
    storage.checksum on
    storage.backlog.mem_limit 15M # Объем памяти, занимаемый чанками при их возвращении с
диска в память. Должен быть не меньше, чем значение Buffer_Chunk_Size в секции INPUT
...
[INPUT]
    Name syslog
    Parser syslog-rfc5424
    Mode           tcp
    Listen         0.0.0.0
```

```
    Port           5140
    Buffer_Max_Size 64KB # Максимальный размер сообщения
    Buffer_Chunk_Size 15MB # Размер чанка с сообщениями (не должен быть меньше
максимального размера сообщения)
    storage.type filesystem
...
[OUTPUT]
    Name syslog
    syslog_format rfc5424
    syslog_maxsize 64KB # Максимальный размер сообщения
    Match *
    host {{ Адрес для отправки сообщений в SIEM-систему }}
    port {{ Порт для отправки сообщений в SIEM-систему }}
    mode {{ Протокол для отправки сообщений в SIEM-систему (tcp или udp)}}
    syslog_severity_preset 6
    syslog_facility_preset 16
    syslog_hostname_key host
    syslog_appname_key ident
    syslog_procid_key pid
    syslog_msgid_key msgid
    syslog_message_key message
    storage.total_limit_size 3000MB # Максимальный объем сохраняемых на диск данных (при
превышении будет выполняться ротация)
    Retry_Limit False # Максимальное количество попыток отправки сообщения при
недоступности SIEM-системы (False - бесконечно)
```

15.24.2. Установка Fluent Bit в виде Helm Chart

Установите Fluent Bit в виду Helm Chart, если агент установлен с помощью Ingress-контроллера.

- Чтобы установить Fluent Bit в виде Helm Chart для Kubernetes:

  1. Скачайте файл `values.yaml` и укажите в нем параметры, приведенные ниже, одним из способов:

     - Без использования Storage — если лимит памяти для хранения чанков превышен, Fluent Bit перестанет принимать новые сообщения.
     - С использованием Storage — если лимит памяти для хранения чанков превышен, Fluent Bit будет записывать новые чанки на диск. При превышении максимального объема данных на диске будет выполняться ротация.

     Остальные параметры в файле указываются в соответствии с требованиями конкретной инфраструктуры.

  2. Установите Fluent Bit.

Настройка конфигурации без использования Storage

- Чтобы настроить конфигурацию Fluent Bit без использования Storage,

  в файле `values.yaml` укажите параметры:

```
kind: Deployment
config:
    service: |
      [SERVICE]
        daemon Off
        flush 1
        log_level info
        parsers_File parsers.conf
        plugins_File plugins.conf
        http_Server Off
        http_Listen 0.0.0.0
        http_Port 2020
        storage.metrics on
## https://docs.fluentbit.io/manual/pipeline/inputs
    inputs: |
      [INPUT]
        Name syslog
        Parser syslog-rfc5424
        Mode tcp
        Listen 0.0.0.0
        Port 5140
        Buffer_Max_Size 128KB # Максимальный размер сообщения
        Buffer_Chunk_Size 15MB # Размер чанка с сообщениями (не должен быть меньше
максимального размера сообщения)
        Mem_Buf_Limit 300MB # Лимит памяти для хранения чанков, при превышении которого
Fluent Bit перестанет принимать новые сообщения
## https://docs.fluentbit.io/manual/pipeline/outputs
    outputs: |
      [OUTPUT]
        name syslog
        syslog_format rfc5424
        Match *
        host {{ Адрес для отправки сообщений в SIEM-систему }}
    port {{ Порт для отправки сообщений в SIEM-систему }}
        mode {{ Протокол для отправки сообщений в SIEM (tcp или udp)}}
        syslog_severity_preset 6
        syslog_facility_preset 16
        syslog_hostname_key host
        syslog_appname_key ident
        syslog_procid_key pid
        syslog_msgid_key msgid
        syslog_message_key message
        Retry_Limit False # Максимальное количество попыток отправки сообщения при
недоступности SIEM-системы (False - бесконечно)
```

```
extraPorts:
    - port: 5140
    containerPort: 5140
    protocol: TCP
    name: tcp
    # nodePort: {{ .nodePort }} # Раскомментировать, если используется сервис типа
nodePort
resources:
    limits:
    cpu: 100m
    memory: {{ (Mem_Buf_Limit + 30m) или (storage.max_chunks_up * Buffer_Chunk_Size +
30m), в зависимости от того, используется ли Storage }}
requests:
    cpu: 100m
    memory: {{ (Mem_Buf_Limit + 30m) или (storage.max_chunks_up * Buffer_Chunk_Size +
30m), в зависимости от того, используется ли Storage }}
```

Настройка конфигурации с использованием Storage

- Чтобы настроить конфигурацию Fluent Bit с использованием Storage,

  в файле `values.yaml` укажите параметры:

```
kind: Deployment
config:
    service: |
      [SERVICE]
        flush 1
        daemon Off
        log_level info
        parsers_file parsers.conf
        plugins_file plugins.conf
        http_server Off
        http_listen 0.0.0.0
        http_port 2020
        storage.metrics off
        storage.max_chunks_up 50 # Количество чанков в оперативной памяти. При его
превышении чанки будут записываться на диск
        storage.path /var/log/flb-storage/ # Путь, по которому будут сохраняться чанки
        storage.checksum on
        storage.backlog.mem_limit 15M # Объем памяти, занимаемый чанками при их
возвращении с диска в память. Должен быть не меньше, чем значение Buffer_Chunk_Size в
секции INPUT
## https://docs.fluentbit.io/manual/pipeline/inputs
    inputs: |
      [INPUT]
        Name syslog
        Parser syslog-rfc5424
        Mode tcp
        Listen 0.0.0.0
        Port 5140
```

```
        Buffer_Max_Size 128KB # Максимальный размер сообщения
    Buffer_Chunk_Size 15MB # Размер чанка с сообщениями (не должен быть меньше
максимального размера сообщения)
        storage.type filesystem
## https://docs.fluentbit.io/manual/pipeline/outputs
    outputs: |
      [OUTPUT]
        Name syslog
        syslog_format rfc5424
        host {{ Адрес для отправки сообщений в SIEM }}
        port {{ Порт для отправки сообщений в SIEM }}
        mode {{ Протокол для отправки сообщений в SIEM (tcp или udp)}}
        syslog_severity_preset 6
        syslog_facility_preset 16
        syslog_hostname_key host
        syslog_appname_key ident
        syslog_procid_key pid
        syslog_msgid_key msgid
        syslog_message_key message
        storage.total_limit_size 3000MB # Максимальный объем сохраняемых на диск данных
(при превышении будет выполняться ротация)
        Retry_Limit False # Максимальное количество попыток отправки сообщения при
недоступности SIEM (False - бесконечно)
extraPorts:
    - port: 5140
    containerPort: 5140
    protocol: TCP
    name: tcp
    # nodePort: {{ .nodePort }} # Раскомментировать, если используется сервис типа
nodePort
resources:
    limits:
        cpu: 100m
        memory: {{ (Mem_Buf_Limit + 30m) или (storage.max_chunks_up * Buffer_Chunk_Size +
30m), в зависимости от того, используется ли Storage }}
    requests:
        cpu: 100m
        memory: {{ (Mem_Buf_Limit + 30m) или (storage.max_chunks_up * Buffer_Chunk_Size +
30m), в зависимости от того, используется ли Storage }}
```

Установка Fluent Bit

- Чтобы установить Fluent Bit,

  выполните команду:

```
sudo helm repo add fluent https://fluent.github.io/helm-charts
sudo helm install fluent-bit fluent/fluent-bit --values values.yaml --version 0.44.0
```

15.24.3. Настройка агента для отправки событий в SIEM-систему

Способ настройки агента для отправки событий в SIEM-систему зависит от способа установки Fluent Bit. Настройка предполагает задание в конфигурационном файле переменных окружения, в соответствии с которыми события будут отправляться в SIEM-систему.

Настройка агента, если Fluent Bit установлен в виде deb-пакета

Агент установлен из deb-пакета или ISO-образа

- Чтобы настроить агент:

1. В файле `/lib/systemd/system/ptafd.service` в секции `[Service]` задайте переменные окружения:

```
[Service]
Environment="EVENT_SENDER_ENABLED=1"
Environment="EVENT_SENDER_HOST=<IP-адрес для отправки сообщений в Fluent Bit>"
Environment="EVENT_SENDER_PORT=<Порт для отправки сообщений в Fluent Bit>"
Environment="EVENT_SENDER_TIMEOUT=3"
Environment="EVENT_WEB_UI_URL=http[s]://[адрес_WebUI]/events/attacks/%s/general/;
ExecStartPre=mkdir -p /run/ptaf/ptafd
ExecStart=/opt/ptaf/bin/ptafd
Restart=always
```

2. Выполните команду:

```
sudo systemctl daemon-reload
```

3. Перезапустите службу ptafd:

```
sudo systemctl restart ptafd
```

4. Перезапустите nginx:

```
sudo systemctl restart nginx
```

Агент установлен из Docker-образа

- Чтобы настроить агент:

1. В файле `compose.yml` в секции `environment` задайте переменные окружения:

```
- EVENT_SENDER_ENABLED=1
- EVENT_SENDER_HOST=<IP-адрес для отправки сообщений в Fluent Bit>
- EVENT_SENDER_PORT=<Порт для отправки сообщений в Fluent Bit>
- EVENT_SENDER_TIMEOUT=3
- EVENT_WEB_UI_URL=http[s]://[адрес_WebUI]/events/attacks/%s/general/
```

2. Перезапустите Docker Compose:

```
sudo docker compose up
```

Настройка агента, если Fluent Bit установлен в виде Helm Chart

- Чтобы настроить агент:

  1. В файле `values.yaml` в секции `ptaf` → `env` задайте переменные окружения:

     ```
     name: EVENT_SENDER_ENABLED
     value: 1
     name: EVENT_SENDER_HOST
     value: {{ IP-адрес для отправки сообщений в Fluent Bit }}
     name: EVENT_SENDER_PORT
     value: {{ Порт для отправки сообщений в Fluent Bit }}
     name: EVENT_WEB_UI_URL
     value: "http[s]://[адрес_WebUI]/events/attacks/%s/general"
     ```

  2. Выполните команду:

     ```
     sudo helm upgrade
     ```

Описание переменных окружения для отправки событий в SIEM-системы

Таблица 22. Переменные окружения для настройки отправки событий в SIEM-системы

Переменная для настройки агента, установленного из deb-пакета, ISO-образа или с помощью Ingress-контроллера	Переменная для настройки агента, установленного из Docker-образа	Описание	Тип и возможные значения	Значение по умолчанию
`EVENT_SENDER_ENABLED`	`EVENT_SENDER_ENABLED`	Отправка событий во внешний сборщик	Булево значение: — 1 — отправка включена; — 0 — отправка выключена	`0`
`EVENT_SENDER_HOST`	`EVENT_SENDER_HOST`	Адрес узла внешнего сборщика для отправки событий	Строка: IP-адрес или имя узла	`localhost`

Переменная для настройки агента, установленного из deb-пакета, ISO-образа или с помощью Ingress-контроллера	Переменная для настройки агента, установленного из Docker-образа	Описание	Тип и возможные значения	Значение по умолчанию
`EVENT_SENDER_PORT`	`EVENT_SENDER_PORT`	Порт для отправки событий во внешний сборщик	Целое число:от 0 до 65 535	`5140`
`EVENT_SENDER_TIMEOUT`	`EVENT_SENDER_TIMEOUT`	Тайм-аут на отправку событий в секунду	Целое число: 0..INT_MAX (2^{31}-1)	`3`
`EVENT_WEB_UI_URL`	`EVENT_WEB_UI_URL`	Шаблон для задания URL, по которому в интерфейсе PT AF доступны данные о событии безопасности	Строка `http[s]://адрес_WebUI/events/attacks/%s/general`	—

15.25. Обновление базы GeoIP для агента

Чтобы PT AF мог корректно определять географическое расположение пользователей по их IP-адресам, необходимо периодически обновлять базу GeoIP для агента.

Для обновления базы GeoIP потребуется скачать файл формата MMDB с актуальной базой, например на сайте ГРЧЦ. Файл необходимо загрузить на сервер с агентом.

Процесс обновления базы GeoIP зависит от способа установки агента.

В этом разделе

Агент установлен из deb-пакета или ISO-образа (см. раздел 15.25.1)

Агент установлен из Docker-образа (см. раздел 15.25.2)

15.25.1. Агент установлен из deb-пакета или ISO-образа

Для обновления базы GeoIP на сервере агента необходимы права `root` или `sudo`.

Внимание! Для обновления базы GeoIP потребуется перезапустить сервис ptaf-nginx, что приведет к кратковременному прерыванию обработки трафика. Рекомендуется обновлять базу GeoIP в технологическое окно.

- Чтобы обновить базу GeoIP:

  1. Создайте резервную копию текущей базы GeoIP:

     ```
     sudo cp /<Путь до файла с текущей базой>/<Имя файла с текущей базой>.mmdb{,.bak}
     ```

     Например:

     ```
     sudo cp /opt/ptaf/data/GeoLite2-City.mmdb{,.bak}
     ```

  2. Замените файл с текущей базой GeoIP на новый:

     ```
     sudo cp <Имя файла с новой базой>.mmdb /<Путь до файла с текущей базой>/<Имя файла с текущей базой>.mmdb
     ```

     Например:

     ```
     sudo cp RU-GeoIP-City.mmdb /opt/ptaf/data/GeoLite2-City.mmdb
     ```

  3. Перезапустите сервисы обработки трафика:

     ```
     sudo systemctl restart ptafd ptaf-nginx ptaf-core-ctl
     ```

  База GeoIP обновлена. Запросы обрабатываются с учетом новой базы.

15.25.2. Агент установлен из Docker-образа

Процесс обновления базы GeoIP зависит от способа запуска контейнера.

Внимание! Для обновления базы GeoIP потребуется пересоздать контейнер агента, что приведет к кратковременному прерыванию обработки трафика. Рекомендуется обновлять базу GeoIP в технологическое окно.

Контейнер запускается с помощью docker compose

- Чтобы обновить базу GeoIP:

  1. В файле `docker-compose.yml` в секцию `volumes` добавьте строку для подмены базы в режиме «только чтение» (`:ro`):

     ```
     services:
       ptaf-agent:
         image: ptaf-agent:...
         volumes:
           - /<Путь до файла с новой базой>/<Имя файла с новой базой>.mmdb:/<Путь до файла с текущей базой>/<Имя файла с текущей базой>.mmdb:ro
     ```

     Например:

     ```
     services:
       ptaf-agent:
         image: ptaf-agent:...
     ```

```
volumes:
  - /opt/ptaf-data/RU-GeoIP-City.mmdb:/opt/ptaf/data/GeoLite2-City.mmdb:ro
```

2. Примените изменения и пересоздайте контейнер:
   ```
   sudo docker compose up -d --force-recreate
   ```

База GeoIP обновлена. Запросы обрабатываются с учетом новой базы.

Контейнер запускается с помощью docker run

- Чтобы обновить базу GeoIP:

  1. Остановите текущий работающий контейнер агента:
     ```
     sudo docker stop <Имя контейнера>
     ```
  2. Удалите контейнер:
     ```
     sudo docker rm <Имя контейнера>
     ```
  3. Запустите контейнер заново, добавив в команду запуска флаг `-v`:
     ```
     sudo docker run -d \
       --name <Имя контейнера> \
       -v /<Путь до файла с новой базой>/<Имя файла с новой базой>.mmdb:/<Путь до файла с текущей базой>/<Имя файла с текущей базой>.mmdb:ro \
       [Другие параметры запуска] \
       <Имя Docker-образа>
     ```

     Например:
     ```
     sudo docker run -d \
       --name < ptaf-agent> \
       -v /opt/ptaf-data/RU-GeoIP-City.mmdb:/opt/ptaf/data/GeoLite2-City.mmdb:ro \
       [Другие параметры запуска контейнера] \
       ptaf-core-nginx-agent:release-4.3.1.466071-debian-bullseye-nginx-1.30.2
     ```

  База GeoIP обновлена. Запросы обрабатываются с учетом новой базы.

15.26. Изменение списка NTP-серверов

Вы можете изменить список NTP-серверов после установки PT AF с помощью файла конфигурации `chrony.conf`.

- Чтобы изменить список NTP-серверов:

  1. Откройте файл `chrony.conf`:
     ```
     sudo nano /etc/chrony/chrony.conf
     ```
  2. Измените пул NTP-серверов:

     - Если нужно изменить существующий NTP-сервер или пул, отредактируйте соответствующую строку.

- Если нужно добавить новый NTP-сервер или пул, добавьте его в конец списка. Например:

```
## Старые пулы NTP-серверов
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 3.debian.pool.ntp.org iburst


## Новый дополнительный NTP-сервер или пул
pool ntp1.vniiftri.ru iburst
server ntp2.vniiftri.ru iburst


# This directive specify the location of the file containing ID/key pairs for
# NTP authentication.
keyfile /etc/chrony/chrony.keys
```

3. Сохраните изменения и перезапустите сервис chrony:

```
sudo systemctl restart chrony
```

4. Проверьте наличие изменений и синхронизацию NTP-серверов:

```
chronyc sources
sudo timedatectl status
```

15.27. Скрытие информации о версии nginx из сообщения об ошибке

При обработке трафика агентом в сообщении об ошибке, возвращаемой клиенту, может содержаться версия nginx. Во избежание утечки чувствительных данных вы можете скрыть ее.

За отображение версии nginx в сообщении об ошибке отвечает параметр `server_tokens`, который можно задать в конфигурационном файле во время установки агента. Также вы можете задать этот параметр после установки агента.

Агент установлен из deb-пакета, ISO-образа или Docker-образа

- Чтобы скрыть версию nginx из сообщения об ошибке,

  в файле `nginx.conf` в секцию `http` добавьте параметр `server_tokens` со значением `off`.

  Примечание. Если агент установлен из Docker-образа и файл конфигурации nginx был создан автоматически на основе переменных окружения, указанных в файле `compose.yaml`, отображение версии nginx в сообщении об ошибке отключено по умолчанию. Подробнее о способах создания файла конфигурации nginx при установке агента из Docker-образа см. в разделе «Установка агента из Docker-образа».

Агент установлен с помощью Ingress-контроллера

- Чтобы скрыть версию nginx из сообщения об ошибке:

  1. В папке распакованного пакета Helm найдите файл `ingress-nginx-helm-chart-<Номер версии>/templates/controller-configmap.yaml` и внесите в него следующие изменения:

     - В секцию `http` добавьте параметр `server_tokens` со значением `off`:

     ```
     http {
         `}}
             ptaf_config {{ .Values.ptaf.connect_string }}
         {{`
             include /etc/nginx/mime.types;
             default_type application/octet-stream;
             server_tokens off;
             {{- if .HTTPSnippets}}
     ```

     - В секции `http` → `server`. найдите строку `server_tokens "{{.ServerTokens}}";` и замените ее на `server_tokens off;`.

  2. Выполните команду:

     ```
     sudo helm upgrade ptaf-helmchart nginx-ingress/ --namespace <Пространство имен защищаемого приложения> f ingress-nginx-helm-chart-<Номер версии>/values.yaml
     ```

  3. Для каждого приложения в файл `ingress_<Идентификатор приложения>.yaml` в секцию `annotations` добавьте параметр `nginx.org/server-tokens` со значением `False`:

     ```
     apiVersion: networking.k8s.io/v1
     kind: Ingress
     metadata:
       name: <Название приложения>
       namespace: <Пространство имен защищаемого веб-приложения>
       annotations:
         nginx.org/server-tokens: "False"
     spec:
     ...
     ```

  4. Примените изменения для каждого файла `ingress_<Идентификатор приложения>.yaml`:

     ```
     sudo kubectl apply -f ingress_<Идентификатор приложения>.yaml
     ```

16. Интеграция PT AF с Grafana

Grafana — система для визуализации данных. Grafana отображает информацию в удобном для анализа виде и может использоваться для мониторинга работы PT AF.

Для интеграции необходимо установить Grafana на узлы PT AF. Вы можете установить Grafana при установке PT AF или позднее. Если развернута кластерная конфигурация PT AF, установка Grafana выполняется на узле предварительной настройки кластера.

В этом разделе

Установка Grafana (см. раздел 16.1)

Смена сертификата для веб-интерфейса Grafana (см. раздел 16.2)

Настройка передачи данных о работе PT AF на отдельный сервер с Grafana (см. раздел 16.3)

16.1. Установка Grafana

- Чтобы установить Grafana,

  выполните команду:

  ```
  sudo /var/pt/infra/current/deploy.sh --action=add_monitoring
  ```

После установки веб-интерфейс Grafana будет доступен по IP-адресу и порту, указанным в процессе развертывания PT AF при настройке виртуальных IP-адресов с помощью команды WSC `vip set monitoring` (по умолчанию используется порт 3000). Кроме того, вместо IP-адреса вы можете вводить FQDN, если между ними настроено соответствие в DNS.

Для первого входа необходимо ввести логин `admin` и пароль `admin`. После входа вам потребуется сменить пароль. Веб-интерфейс Grafana содержит предварительно настроенные дашборды для мониторинга работы PT AF и операционной системы.

16.2. Смена сертификата для веб-интерфейса Grafana

При установке Grafana для ее веб-интерфейса автоматически устанавливается самоподписанный сертификат. Также при обновлении PT AF на версию 4.5.0 сертификат Grafana удаляется. Поэтому при попытке подключения к веб-интерфейсу Grafana вы получите предупреждение о том, что подключение не защищено.

Вы можете заменить сертификат для веб-интерфейса Grafana. Для этого вам понадобятся файлы нового сертификата и закрытого ключа.

► Чтобы заменить сертификат для веб-интерфейса Grafana:

1. Скопируйте файлы закрытого ключа и сертификата:
   ```
   sudo cp <Имя файла сертификата> tls.crt
   sudo cp <Имя файла закрытого ключа> tls.key
   ```
2. Сохраните резервную копию существующего секрета:
   ```
   kubectl -n ptaf-infra get secret grafana-certs -o yaml > grafana-certs-old.yaml
   ```
3. Удалите существующий секрет из кластера:
   ```
   kubectl -n ptaf-infra delete secret grafana-certs
   ```
4. Создайте новый секрет:
   ```
   sudo kubectl -n ptaf-infra create secret tls grafana-certs --cert=tls.crt --key=tls.key
   ```
5. Перезапустите под:
   ```
   for pod in `kubectl -n ptaf-infra get pod -o custom-columns=:.metadata.name |grep grafana`; do kubectl -n ptaf-infra delete pod $pod; done
   ```

   Сертификат для веб-интерфейса Grafana заменен. Вы можете удалить резервную копию секрета, сохраненную на шаге 2.

16.3. Настройка передачи данных о работе PT AF на отдельный сервер с Grafana

Отдельный сервер с Grafana может использоваться для мониторинга работы всех информационных систем организации, в том числе и для мониторинга работы PT AF.

Для получения данных от PT AF необходимо указать в параметрах конфигурации системы Grafana, установленной на отдельном сервере, следующие адреса в качестве источников данных:

— `https://<IP-адрес или FQDN для доступа к веб-интерфейсу Grafana, установленной на сервере PT AF>:<Порт>/api/datasources/proxy/1` — для подключения к VictoriaMetrics;

— `https://<IP-адрес или FQDN для доступа к веб-интерфейсу Grafana, установленной на сервере PT AF>:<Порт>/api/datasources/proxy/2` — для подключения к Grafana Loki.

В качестве учетных данных для входа необходимо указать логин и пароль, которые используются для входа в систему Grafana, установленную на узлах PT AF.

17. Решение проблем

Этот раздел содержит информацию для решения проблем при работе PT AF.

В этом разделе

Просмотр информации о системе PT AF (см. раздел 17.1)

Проблемы, связанные с лицензиями (см. раздел 17.2)

Ошибки при установке PT AF (см. раздел 17.3)

Не переименовались сетевые интерфейсы (см. раздел 17.4)

Метрики для мониторинга работы PT AF (см. раздел 17.5)

Ошибка при обновлении узла PT AF (см. раздел 17.6)

Не запускается под после обновления (см. раздел 17.7)

Не отправляются события на syslog-сервер после обновления Docker-агента (см. раздел 17.8)

На схеме конфигурации не отображается сервер и профиль обработки трафика (см. раздел 17.9)

Ошибка восстановления из резервной копии (см. раздел 17.10)

Исключение узла из обработки трафика (см. раздел 17.11)

Особенности маршрутизации исходящего трафика (см. раздел 17.12)

Проблема подключения агента (см. раздел 17.13)

Сбор системных журналов (см. раздел 17.14)

17.1. Просмотр информации о системе PT AF

Вы можете просмотреть версии компонентов системы, лицензионное соглашение с конечным пользователем ПО и параметры лицензии, в настоящий момент активированной в PT AF. Информация о версиях компонентов может понадобиться при обращении в службу технической поддержки Positive Technologies.

Примечание. Также версия системы отображается на странице входа в PT AF.

- Чтобы просмотреть информацию о системе PT AF:

  1. В главном меню нажмите ? и в раскрывшемся меню выберите пункт **О продукте**.

     Откроется карточка с информацией об активной лицензии и версиях используемых компонентов.

  2. Если вам необходимо просмотреть подробную информацию о лицензии, в строке **Номер** нажмите →.

Откроется карточка с информацией о лицензии.

3. Если вам необходимо просмотреть лицензионное соглашение, нажмите ссылку **Пользовательское соглашение**.

   Лицензионное соглашение откроется в формате PDF.

17.2. Проблемы, связанные с лицензиями

Могут возникнуть ситуации, когда работа системы PT AF нарушена или ограничена из-за проблем с лицензиями.

Таблица 23. Ошибки, связанные с лицензиями

Сообщение в веб-интерфейсе PT AF	Проблема	Решение
Нет лицензии	Не удается продолжить работу с веб-интерфейсом после входа в систему или активировать загруженную лицензию. Вы не загрузили лицензию или ваша лицензия недействительна, поэтому использование системы невозможно	Загрузите лицензию и активируйте ее
Лицензия истекла	Срок действия лицензии истек, в PT AF нет активированных лицензий. Использование системы невозможно	Активируйте загруженную лицензию или загрузите новую лицензию и активируйте ее. В случае отсутствия новой лицензии обратитесь к производителю
Произошла ошибка	Не удается подключиться к лицензии. Лицензия удалена, токен принадлежит серверу с другими аппаратными характеристиками или происходит загрузка и активация новой лицензии	Перезагрузите страницу или восстановите активную лицензию
Внутренняя ошибка лицензии	Не удается подключить лицензию. Произошла внутренняя ошибка	Обратитесь в службу технической поддержки

17.3. Ошибки при установке PT AF

В этом разделе описаны возможные ошибки при установке PT AF и варианты их решения.

Таблица 24. Ошибки при установке PT AF

Сообщение в командной строке	Проблема	Решение

`TASK [system_checks : Ensure that there if enough CPU cores] ******************`
 	
`fatal: [oblivion.local]: FAILED! => {`
 	
`"assertion": "ansible_processor_vcpus >= 6 or not set_resources_requests|bool",`
 	
`"changed": false,`
 	
`"evaluated_to": false`
 	
`}`
	Количество ядер центрального процессора не соответствует минимальным требованиям	Перед установкой продукта убедитесь, что соблюдены аппаратные и программные требования (см. раздел 4)

`TASK [system_checks : Ensure that there is enough memory] *********************`
 	
`fatal: [ptaf4.local]: FAILED! => {`
 	
`"assertion": "ansible_memory_mb.real.total >= 8000 or not set_resources_requests|bool",`
 	
`"changed": false,`
 	
`"evaluated_to": false`
 	
`}`
	ОЗУ не соответствует минимальным требованиям	Перед установкой продукта убедитесь, что соблюдены аппаратные и программные требования (см. раздел 4)

`TASK [system_packages : Standard debian packages | Install] ******************`
 	
`fatal: [ptaf4.local]: FAILED! => {`
 	
`"cache_update_time": 1726873677,`
 	
`"cache_updated": false,`
 	
`"changed": false,`
 	
`"rc": 100`
 	
`}`
	Версия компонентов ОС выше, чем требуется	Заново выполните одно из действий:
		— Установите ОС из ISO-образа.
		— Импортируйте виртуальную машину из OVA-образа.
		— Создайте и настройте виртуальную машину на основе COW2-образа.

Сообщение в командной строке	Проблема	Решение
		Не обновляйте компоненты ОС после ее установки. Перезапустите установку PT AF

`TASK [kubernetes/preinstall : Install packages requirements] ******************`
 	
`FAILED - RETRYING: Install packages requirements (4 retries left).`
 	
`FAILED - RETRYING: Install packages requirements (3 retries left).`
 	
`FAILED - RETRYING: Install packages requirements (2 retries left).`
 	
`FAILED - RETRYING: Install packages requirements (1 retries left).`
 	
`fatal: [oblivion.local]: FAILED! => {`
 	
`"attempts": 4,`
 	
`"changed": false`
 	
`}`
 	
`MSG:`
 	
`No package matching 'bash-completion' is available`
	Не установлены стандартные системные пакеты ОС	Установите вручную пакеты ОС, указанные в последней строке ошибки, либо подключите требуемые репозитории. После этого перезапустите установку PT AF

`TASK [../roles/deploy_distribution : Distribute ssh pubkey] ******************`
 	
`[WARNING]: Unable to find '/home/ptdeploy/.ssh/id_rsa.ptaf.pub' in expected`
 	
`paths (use -vvvvv to see paths)`
 	
`fatal: [af.attdett.stf]: FAILED! => {}`
	Сценарий установки не находит SSH-ключи	Варианты решения:
		— Создайте каталог `/home/ptdeploy/.ssh/`, переместите в него ключи и запустите установку заново.
		— Запустите предварительную настройку

Сообщение в командной строке	Проблема	Решение
MSG: An unhandled exception occurred while running the lookup plugin 'file'. Error was a <class 'ansible.errors.AnsibleError'>, original message: could not locate file in lookup: /home/ptdeploy/.ssh/id_rsa.ptaf.pub PLAY RECAP ********** *** af.attdett.stf : ok=7 changed=2 unreachable=0 failed=1 skipped=14 rescued=0 ignored=0 2025-07-02 14:40:10,891 INFO:'Sync installation over all nodes' summary: {'ok': 7, 'changed': 2, 'unreachable': 0, 'failed': 1, 'skipped': 14, 'rescued': 0, 'ignored': 0}. 2025-07-02 14:40:10,891 WARNING:This playbook last failure is on '../roles/deploy_distribution : Distribute ssh pubkey' task.		Kubernetes от имени суперпользователя (root). — Проверьте значения в файле /etc/hosts

TASK [Install WSC depends] **********
 	
fatal: [localhost]: FAILED! => {
 	
"changed": false
 	
}
 	
MSG:
 	
No package matching 'sshpass' is available
	Не установлены пакеты или не подключены репозитории ОС, необходимые для работы WSC	Установите вручную пакеты ОС, указанные в последней строке ошибки, либо подключите требуемые репозитории. После этого перезапустите установку PT AF

17.4. Не переименовались сетевые интерфейсы

При установке Debian из подготовленного ISO-образа сетевые интерфейсы автоматически переименовываются. Если они не переименовались из-за сбоя в работе сценария установки, вы можете переименовать их вручную с помощью команды `sudo /usr/local/bin/wsc --rename-interfaces`.

Для автоматического переименования сетевых интерфейсов выполняется сценарий WSC. Если сетевой интерфейс подключен с помощью отличной от PCI шины, при попытке переименования интерфейса может возникнуть ошибка. Во избежание ошибки необходимо исключить из сценария переименования сетевые интерфейсы, подключенные с помощью отличных от PCI шин.

- Чтобы исключить сетевые интерфейсы из сценария переименования,

  переопределите переменную `EXTERNAL_CONTROL_INTERFACES_PATTERNS` указав в ее значении фильтруемые префиксы или сетевые интерфейсы:

  ```
  export EXTERNAL_CONTROL_INTERFACES_PATTERNS="docker;kube-ipvs;tunl;veth;cali;flannel;vif;<префиксы или сетевые интерфейсы через точку с запятой, которые нужно исключить из сценария переименования>"
  ```

  Например:

  ```
  export EXTERNAL_CONTROL_INTERFACES_PATTERNS="docker;kube-ipvs;tunl;veth;cali;flannel;vif;usb;eth1"
  ```

Значение переменной по умолчанию:
`EXTERNAL_CONTROL_INTERFACES_PATTERNS="docker;kube-ipvs;tunl;veth;cali;flannel;vif"`

- Чтобы вернуть переменной `EXTERNAL_CONTROL_INTERFACES_PATTERNS` значение по умолчанию,

  выполните команду:

  ```
  unset EXTERNAL_CONTROL_INTERFACES_PATTERNS
  ```

17.5. Метрики для мониторинга работы PT AF

В разделе описаны возможные проблемы в работе PT AF, приведены метрики для их мониторинга, даны рекомендации по устранению проблем.

Количество запросов в секунду значительно превышает среднее часовое значение

Возможная причина: DDoS-атака.

Рекомендуемый источник данных: Grafana (виджет **Tenants** → **WebApp RPS**), метрики `core_static_requests` и `core_dynamic_requests`.

Признак: сумма метрик `core_static_requests` и `core_dynamic_requests` всех подов превышает среднее часовое значение более чем на 30%.

Рекомендуемые действия:

1. Отследить паттерн DDoS-атаки; если возможно, создать пользовательское правило.
2. Ограничить максимальное количество запросов в секунду (rate limit).

   Примечание. При подборе пороговых значений для исключения ложных срабатываний нужно учитывать приемлемые отклонения.

Тип сообщения для мониторинга: предупреждение о проблеме.

Общее количество запросов в секунду значительно снизилось

Возможные причины: сбои в сетевой доступности веб-приложений или проблемы в их работе.

Рекомендуемый источник данных: Grafana (виджет **Tenants** → **WebApp RPS**), метрики `core_static_requests` и `core_dynamic_requests`.

Признак: сумма метрик `core_static_requests` и `core_dynamic_requests` всех подов ниже среднего часового значения более чем на 40% (для предупреждения) или 60% (для ошибки).

Рекомендуемые действия:

1. Поверить сетевую доступность веб-приложений.
2. Проверить состояние веб-приложений.

   Примечание. При подборе пороговых значений для исключения ложных срабатываний нужно учитывать приемлемые отклонения.

Тип сообщения для мониторинга:

— при снижении более чем на 40% — предупреждение о проблеме;

— более чем на 60% — сообщение об ошибке.

Рост числа ошибок в ответах на запросы

Возможные причины: некорректная настройка правил и (или) сбой в работе веб-приложения.

Рекомендуемый источник данных: Grafana (виджет **Tenants** → **Backend responses per second**), метрика `core_resp_50X_codes`.

Признак: наличие ненулевых значений метрики `core_resp_50X_codes`.

Рекомендуемые действия:

1. Проверить статус применения конфигурации.
2. Проверить состояние системы и обработчиков трафика (поды, нагрузка).
3. Проанализировать события безопасности.
4. Проверить доступность и работоспособность веб-приложения.

Тип сообщения для мониторинга: сообщение об ошибке.

Рост числа неотвеченных запросов

Возможные причины: атака или некорректная настройка правил.

Рекомендуемый источник данных: Grafana (виджеты **Tenants** → **WepApp RPS** и **Tenants** → **Backend responses per second**), метрики `core_static_requests`, `core_dynamic_requests`, `core_resp_10X_codes`, `core_resp_20X_codes`, `core_resp_30X_codes`, `core_resp_40X_codes`, `core_resp_50X_codes`.

Признак: сумма метрик `core_static_requests` и `core_dynamic_requests` более чем на 5% (для предупреждения) или 10% (для ошибки) выше среднего часового значения и разница `(core_static_requests+core_dynamic_requests)-(core_resp_10X_codes+core_resp_20X_codes+core_resp_30X_codes+core_resp_40X_codes+core_resp_50X_codes)` больше 5% от суммы `core_static_requests+core_dynamic_requests`.

Рекомендуемые действия:

1. Просмотреть дашборд на наличие атак.
2. Если атака идет со статических IP-адресов, добавить их в черный список.
3. Проверить параметры агрегации.
4. Если атаки PT AF не обнаружены, просмотреть файл `access.log` на внешнем балансировщике. При наличии нелегитимных запросов нужно заблокировать их исходящие IP-адреса (написать правило).

Тип сообщения для мониторинга:

— при превышении более чем на 5% — предупреждение о проблеме;

— более чем на 10% — сообщение об ошибке.

Рост числа инцидентов

Возможная причина: атака.

Рекомендуемый источник данных: Grafana (виджет **Clickhouse** → **Insert Query**), метрика `ClickHouseProfileEvents_InsertQuery`.

Признак: метрика `ClickHouseProfileEvents_InsertQuery` отклоняется от среднего часового значения более чем на 20%.

Рекомендуемые действия:

1. Просмотреть дашборд на наличие атак.
2. Если атака идет со статических IP-адресов, добавить их в черный список.
3. Проверить параметры агрегации.

Тип сообщения для мониторинга: предупреждение о проблеме.

Значения метрик RPS не обновляются

Возможная причина: потеря связи с подом (веб-приложение не получает трафик от пода).

Рекомендуемый источник данных: Grafana (виджет **Tenants** → **WebApp RPS**), метрики `core_static_requests` и `core_dynamic_requests`.

Признак: последние значения метрик `core_static_requests` и `core_dynamic_requests` получены от пода более 1 минуты назад.

Рекомендуемые действия:

1. Проверить состояние подов core rs и состояние узлов обработки трафика.
2. Проверить статус применения конфигурации.

Тип сообщения для мониторинга: сообщение об ошибке.

Низкая скорость считывания событий безопасности

Возможная причина: деградация ClickHouse.

Источник данных: тестовый API-запрос.

```
/api/ptaf/v4/threats/events?page={"offset":0,"length":<Количество последних событий>}
&filters=[{"path":"timestamp","type":"gte","value":<Время для отчета последних
событий>}]&fields=["timestamp","rule_id","rule_name","event_severity","client_ip_addr
ess","client_geo.country_code","application_name","response_code","request_method","r
equest_uri","request_headers.value","request_headers.key","id"]
```

Признак: время ответа на тестовый API-запрос более 3 секунд (для предупреждения) или 10 секунд (для ошибки).

Например:

```
/api/ptaf/v4/threats/events?page={"offset":0,"length":20}
&filters=[{"path":"timestamp","type":"gte","value":1700486167.222}]&fields=["timestam
p","rule_id","rule_name","event_severity","client_ip_address","client_geo.country_cod
e","application_name","response_code","request_method","request_uri","request_headers
.value","request_headers.key","id"]
```

Рекомендуемые действия:

1. Проверить статус службы ClickHouse.
2. Проверить статус службы ZooKeeper.
3. Проверить статусы подов в Kubernetes.

   Примечание. При наличии большого потока событий рекомендуется считывать события, поступившие за последний час.

Тип сообщения для мониторинга:

— при задержке более чем на 3 секунды — предупреждение о проблеме;

— более чем на 10 секунд — сообщение об ошибке.

Низкая скорость разбора очереди событий аудита

Возможная причина: деградация сервиса ptaf-audit-mgr-lb.

Рекомендуемые источники данных: Grafana, RabbitMQ.

Признак: рост числа сообщений в очереди ptaf-audit-mgr более чем на 1000% от среднего значения за час.

Рекомендуемые действия:

1. Проверить статус пода ptaf-audit-mgr и просмотреть его журналы.
2. Проверить статус RabbitMQ.
3. Проверить статус всех подов в Kubernetes.

   Примечание. Вы можете просмотреть список очередей с помощью команды `sudo rabbitmqctl list_queues --vhost=ptaf`.

Тип сообщения для мониторинга: предупреждение о проблеме.

Низкая скорость разбора очереди сообщений для фильтрующих ядер

Возможная причина: деградация сервиса ptaf-border-lb.

Рекомендуемые источники данных: Grafana, RabbitMQ.

Признак: рост количества сообщений очереди border-core-conf более чем на 1000% от среднего значения за час или отсутствие уменьшения очереди в течение 10 минут.

Тип сообщения для мониторинга: предупреждение о проблеме.

Низкая скорость разбора очереди сообщений на стороне коррелятора

Возможная причина: деградация коррелятора.

Рекомендуемые источники данных: Grafana, RabbitMQ.

Признак: рост числа сообщений в очереди border-correlator-comm более чем на 1000% от среднего значения за час.

Тип сообщения для мониторинга: предупреждение о проблеме.

Низкая скорость разбора очереди сообщений об инцидентах

Возможная причина: деградация сервиса ptaf-incident-mgr-lb.

Рекомендуемые источники данных: Grafana, RabbitMQ.

Признак: рост числа сообщений в очереди ptaf-incident-mgr более чем на 1000% от среднего значения за час.

Рекомендуемые действия:

1. Проверить статус пода ptaf-incident-mgr и просмотреть его журналы.
2. Проверить статус RabbitMQ.
3. Проверить статус всех подов в Kubernetes.

   Примечание. Вы можете просмотреть список очередей с помощью команды `sudo rabbitmqctl list_queues --vhost=ptaf`.

Тип сообщения для мониторинга: предупреждение о проблеме.

17.6. Ошибка при обновлении узла PT AF

При попытке обновления узла PT AF возникает ошибка, например:

```
STDERR:
gzip: stdout: No space left on device
E: mkinitramfs failure gzip 1
update-initramfs: failed for /boot/initrd.img-5.10.0-33-amd64 with 1.
```

Возможные причины

Если ранее вы уже обновляли узел PT AF, в каталоге `/boot` могли сохраниться файлы предыдущих версий ядра операционной системы, что привело к недостатку свободного места в каталоге.

Решение

- Чтобы решить проблему:

  1. Проверьте текущую версию ядра операционной системы:
     ```
     uname -r
     ```
  2. Проверьте всех список установленных файлов ядра операционной системы и заголовочных файлов:
     ```
     dpkg --list | grep linux-image
     dpkg --list | grep linux-headers
     ```
  3. Удалите файлы ядра операционной системы и связанные с ними заголовочные файлы за исключением текущей версии:
     ```
     sudo apt-get --purge remove linux-image-<удаляемая версия файла ядра ОС>
     sudo apt-get --purge remove linux-headers-<удаляемая версия заголовочного файла ОС>
     ```
  4. Обновите конфигурацию загрузчика:
     ```
     sudo update-grub2
     ```
  5. Перезагрузите сервер:
     ```
     sudo shutdown -r now
     ```

17.7. Не запускается под после обновления

После обновления под находится в статусе **Pending**. Подробная информация о состоянии пода, получаемая по команде `kubectl describe pods <Имя пода>`, содержит сообщение `node.kubernetes.io/disk-pressure`.

Возможные причины

Диск, на котором размещен под, занят на 85 процентов или более.

Решение

- Чтобы решить проблему:

  1. Просмотрите список образов прошлых версий PT AF, сохраненных на диске:
     ```
     sudo crictl image ls
     ```
  2. Если в списке есть версии ниже обновляемой, удалите их:
     ```
     sudo crictl rmi <Название образа>:<Метка>
     ```
     Например, если вы обновляете систему с версии 4.1.4 до 4.1.5, нужно удалить версии 4.1.3 и ниже:
     ```
     sudo crictl rmi registry.docker-registry.svc.cluster.local:7000/ptaf-task-mgr:release-4.1.3.317180
     ```

17.8. Не отправляются события на syslog-сервер после обновления Docker-агента

Проблема

После обновления агента, установленного из Docker-образа, события безопасности не отправляются на внешний syslog-сервер.

Возможные причины

Проблема может возникнуть в следующих случаях:

— В файле `compose.yaml` указаны старые переменные для отправки событий на внешний syslog-сервер. Начиная с версии 4.1.6 переменные указываются без префикса `NGINX_ENV_`, и необходимо их отредактировать.

— Переменные окружения, отвечающие за отправку событий на внешний syslog-сервер, указаны в файле `nginx.conf`, который используется в качестве внешней конфигурации агента. Необходимо перенести эти переменные в файл `compose.yaml`.

Решение

- Чтобы отредактировать переменные в файле `compose.yaml`:
  1. Откройте файл `compose.yml`.
  2. Исправьте переменные, отвечающие за отправку событий на внешний syslog-сервер, в соответствии с разделом «Переменные окружения».
  3. Перезапустите Docker Compose:
     ```
     sudo docker compose up -d
     ```
- Чтобы перенести переменные окружения из файла `nginx.conf` в файл `compose.yaml`:
  1. Откройте файл `/opt/ptaf/conf/nginx.conf`.
  2. Удалите строки, содержащие переменные окружения, которые отвечают за отправку событий безопасности на внешний syslog-сервер: `EVENT_SENDER_ENABLED`, `EVENT_SENDER_HOST`, `EVENT_SENDER_PORT`, `EVENT_SENDER_TIMEOUT`, `EVENT_WEB_UI_URL`.
  3. Откройте файл `compose.yml`.
  4. В секцию `environment` добавьте переменные окружения для отправки событий безопасности на внешний syslog-сервер.
  5. Перезапустите Docker Compose:
     ```
     sudo docker compose up -d
     ```

17.9. На схеме конфигурации не отображается сервер и профиль обработки трафика

Проблема

На схеме конфигурации в блоках **Профили трафика** и **Защищаемые серверы** не отображается сервер и профиль обработки трафика.

Возможные причины

Обработку входящего трафика выполняет агент PT AF.

Решение

Если для обработки входящего трафика вы подключили агент PT AF, настройка серверов и профилей обработки входящего трафика выполняется на самом агенте. Поэтому для изолированного пространства, в параметрах которого в качестве типа профиля обработки трафика указано значение **Агент**, на схеме конфигурации не отображаются серверы и профили обработки входящего трафика.

17.10. Ошибка восстановления из резервной копии

Проблема

Процедура восстановления не запущена или прервана. Параметры системы возвращены к предыдущему состоянию.

Возможные причины

Процедура восстановления не будет запущена или будет прервана, если на любом из этапов восстановления обнаружена ошибка.

Решение

Возможные ошибки и варианты их решения указаны в таблице ниже.

Таблица 25. Ошибки, связанные с восстановлением из резервной копии

Этап	Ошибка	Решение
Проверка возможности восстановления (целостность архива, поддерживаемая версия резервной копии)	Недействительная резервная копия. Файл поврежден или версия резервной копии не поддерживается	Загрузите новый файл. Восстановите систему из другой резервной копии
Запуск процесса восстановления	Неверно введено название резервной копии для запуска процесса восстановления	Повторно введите имя резервной копии
	Неверно введен пароль резервной копии для запуска процесса восстановления	Начните процедуру восстановления заново и введите верный пароль. Воспользуйтесь подсказкой в карточке резервной копии, чтобы вспомнить пароль
Расшифровка файла архива резервной копии	На устройстве недостаточно памяти для расшифровки файла архива	Освободите память на устройстве
Восстановление данных в базе	Неверная версия базы знаний	Обновите базу знаний до той версии, которая находится в резервной копии

17.11. Исключение узла из обработки трафика

Вы можете безопасно исключить узел из обработки трафика и временно перенести его поды на другие активные узлы. Например, это может потребоваться для технического обслуживания сервера.

- Чтобы исключить узел из обработки трафика,

  выполните команду:

  ```
  sudo kubectl drain <Имя узла> --ignore-daemonsets --delete-emptydir-data
  ```

  Например:

  ```
  sudo kubectl drain node3.af.example.com --ignore-daemonsets --delete-emptydir-data
  ```

  По завершении переноса подов появится сообщение:

  ```
  node/node3.af.example.com evicted
  ```

  Примечание. Вы можете ускорить процесс переноса, не дожидаясь завершения медленных сессий, с помощью ключей `--force=true --grace-period=-1 --timeout=0s`.

  Например:

  ```
  sudo kubectl drain node3.af.example.com --ignore-daemonsets --delete-emptydir-data --force=true --grace-period=-1 --timeout=0s
  ```

- Чтобы вернуть узел в процесс обработки трафика,

  выполните команду:

  ```
  sudo kubectl uncordon <Имя узла>
  ```

  Например:

  ```
  sudo kubectl uncordon node3.af.example.com
  ```

17.12. Особенности маршрутизации исходящего трафика

При настройке маршрутизации исходящего трафика нужно учитывать важную особенность. Если интерфейс имеет назначенный IP-адрес, не является интерфейсом `lo` и отображается первым в выводе команды `ip a`, и вы добавили правило, которое направляет исходящий трафик этого интерфейса в отдельную таблицу маршрутизации, нужно добавить более приоритетные правила, которые направят входящий и исходящий трафик интерфейса, адресованный внутренней IP-подсети кластера Kubernetes, в таблицу маршрутизации по умолчанию `main`.

Например, для интерфейса `eth-ext1` вы добавили правило, которое направляет исходящий трафик с IP-адреса интерфейса `192.0.2.56` в отдельную таблицу маршрутизации `mytable`:

```
sudo wsc -c "route rule add eth-ext1 from 192.0.2.56/32 pref <N> table mytable"
```

Если интерфейс `eth-ext1` является первым интерфейсом в выводе команды `ip a` (не считая интерфейс `lo`), необходимо также добавить более приоритетные правила:

```
sudo wsc -c "route rule add eth-ext1 from 192.0.2.56/32 to <Подсеть кластера Kubernetes> pref <N-1> table main"
sudo wsc -c "route rule add eth-ext1 from <Подсеть кластера Kubernetes> to 192.0.2.56/32 pref <N-2> table main"
sudo wsc -c "config commit"
```

Где:

— `<Подсеть кластера Kubernetes>` — IP-адреса внутренней подсети кластера Kubernetes (по умолчанию `10.233.0.0/17`);

— `<N>`, `<N-1>`, `<N-2>` — приоритет правила (чем меньше число, тем выше приоритет).

См. также

Команды управления сетевыми маршрутами (см. приложение А.9)

17.13. Проблема подключения агента

Проблема

Агент не подключается к PT AF от имени учетной записи нового пользователя. В системном журнале агента содержится ошибка `[err] [ptafd:114190] [PTAFD] int main(int, char**); exception: 'Permission denied'`.

Возможные причины

Некорректная работа прав доступа учетной записи.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что сначала был установлен веб-сервер nginx, а затем агент.
  2. Если порядок установки не нарушен, принудительно завершите все процессы nginx и агента:

```
apt -y install psmisc
killall -9 ptaf-nginx || echo "ignore"
killall -9 ptaf-core-ctl || echo "ignore"
killall -9 ptafd || echo "ignore"
killall -9 nginx || echo "ignore"
rm -rf /dev/shm/ptaf_*
ipcrm --all=sem
rm -rf /tmp/ipl
```

```
rm -rf /opt/ptaf/cache/regex_cache/*
rm -rf /tmp/lmdb_shared_storage
```

3. Если порядок установки нарушен, удалите компоненты и установите их снова.

17.14. Сбор системных журналов

Для анализа и локализации проблем, возникающих при работе с PT AF, вы можете использовать системные журналы.

Возможные варианты сбора системных журналов:

- просмотр и выгрузка записей журнала о работе PT AF с помощью сервиса Grafana Loki (см. раздел 17.14.1);
- выгрузка журнала сетевых событий с помощью браузера на базе Chromium (см. раздел 17.14.2);
- получение общего журнала событий в каталоге /var/log (см. раздел 15.14);
- получение журнала событий установки и обновлений PT AF в каталоге `/var/log/ptaf/deploy`;
- сбор журналов событий и дампов с помощью утилиты harvester (см. раздел 17.14.3);
- сбор системных журналов с событиями уровня debug.

В этом разделе

Выгрузка системного журнала с помощью сервиса Grafana (см. раздел 17.14.1)

Выгрузка журнала сетевых событий на клиентской стороне (см. раздел 17.14.2)

Выгрузка системных журналов с помощью утилиты harvester (см. раздел 17.14.3)

Выгрузка системных журналов уровня debug (см. раздел 17.14.4)

17.14.1. Выгрузка системного журнала с помощью сервиса Grafana

Вы можете просмотреть записи о работе системы и выгрузить журнал событий с помощью сервиса Grafana Loki.

► Чтобы выгрузить записи системного журнала:

1. Войдите в веб-интерфейс Grafana.

   Примечание. Подробные инструкции по работе с Grafana приведены на сайте производителя.

2. В панели слева нажмите  .

   Откроется страница **Explore**.

3. В раскрывающемся списке сверху выберите источник данных **Loki**.
4. Нажмите **Log browser**.
5. В блоке параметров **Labels filters** выберите компонент, для которого необходимо выгрузить журнал.
6. В панели инструментов выберите период, за который требуется выгрузить данные (по умолчанию — последний час).
7. Нажмите **Run query**.

   Отобразятся записи из системного журнала.
8. В панели **Logs** нажмите **Download** и выберите формат данных.

Файл с журналом событий сохранен в локальной папке.

17.14.2. Выгрузка журнала сетевых событий на клиентской стороне

Для анализа работы PT AF на стороне клиента вы можете выгрузить журналы сетевых событий в форматах HAR и JSON с помощью браузера на базе Chromium.

- Чтобы выгрузить журналы событий с помощью браузера:

  1. Откройте браузер в режиме инкогнито.
  2. Откройте веб-приложение и выполните вход.
  3. Откройте страницу, на которой обнаружена проблема.
  4. Нажмите клавишу F12.

     Откроется окно с инструментами разработчика.
  5. Выберите вкладку **Network**.
  6. Перейдите по ссылке `chrome://net-export`.

     Отроется страница **Capture Network Log**.
  7. В блоке параметров **Options** выберите вариант **Include raw bytes (will include cookies and credentials)**.
  8. Нажмите **Start Logging to Disk**.
  9. В открывшемся окне выберите папку, в которой необходимо сохранить журнал событий в формате JSON.
  10. Нажмите кнопку **Сохранить**.
  11. Вернитесь на страницу веб-приложения и воспроизведите ситуацию, которая приводит к проблеме.

12. Если требуется, в окне с инструментами разработчика в таблице с данными найдите запросы, с которыми возникли проблемы, и сохраните их URL.
13. В контекстном меню таблицы с данными выберите пункт **Save all as HAR with content**.
14. В открывшемся окне выберите папку, в которой необходимо сохранить журнал событий в формате HAR.
15. Нажмите кнопку **Сохранить**.
16. На странице **Capture Network Log** нажмите **Stop Logging**.

Журналы событий в формате HAR и JSON, а также URL запросов получены для анализа.

17.14.3. Выгрузка системных журналов с помощью утилиты harvester

Для сбора системных журналов с узлов кластера PT AF используется утилита harvester. Она подключается к узлам кластера и собирает следующую информацию:

- файлы журналов установки PT AF;
- файлы журналов с каждого пода (`/opt/ptaf/logs`);
- файлы журналов Grafana Loki;
- системные журналы с каждого узла (`/var/log/messages`);
- дампы памяти процессов ядра, завершенных нештатно (core dumps);
- результаты выполнения команд bash;
- резервные копии данных PostgreSQL.

► Чтобы выгрузить системные журналы с помощью harvester:

1. От имени служебной учетной записи (`pt`) подключитесь по SSH к узлу, на котором выполнялась установка PT AF.
2. Запустите утилиту:

   ```
   harvester -lu --time-zone="<Текущий часовой пояс>"
   ```

   Примечание. По умолчанию harvester собирает журналы за последние 4 часа, но вы можете задать другой период с помощью параметров запуска (см. таблицу 26).

Архив с журналами событий сохранится на узле в том каталоге, из которого запускалась утилита harvester. Имя файла имеет формат: `<Имя узла>-<Дата и время начала записи событий>__<Дата и время окончания записи событий>_harvester_logs.tar.gz`.

Таблица 26. Параметры запуска harvester

Параметр	Обязательный	Описание	Пример
`time-zone`	Да	Часовой пояс. Возможные значения: от –14 до +12. Ноль используется как +0 или –0	`--time-zone="+7"`
`since`	Нет	Временной интервал для сбора событий за последние часы, минуты или секунды. Указывается в формате `XhZmYs`, где `X`, `Z` и `Y` — положительные целые числа больше нуля. Параметр игнорируется, если указан параметр `time-from` или `time-to`	`--since=5m30s`
`time-from` и `time-to`	Нет	Период, за который необходимо выгрузить записи журналов	`--time-from="2022-03-10 12:05" --time-to="2022-03-10 13:21"`

17.14.4. Выгрузка системных журналов уровня debug

Для более глубокого анализа проблемы в работе PT AF могут понадобиться записи журналов уровня debug, сформированные в момент возникновения проблемы.

Инструкцию необходимо выполнять от имени учетной записи `pt` на узле, который использовался для установки PT AF.

Внимание! Включение уровня журналирования debug для всех изолированных пространств значительно увеличит объем записей на диске.

- Чтобы выгрузить системные журналы уровня debug:

1. Включите журналирование уровня debug для всех необходимых подов, выполнив запрос к REST API для каждого из необходимых изолированных пространств:

```
PATCH <Корневой URL API>/config/traffic_settings
{
  "core_nginx_log_level": "debug",
  "core_envoy_log_level": "debug",
  "core_ptaf_log_level": "debug",
```

```
  "envoy_proxy_log_level": "debug"
}
```

2. Если требуется, просмотрите идентификаторы подов в составе пространства имен PT AF:

   ```
   kubectl get pods -n ptaf-core
   ```

3. Убедитесь, что журналирование уровня debug (dbg) включено:

   - Если для обработки трафика используется сервер nginx:

     ```
     kubectl -n ptaf-core logs ptaf-core-rs-<Идентификатор пода>| grep debug
     ```

   - Если для обработки трафика используется сервер Envoy:

     ```
     kubectl -n ptaf-core logs ptaf-core-envoy-rs-<Идентификатор_пода> | grep debug
     ```

4. Воспроизведите несколько раз ситуацию, которая приводит к проблеме.

   PT AF сохранит все события в течение трех минут.

5. Выгрузите журналы событий за последний час с помощью утилиты harvester (см. раздел 17.14.3):

   ```
   harvester -lu --since 1h --time-zone <Часовой пояс>
   ```

   Архив с журналами событий сохранится на узле в том каталоге, из которого запускалась утилита harvester. Имя файла имеет формат: `<Имя узла>-<Дата и время начала записи событий>__<Дата и время окончания записи событий>_harvester_logs.tar.gz`.

6. Отключите журналирование уровня debug для всех необходимых подов, выполнив запрос к REST API для каждого из необходимых изолированных пространств:

   ```
   PATCH <Корневой URL API>/config/traffic_settings
   {
     "core_nginx_log_level": "error",
     "core_envoy_log_level": "error",
     "core_ptaf_log_level": "error",
     "envoy_proxy_log_level": "error"
   }
   ```

18. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на PT AF в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы и сроки ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к порталу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку на портале технической поддержки и предоставить следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и наборы диагностических данных, которые требуются для анализа;

— снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 27. Время реакции на заявку

Уровень значимости заявки	**Критерии значимости заявки**	**Время реакции на заявку**
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

  Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Приложение А. Команды оболочки WSC

В WSC выполняется основная сетевая и кластерная настройка PT AF: настройка интерфейсов, маршрутов, таблиц и правил маршрутизации, виртуальных IP-адресов и параметров сборки и реконфигурации кластера Kubernetes.

Команды WSC делятся на несколько типов — служебные, информационные и секционные.

Секционные команды позволяют как переходить в отдельные конфигурационные секции, если задана команда без аргументов, так и просматривать и изменять параметры секции, если команда задана с аргументами.

Например, выполнить команду добавления узла кластера Kubernetes можно следующими способами:

— с переходом в подсекцию:
```
wsc> inventory node
add <node_name>
```

— с переходом в секцию:
```
wsc> inventory
node add <node_name>
```

— без перехода в секцию:
```
wsc> inventory node add <node_name>
```

Внимание! При выполнении настройки сети в WSC меняется лишь локальная конфигурация оболочки. Для применения изменений на узле дополнительно необходимо выполнить команды секции `config`.

В WSC вы можете использовать комбинацию клавиш Ctrl+D для выхода из секции, комбинацию клавиш Ctrl+R для просмотра истории команд и клавишу Tab для автоматического дополнения команды или аргумента.

Далее приведен список команд WSC и их описание.

При написании команд используются следующие условные обозначения:

— | — знак «или» разделяет альтернативные, взаимоисключающие параметры;

— [ ] — в квадратных скобках указаны необязательные параметры, ввод которых дает дополнительные возможности;

— { } — в фигурных скобках указаны обязательные параметры;

— <> — в угловых скобках указаны условные значения параметров, которые при вводе команды необходимо заменить реальными значениями (например, вместо <interface> ввести eth-cluster).

Внимание! Для корректной работы команд WSC не используйте следующие спецсимволы в вводимых значениях (например, в пароле): ', \, ", пробел, табуляцию и $ в начале строки.

В этом разделе

Служебные команды WSC (см. приложение A.1)

Информационные команды WSC (см. приложение A.2)

Команды настройки подключения WSC к сервису конфигурации (см. приложение A.3)

Команды настройки параметров DHCP-клиента (см. приложение A.4)

Команды настройки сетевых интерфейсов (см. приложение A.5)

Команды сбора и реконфигурации кластера Kubernetes (см. приложение A.6)

Команды генерации ключей SSH (см. приложение A.7)

Команды настройки пула NTP-серверов (см. приложение A.8)

Команды управления сетевыми маршрутами (см. приложение A.9)

Команды настройки виртуальных IP-адресов (см. приложение A.10)

Часто задаваемые вопросы о работе с WSC (см. приложение A.11)

A.1. Служебные команды WSC

Служебные предназначены для вывода технической информации и позволяют управлять самой оболочкой.

admin

Служебная команда `admin` позволяет непривилегированному пользователю перейти в командную оболочку Linux. Для выполнения команды нужно ввести пароль пользователя pt.

```
# Войти в командную оболочку Linux
wsc> admin
Password:
```

Внимание! Для корректной работы команд WSC не используйте следующие спецсимволы в вводимых значениях (например, в пароле): `'`, `\`, `"`, пробел, табуляцию и `$` в начале строки.

config

Служебная команда `config`, выполненная без аргументов, позволяет просмотреть локальную конфигурацию WSC. Если настройка системы позволяет и текущая конфигурация при выводе превышает размер экрана, то используется пагинатор.

```
# Просмотреть локальную конфигурацию WSC
wsc> config
```

config commit

Служебная команда `config` с аргументом `commit` позволяет применить в системе все изменения, внесенные в WSC.

```
# Применить в системе все изменения локальной конфигурации оболочки
wsc> config commit
```

Внимание! Если после выполнения команды `config commit` какая-то часть конфигурации не была применена в системе из-за ошибок, вы можете использовать команду `config commit force`, которая принудительно перезапишет всю локальную конфигурацию оболочки в системную.

config commit network

Служебная команда `config` с аргументами `commit network` позволяет применить в системе только сетевую локальную конфигурацию, то есть применить параметры, настроенные командами `dhcp`, `timezone`, `ntp`, `route`, `if`.

```
# Применить в системе только сетевую конфигурацию
wsc> config commit network
```

config commit force

Служебная команда `config` с аргументами `commit force` позволяет принудительно сохранить в системе всю конфигурацию оболочки WSC.

```
# Принудительного сохранить в системе всю конфигурацию оболочки WSC
wsc> config commit force
```

config reset

Служебная команда `config` с аргументом `reset` позволяет создать новую конфигурацию WSC на основе системной. При выполнении указанной команды также происходит удаление имеющейся конфигурации WSC.

```
# Создать новую конфигурацию WSC
config reset
```

config try

Служебная команда `config` с аргументом `try` позволяет временно применить конфигурацию WSC в системе. После выполнения команды `config` с аргументом `try` в течение 10 минут необходимо ввести команду `config accept`, иначе система вернется к предыдущим значениям параметров.

```
# Временно применить конфигурацию WSC в системе
wsc> config try
```

config accept

Служебная команда `config` с аргументом `accept` позволяет применить временную конфигурацию на системную после выполнения команды `config try`. Ввести команду `config accept` и подтвердить конфигурацию можно из любой SSH-сессии.

```
# Подтверждение применения конфигурации после выполнения команды config try
wsc> config accept
```

exit

Служебная команда `exit` позволяет выйти из секции.

```
# Выйти из секции route table
wsc:route:table> exit
```

help

Служебная команда `help` предназначена для получения справочной информации о командах WSC.

Если команда `help` введена без аргументов, будет показан список доступных команд той секции, в которой она выполнена.

```
# Вывести список доступных команд секции inventory
wsc:inventory> help
```

Если команда `help` указана после названия секционной команды, будет показано, для каких команд секции доступны подсказки, а для каких нет.

```
# Вывести данные о наличии справки для команд секции if
wsc> if help
```

Если команда `help` указана перед секционной командой, то будет выведена информация обо всех командах этой секции.

```
# Вывести справку по командам секции route
wsc> help route
```

Если команда `help` указана между секционной командой и ее аргументом, будет показана информация об этом аргументе.

```
# Вывести справку о команде list секции if
wsc> if help list
```

history

Служебная команда `history` позволяет вывести ранее введенные команды. Для просмотра списка команд вы можете использовать клавиши ↑ и ↓. В истории хранятся команды текущей и всех предыдущих сессий. Количество хранимых команд — 255.

```
# Вывести список введенных команд
wsc> history
```

info

Служебная команда `info` позволяет вывести информацию о системе, включая ее версию, версию ядра и компонентов, текущее локальное время.

snapshot

Команда `snapshot`, введенная без аргументов, позволяет выполнить вход в секцию `snapshot`.

```
# Перейти в секцию snapshot
wsc> snapshot
```

snapshot restore

Служебная команда `snapshot restore` позволяет восстановить конфигурацию оболочки WSC, сохраненную после последнего применения параметров командой `config commit`.

```
# Восстановить конфигурацию оболочки WSC
wsc> snapshot restore
```

A.2. Информационные команды WSC

Информационные команды позволяют просмотреть имя узла и часовой пояс, а также изменить часовой пояс.

hostname

Информационная команда `hostname`, введенная без аргументов, позволяет вывести имя узла.

```
# Вывести имя узла
wsc> hostname
```

timezone

Информационная команда `timezone`, введенная без аргументов, позволяет вывести текущее значение часового пояса.

```
# Вывести значение часового пояса
wsc> timezone
```

Команда `timezone` с параметром `<Часовой пояс>` позволяет установить часовой пояс. Часовой пояс не рекомендуется изменять после завершения установки PT AF.

```
# Установить часовой пояс Europe/Moscow
wsc> timezone Europe/Moscow
```

A.3. Команды настройки подключения WSC к сервису конфигурации

border

Команды секции `border` позволяют просматривать, генерировать и менять ключ для доступа WSC к сервису Border, а также заново генерировать сертификат для доступа к этому сервису.

```
# Перейти в секцию border
wsc> border
```

border list

Команда `border list` позволяет просмотреть значение настроенного ключа.

```
# Показать ключ
wsc> border list
```

border generate_token

Команда `border generate_token` позволяет сгенерировать и установить ключ для доступа WSC к параметрам маршрутизации прослушиваемых IP-адресов на том узле, где выполняется настройка. Если ключ уже был сгенерирован, то требуется использовать аргумент `force` для повторной генерации ключа. В ином случае существующий ключ изменен не будет. Для применения изменений необходимо после настройки выполнить команду `config commit`.

```
# Сгенерировать ключ для доступа WSC к параметрам маршрутизации прослушиваемых IP-адресов
wsc> border generate_token
# Заново генерировать ключ
wsc> border generate_token force
```

border renew_certs

Команда позволяет вызвать принудительное обновление серверных сертификатов для сервиса взаимодействия с агентом.

> **Примечание.** Обновление происходит после выполнения команды `config commit`.

```
# Обновить серверные сертификаты
wsc> border renew_certs
```

border set token

Команда `border set token` позволяет установить ключ для доступа WSC к параметрам маршрутизации прослушиваемых IP-адресов на том узле, где выполняется настройка. Для применения изменений необходимо после настройки выполнить команду `config commit`.

```
# Установить ключ
wsc> border set <Ключ>
```

A.4. Команды настройки параметров DHCP-клиента

dhcp

Команды секции `dhcp` позволяют настроить параметры DHCP-клиента.

```
# Перейти в секцию dhcp
wsc> dhcp
```

dhcp list

Команда `dhcp list` позволяет вывести список параметров и их значения для команды `dhcp`.

```
# Вывести список параметров и их значения для команды dhcp
dhcp list
```

dhcp set

Команда `dhcp set` позволяет включить или отключить использование параметров, полученных по DHCP.

```
# Использовать параметры NTP-серверов, полученные по DHCP
dhcp set ntp_servers true
# Отключить использование параметров NTP-серверов, полученных по DHCP. Применяется локальная конфигурация, которая может быть настроена командами секции ntp
dhcp set ntp_servers false
# Использовать адреса маршрутизаторов, полученные по DHCP. В случае применения данной команды настройка адресов шлюза (inet_gateway) для интерфейсов в WSC будет недоступна
dhcp set routers true
# Отключить использование адресов маршрутизаторов, полученных по DHCP. В случае применения данной команды возможна ручная настройка адресов шлюза (inet_gateway) для интерфейсов в WSC
dhcp set routers false
```

A.5. Команды настройки сетевых интерфейсов

if

Команды секции `if` позволяют настраивать сетевые интерфейсы. Команда `if`, введенная без аргументов, позволяет войти в секцию настройки сетевых интерфейсов.

if bond

Команда `if bond` позволяет объединить сетевые интерфейсы в один виртуальный интерфейс для обеспечения отказоустойчивости и повышения пропускной способности сети. Созданный bond-интерфейс автоматически именуется как `bondN`, где N — его номер.

> **Внимание!** Виртуальный интерфейс с ролью `CLUSTER` можно создавать только при развертывании PT AF. Создание такого интерфейса на уже развернутой системе приведет к ошибкам в ее работе.

```
# Объединить интерфейсы eth-ext1 и eth-int1 в bond0
wsc> if bond 0 eth-ext1 eth-int1
```

if del

Команда `if del` позволяет удалить интерфейсы, которые не являются физическими.

```
# Удалить интерфейс bond0
wsc> if del bond0
```

if list

Команда `if list` позволяет вывести список всех интерфейсов и их свойства.

```
# Вывести список всех интерфейсов и их свойства
wsc> if list
# Вывести свойства интерфейса eth-mgmt
wsc> if list eth-mgmt
# Вывести системную конфигурацию интерфейсов
wsc> if list system
```

if mode

Команда `if mode` позволяет установить режим получения IP-адреса для сетевого интерфейса. Возможные значения: `static`, `manual` и `dhcp`.

```
# Установить режим static для интерфейса eth-mgmt
wsc> if mode eth-mgmt static
```

if roles

Команда `if roles` с параметром `add` назначает одну или несколько ролей сетевому интерфейсу. Назначенные роли добавляются к уже имеющимся.

```
# Назначить роли WAN и LAN интерфейсу eth-ext1
if roles eth-etx1 add WAN LAN
```

Команда `if roles` с параметром `remove` снимает одну или несколько ролей с сетевого интерфейса.

```
# Снять роль WAN с интерфейса eth-ext1
if roles eth-etx1 remove WAN
```

if set

Команда `if set` позволяет выполнить настройку сетевых интерфейсов. Вы можете настраивать как один параметр интерфейса, так и несколько параметров одновременно.

Внимание! Для каждого сетевого интерфейса нужно выделять отдельную подсеть.

Команда `if set` с параметром `downdelay` позволяет установить время задержки (в миллисекундах) перед отключением интерфейса, входящего в состав bond-интерфейса, если произошел сбой соединения. Установленное значение должно быть кратно значению miimon (см. приложение А.5). Значение по умолчанию — 200 миллисекунд.

```
# Установить значение параметра downdelay равным 300 для интерфейса bond3
wsc> if set bond3 downdelay 300
```

Команда `if set` с параметром `inet_address` позволяет как установить, так и удалить IPv4-адрес интерфейса.

```
# Установить IP-адрес интерфейса eth-mgmt
wsc> if set eth-mgmt inet_address 192.168.0.2
# Удалить IP-адрес интерфейса eth-mgmt
wsc> if set eth-mgmt inet_address none
```

Команда `if set` с параметром `inet_gateway` позволяет настроить IPv4-адрес шлюза на интерфейсе. Вы не сможете изменить шлюз, если используется параметр `dhcp set routers true`.

```
# Назначить шлюз интерфейсу eth-mgmt
wsc> if set eth-mgmt inet_gateway 192.168.0.1
# Удалить назначенный шлюз интерфейса eth-mgmt
wsc> if set eth-mgmt inet_gateway none
```

Команда `if set` с параметром `inet_method` позволяет указать способ получения значений параметров IPv4 сети на интерфейсе:

— `static` — значения параметров указывает пользователь;

Для метода `static` необходимо также задать IP-адрес и маску или IP-адрес и префикс. В ином случае применение параметров не будет выполнено.

— `dhcp` — значения параметров запрашиваются по DHCP;

— `manual` — значения параметров устанавливаются другими компонентами или устройствами.

```
# Установить метод static для интерфейса eth-mgmt
wsc> if set eth-mgmt inet_method static
```

Команда `if set` с параметром `inet_netmask` позволяет как установить, так и удалить маску или префикс подсети на интерфейсе.

```
# Установить адрес и сетевую маску интерфейса eth-mgmt
wsc> if set eth-mgmt inet_address 192.168.0.2 inet_netmask 255.255.255.0
# Настроить префикс подсети для интерфейса eth-mgmt
wsc> if set eth-mgmt inet_netmask 30
```

Команда `if set` с параметром `is_active` позволяет как включить, так и отключить физический интерфейс.

```
# Включить физический интерфейс eth-mgmt
wsc> if set eth-mgmt is_active true
# Отключить физический интерфейс eth-mgmt
wsc> if set eth-mgmt is_active false
```

Команда `if set` с параметром `lacp_rate` позволяет настроить интервал, с которым будут запрашиваться LACPDU-пакеты в режиме 802.3a. Возможные значения: `0` (запрос на передачу LACPDU-пакетов каждые 30 секунд) и `1` (запрос на передачу LACPDU-пакетов каждую секунду). Значение по умолчанию — `1`.

```
# Установить размер интервала, с которым подключенное устройство должно отправлять
LACPDU-пакеты на bond3, равным 30 секундам
wsc> if set bond3 lacp_rate 0
```

Команда `if set` с параметром `miimon` позволяет настроить на bond-интерфейсе период проверки состояния связи на наличие сбоев в миллисекундах. Значение по умолчанию — 100 миллисекунд.

```
# Установить значение параметра miimon равным 150 для интерфейса bond1
wsc> if set bond1 miimon 150
```

Команда `if set` с параметром `mode` позволяет задать режим работы bond-интерфейса.

Доступны следующие значения:

— 0 — round-robin;

— 1 — active-backup (используется по умолчанию);

— 2 — balance-xor;

— 3 — broadcast;

— 4 — 802.3ad;

— 5 — balance-tlb;

— 6 — balance-alb.

```
# Установить для интерфейса bond6 режим round-robin
wsc> if set bond6 mode 0
```

Команда `if set` с параметром `mtu` позволяет для физических интерфейсов настроить максимальный объем данных (MTU), который может быть передан протоколом за одну итерацию.

```
# Установить размер MTU равным 1480 для интерфейса eth-mgmt
wsc> if set eth-mgmt mtu 1480
```

Команда `if set` с параметром `role` и значением `WAN` позволяет выбрать WAN-интерфейс, на который планируется передавать запросы от маршрутизатора, балансировщика, межсетевого экрана и других устройств, направляющих трафик от клиентов на PT AF для его анализа и дальнейшего проксирования.

```
# Настроить роль WAN на интерфейс eth-ext1
wsc> if set eth-ext1 role WAN
```

Команда `if set` с параметром `role` и значением `LAN` указывает интерфейс для соединения PT AF с защищаемыми веб-приложениями. Единовременно только один интерфейс узла может иметь роль `LAN`. По умолчанию эта роль не назначена ни на один интерфейс.

```
# Настроить роль LAN на интерфейс eth-int1
wsc> if set eth-int1 role LAN
```

Команда `if set` с параметром `slaves` позволяет указать, какие интерфейсы входят в состав bond-интерфейса.

```
# Объединить интерфейсы eth-int1 и eth-ext1 в bond3
wsc> if set bond3 slaves eth-ext1 eth-int1
```

Команда `if set` с параметром `updelay` позволяет указать время задержки (в миллисекундах) перед включением интерфейса, входящего в состав bond-интерфейса, при обнаружении восстановления канала. Значение должно быть кратно значению miimon. Значение по умолчанию — 200 миллисекунд.

```
# Установить значение параметра updelay равным 300 для интерфейса bond3
wsc> if set bond3 updelay 300
```

Команда `if set` с параметром `xmit_hash_policy` позволяет определить политику передачи пакетов через bond-интерфейсы в режимах 2 (balance-xor) или 4 (802.3ad). Доступны следующие значения:

— layer2 — используются только MAC-адреса;

— layer2+3 — используются как MAC-адреса, так и IP-адреса (значение по умолчанию);

— layer3+4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP).

```
# Установить значение параметра xmit_hash_policy равным layer2 для интерфейса bond3
wsc> if set bond3 xmit_hash_policy layer2
```

if vlan

Команда `if vlan` позволяет создать VLAN-интерфейс от родительского интерфейса. Создаваемые интерфейсы автоматически именуются утилитой как `<interface_name>.N`, где N — метка. Для настройки параметров интерфейса используется команда `if set`.

```
# Создать VLAN-интерфейс с метками 1060, 1070, 1080 от интерфейса eth-ext1
wsc> if vlan eth-ext1 1060 1070 1080
# Настроить созданные интерфейсы VLAN
wsc> if set eth-ext1.1060 inet_address 172.16.60.1 inet_netmask 255.255.255.0
wsc> if set eth-ext1.1070 inet_address 172.16.70.1 inet_netmask 255.255.255.0
wsc> if set eth-ext1.1080 inet_address 172.16.80.1 inet_netmask 255.255.255.0
```

A.6. Команды сбора и реконфигурации кластера Kubernetes

inventory

Команды секции `inventory` позволяют собрать или реконфигурировать кластер Kubernetes. Секционная команда `inventory`, введенная без аргументов, позволяет выполнить вход в секцию `inventory`.

```
# Перейти в секцию inventory
wsc> inventory
```

inventory node

Секционная команда `inventory node`, введенная без аргументов, позволяет войти в подсекцию `inventory node`.

```
# Перейти в подсекцию inventory node
wsc> inventory node
```

inventory node list

Команда `inventory node list` позволяет вывести список всех узлов кластера Kubernetes и их параметры.

```
# Вывести список узлов и их параметры
wsc> inventory node list
```

Если в команде `inventory node list` указать в качестве аргумента имя узла, будут показаны параметры только этого узла кластера Kubernetes.

```
# Вывести параметры узла node2
wsc> inventory node list node2
```

inventory node add

Команда `inventory node add` с параметром `<node_name>` позволяет добавить узел кластера Kubernetes. Имя узла необходимо для идентификации. В качестве имени необходимо указывать реальное имя узла (hostname), в ином случае установка не будет выполнена.

> **Внимание!** В существующий кластер можно добавлять только те узлы, которые будут использоваться исключительно для обработки трафика (иметь единственную роль — `worker-traffic`). В этом случае после добавления и настройки узла (см. раздел 15.9) нужно запустить сценарий `./install.sh --action=add_worker`.

```
# Добавить узел node1
wsc> inventory add node1
```

После выполнения команды `inventory node add` нужно настроить доступ к узлу и его роли (см. приложение А.6).

inventory node del

Команда `inventory node del` с параметром `<node_name>` позволяет удалить узел кластера, не имеющий ролей.

> **Внимание!** Из существующего кластера можно удалять только те узлы, которые использовались исключительно для обработки трафика (имели единственную роль — `worker-traffic`). В этом случае перед удалением узла (см. раздел 15.9) нужно запустить сценарий `./install.sh --action=remove_worker --nodes <node_name>`.

```
# Удалить узел node1
wsc> inventory node del node1
```

Команда `inventory node del` с параметром `force` позволяет принудительно удалить узел кластера Kubernetes, даже если для него настроены роли.

```
# Принудительно удалить узел node1
wsc> inventory node del node1 force
```

Команда `inventory node del` с параметром `role` позволяет удалить одну или несколько ролей указанного узла кластера Kubernetes.

```
# Удалить роль worker-traffic для узла node1
wsc> inventory node del node1 role worker-traffic
```

inventory node set

Команда `inventory node set` позволяет настроить доступ к узлу и его роли. Вы можете настраивать как один параметр узла, так и несколько параметров одновременно.

Аргумент `cluster_ip` позволяет настроить IP-адрес частной сети между узлами кластера. Данный параметр обязателен.

```
# Настроить IP-адрес частной сети
wsc> inventory node set node1 cluster_ip 10.120.11.154
```

```
# Удалить IP-адрес частной сети
wsc> inventory node set cluster_ip none
```

Внимание! Вы можете создать кластерный интерфейс с типом VLAN на основе агрегированного bond-интерфейса. Этот bond-интерфейс не допускается использовать как основу для других VLAN-интерфейсов, так как это может привести к выходу из строя кластера. При установке PT AF в кластере на всех узлах должно быть указано одинаковое имя для кластерного интерфейса, например `eth-cluster`.

Аргумент `port` позволяет настроить порт подключения к узлу по SSH.

Внимание! Параметр обязателен, если узел не является локальным. Локальным считается тот узел, на котором выполняется настройка кластера.

```
# Указать порт для подключения к node1 по SSH
wsc> inventory node set node1 port 22013
# Удалить порт для подключения к node1 по SSH
wsc> inventory node set node1 port none
```

Аргумент `ssl_key` позволяет указать расположение файла с закрытым ключом для SSH-аутентификации при подключении к узлу. Для файла с закрытым ключом необходимо настроить права доступа 600, сам ключ не должен быть защищен паролем.

Внимание! Параметр обязателен, если узел не является локальным и не указан пароль пользователя. При использовании аргумента `ssl_key` требуется также настроить пароль `sudo_password`.

```
# Указать путь до закрытого ключа для SSH-аутентификации
wsc> inventory node set node1 ssl_key /root/.ssh/id_rsa
# Удалить информацию о ключе для SSH-аутентификации при подключении к node3
wsc> inventory node set node3 ssl_key none
```

Примечание. Для генерации ключевой пары SSH вы можете использовать утилиту ssh-keygen. При генерации парольную фразу указывать не нужно.

Аргумент `sudo_password` позволяет указать пароль для выполнения команд с правами администратора. Если `sudo_password` не задан, в качестве его значения будет автоматически использован `user_password`.

```
# Настроить пароль для выполнения на узле команд с правами администратора
wsc> inventory node set node1 sudo_password P@ssw0rd
# Удалить пароль для выполнения на узле команд с правами администратора
wsc> inventory node set node1 sudo_password none
```

Аргумент `user_name` позволяет настроить имя пользователя для доступа к узлу по SSH. Параметр обязателен, если узел не является локальным.

```
# Настроить имя пользователя для доступа к узлу
wsc> inventory node set node1 user_name root
# Удалить имя пользователя для доступа к узлу
wsc> inventory node set node1 user_name none
```

Аргумент `user_password` позволяет указать пароль пользователя `user_name` для аутентификации при подключении к узлу по SSH.

Внимание! Параметр обязателен, если узел не является локальным и не указан SSL-ключ.

```
# Настроить пароль для SSH-аутентификации при подключении к node3
wsc> inventory node set node3 user_password P@ssw0rd
# Удалить пароль для SSH-аутентификации при подключении к node3
wsc> inventory node set node3 user_password none
```

Аргумент `role` позволяет настроить роли узла кластера Kubernetes. Доступные значения: `master`, `worker-backend`, `worker-traffic`, `postgresql`, `rabbitmq`, `clickhouse`, `minio`. Каждая роль соответствует определенным службам и сервисам, которые будут созданы на узле кластера. Настройка ролей узла кластера Kubernetes является обязательной, если не настроены внешние сервисы с аналогичной ролью. В кластере должен быть хотя бы один узел с каждой из ролей (`master`, `worker-backend`, `worker-traffic`, `postgresql`, `rabbitmq`, `clickhouse`, `minio`).

Примечание. При назначении узлу кластера роли `master` ему автоматически также назначается роль `etcd`. Вы можете настроить только нечетное количество узлов с ролью `master`, это позволит сохранить работоспособность кластера при отказе части узлов.

```
# Настроить роли для узла кластера node1
wsc> inventory node set node1 role master,worker-backend,worker-
traffic,postgresql,clickhouse,rabbitmq,minio
# Удалить все роли для узла node1
wsc> inventory node set node1 role none
```

Внимание! Роль `clickhouse` должна быть назначена только одному узлу или четному количеству узлов.

inventory check

Команда `inventory check` позволяет проверить корректность настроенных параметров узлов и сервисов.

```
# Выполнить проверку параметров узлов и сервисов
wsc> inventory check
```

inventory render

Команда `inventory render` с аргументом `type` позволяет вывести параметры кластера Kubernetes в заданном формате (JSON или YAML).

```
# Вывести параметры кластера Kubernetes в формате JSON
wsc> inventory render type json
# Вывести параметры кластера Kubernetes в формате YAML
wsc> inventory render type yaml
```

inventory service

Команда `inventory service`, введенная без аргументов, позволяет войти в подсекцию настройки сервисов.

```
# Перейти в подсекцию inventory service
wsc> inventory service
```

inventory service list

Команда `inventory service list` позволяет вывести список всех сервисов и их параметры.

```
# Вывести список сервисов
wsc> inventory service list
```

inventory service add

Команда `inventory service add` позволяет добавить внешний сервис кластера. Имя сервиса определяет его роль: `k8s`, `postgresql`, `rabbitmq`, `clickhouse`, `minio`. Роль `k8s` соответствует ролям `master`, `worker-backend` и `worker-traffic`.

> **Примечание.** Для сборки кластера на основании указанных параметров потребуется также запустить установку infra.

```
# Добавить внешний сервис minio
wsc> inventory service add minio
```

inventory service del

Команда `inventory service del` позволяет удалить сервис кластера.

```
# Удалить внешний сервис minio
wsc> inventory service del minio
```

inventory service set

Команда `inventory service set` позволяет настроить параметры доступа к сервису.

```
# Настройка доступа для сервиса minio
wsc> inventory service set minio address 10.120.11.154:9200 user minio password minio
# Сброс параметров доступа для сервиса minio
wsc> inventory service set minio
```

Аргумент `address` позволяет настроить адрес сервиса. Параметр обязателен для всех сервисов, кроме k8s.

```
# Настроить IP-адрес и порт сервиса k8s
wsc> inventory service set k8s address 10.0.215.3:22013
# Удалить IP-адрес и порт сервиса k8s
wsc> inventory service set k8s
```

Аргумент `config` позволяет указать расположение файла конфигурации сервиса k8s.

Примечание. Файл должен быть скопирован на узел, с которого выполняется настройка кластера.

```
# Указать путь до файла конфигурации
wsc> inventory service set k8s config /root/.kube/config
# Удалить информацию о расположении файла конфигурации
wsc> inventory service set k8s config none
```

Аргумент `user` позволяет указать пользователя для подключения к сервису. Параметр обязателен для всех сервисов, кроме k8s.

```
# Настроить имя пользователя для доступа к сервису minio
wsc> inventory service set minio user minio
# Удалить пользователя для доступа к сервису minio
wsc> inventory service set minio user none
```

Аргумент `password` позволяет настроить пароль пользователя для подключения к сервису. Параметр обязателен для всех сервисов, кроме k8s.

```
# Настроить пароль пользователя для доступа к сервису minio
wsc> inventory service set minio password minio
# Удалить пароль пользователя для доступа к сервису minio
wsc> inventory service set minio password none
```

A.7. Команды генерации ключей SSH

keys

Команда `keys` позволяет войти в секцию `keys` для повторной генерации ключей и сертификатов.

```
# Выполнить вход в секцию keys
wsc> keys
```

keys generate

Команда `keys generate ssh` позволяет повторно сгенерировать ключи SSH на сервере.

```
# Повторно сгенерировать ключи SSH
wsc> keys generate ssh
```

A.8. Команды настройки пула NTP-серверов

ntp

Команда `ntp` без аргументов используется для входа в секцию настройки пула NTP-серверов.

```
# Выполнить вход в секцию ntp
wsc> ntp
```

ntp list

Команда `ntp list` позволяет установить пул NTP-серверов.

```
# Вывести список NTP-серверов
wsc> ntp list
```

ntp list system

Команда `ntp list system` позволяет вывести системную конфигурацию NTP-серверов.

```
# Вывести системную конфигурацию NTP-серверов
wsc> ntp list system
```

ntp add

Команда `ntp add` позволяет добавить один или несколько NTP-серверов.

```
# Добавить NTP-серверы
wsc> ntp add 0.pool.ntp.org 1.pool.ntp.org
wsc> ntp add 1.1.1.1
```

ntp del

Команда `ntp del` позволяет удалить один или несколько NTP-серверов.

```
# Удалить NTP-сервер
wsc> ntp del 0.pool.ntp.org
```

A.9. Команды управления сетевыми маршрутами

route

Команды секции `route` позволяют управлять сетевыми маршрутами. Команда `route`, введенная без аргументов, используется для входа в секцию настройки маршрутизации.

```
# Войти в секцию route
wsc> route
```

route list

Секционная команда `route list` позволяет выводить перечень таблиц маршрутизации со списками включенных в них маршрутов и их свойств. Если команда `route list` введена с аргументом `system`, то в WSC будут показаны только системные параметры маршрутизации. Если команда `route list` введена с аргументом `virtual`, то в WSC будут показаны только параметры маршрутизации прослушиваемых IP-адресов.

```
# Вывести список маршрутов и их свойств
wsc> route list
# Вывести системную конфигурацию маршрутов
```

```
wsc> route list system
# Вывести список маршрутов и их свойства для используемых прослушиваемых IP-адресов
wsc> route list virtual
```

route add

Секционная команда `route add` позволяет добавить статические маршруты в таблицу маршрутизации. Команду нужно вводить в виде `route add <destination> <param1> <value1> [<paramN> <valueN>]`. Вы можете настраивать для одного маршрута несколько параметров одновременно:

```
# Добавить маршрут 10.0.0.0/8 через 192.168.163.2
wsc> route add 10.0.0.0/8 via 192.168.163.2 dev eth-mgmt
```

Примечание. Параметр `dev <interface_name>` обязателен.

```
# Добавить маршрут по умолчанию через 10.120.9.1
wsc> route add default via 10.120.9.1 dev eth-mgmt
```

Команда `route add` с параметром `advmss` позволяет указать максимальный размер сегмента (MSS) для TCP-соединений (в байтах).

```
# Добавить маршрут 10.0.0.0/8 с максимальным размером сегмента 1460
wsc> route add 10.0.0.0/8 dev eth-mgmt advmss 1460
```

Команда `route add` с параметром `dev` позволяет указать интерфейс, через который достижима сеть назначения.

```
# Добавить маршрут 10.11.3.0/24 с порта eth-mgmt
wsc> route add 10.11.3.0/24 dev eth-mgmt
```

Команда `route add` с параметром `dsfield` позволяет указать Differentiated Services Field (DS Field) маршрута.

```
# Добавить маршрут 11.11.11.0/24 с DS Field 0x48
wsc> route add 11.11.11.0/24 dev eth-mgmt dsfield 0x48
```

Команда `route add` с параметром `initcwnd` позволяет задать начальный размер окна перегрузки (в количестве пакетов) при инициализации TCP-соединений по этому маршруту.

```
# Добавить маршрут 10.0.0.0/8 с размером окна перегрузки 10
wsc> route add 10.0.0.0/8 dev eth-mgmt initcwnd 10
```

Команда `route add` с параметром `initrwnd` позволяет задать начальный размер окна приема для TCP-соединений.

```
# Добавить маршрут 172.16.0.0/16 с окном приема 16
wsc> route add 172.16.0.0/16 dev eth-mgmt initrwnd 16
```

Команда `route add` с параметром `metric` позволяет указать метрики маршрута.

```
# Добавить маршрут 172.16.0.0/16 с окном приема 16 и метрикой 10
wsc> route add 172.16.0.0/16 dev eth-ext1 initrwnd 16 metric 10
```

Команда `route add` с параметром `mtu` позволяет настроить максимальный объем данных (MTU), который может быть передан протоколом за одну итерацию.

```
# Добавить маршрут 11.11.11.0/24 с MTU 1460
wsc> route add 11.11.11.0/24 dev eth-mgmt mtu 1460
```

Команда `route add` с параметром `preference` позволяет указать приоритет маршрута.

```
# Добавить маршрут 10.0.0.0/8 с приоритетом 16
wsc> route add 10.0.0.0/8 dev eth-ext1 preference 16
```

Команда `route add` с параметром `proto` позволяет указать идентификатор протокола, по которому был добавлен маршрут.

Примечание. Параметр `proto` может принимать только значение `static`.

```
# Добавить статический маршрут до 172.16.0.0/16
wsc> route add 172.16.0.0/16 dev eth-ext1 proto static
```

Команда `route add` с параметром `realm` позволяет указать номер области маршрута.

```
# Добавить маршрут 10.0.1.3/32 с номером области 6
wsc> route add 10.0.1.3/32 dev eth-ext1 realm 6
```

Команда `route add` с параметром `reordering` позволяет указать максимальное количество пакетов, пришедших в потоке не по порядку, прежде чем будет сделано предположение о том, что пакет был потерян на маршруте.

```
# Добавить маршрут 10.0.1.3/32 с максимальным количеством пакетов 2
wsc> route add 10.0.1.3/32 dev eth-ext1 reordering 2
```

Команда `route add` с параметром `rto_min` позволяет задать минимальное значение задержки повторной передачи для TCP-соединений. Значение необходимо указывать в миллисекундах.

```
# Добавить маршрут 172.16.0.0/16 с rto_min 2
wsc> route add 172.16.0.0/16 dev eth-ext1 rto_min 2
```

Команда `route add` с параметром `rtt` позволяет задать начальное значение времени приема-передачи (round-trip time, RTT) для маршрута. Значение необходимо указывать в миллисекундах.

```
# Добавить маршрут 11.11.11.0/24 с RTT 10
wsc> route add 11.11.11.0/24 dev eth-mgmt rtt 10
```

Команда `route add` с параметром `rttvar` позволяет указать допустимое отклонение от времени кругового обхода. Значение необходимо указывать в миллисекундах.

```
# Добавить маршрут 11.11.11.0/24 с вариацией времени кругового обхода 10
wsc> route add 11.11.11.0/24 dev eth-mgmt rttvar 10
```

Команда `route add` с параметром `scope` позволяет настроить области действия маршрута.

```
# Добавить в таблицу wan маршрут по умолчанию через узел 10.120.9.1 с областью
действия маршрута global
wsc> route add default via 10.120.9.1 dev eth-ext1 table wan scope global
```

Команда `route add` с параметром `src` позволяет указать IP-адрес источника маршрута.

```
# Добавить маршрут 10.0.0.0/8 с адресом источника 10.2.17.64
wsc> route add 10.0.0.0/8 dev eth-ext1 src 10.2.17.64
```

Команда `route add` с параметром `ssthresh` позволяет настроить начальное значение времени замедленного старта. Замедленный старт позволяет избежать перегрузки сети при отправке непропорционально большого сегмента данных. Вы можете применить команду для определения порога срабатывания алгоритмов замедленного старта (`cwnd<ssthresh`) или предотвращения перегрузки (`cwnd>ssthresh`).

```
# Добавить маршрут 172.16.0.0/16 с ssthresh 20
wsc> route add 172.16.0.0/16 dev eth-ext1 ssthresh 20
```

Команда `route add` с параметром `table` позволяет указать таблицу маршрутизации, в которую нужно добавить маршрут. Для создания таблицы маршрутизации используются команды `route table`.

```
# Добавить в таблицу wan маршрут по умолчанию через узел 10.120.9.1
wsc> route add default via 10.120.9.1 dev eth-ext1 table wan
```

Команда `route add` с параметром `tos` позволяет указать тип сервиса (ToS) маршрута.

```
# Добавить маршрут 11.11.11.0/24 с ToS 0x80
wsc> route add 11.11.11.0/24 dev eth-mgmt tos 0x80
```

Команда `route add` с параметром `via` позволяет указать IP-адрес следующего узла маршрута.

```
# Добавить маршрут 10.0.3.0/24 через узел 192.168.1.1
wsc> route add 10.0.3.0/24 via 192.168.1.1 dev eth-ext1
```

route del

Секционная команда `route del` позволяет удалить статические маршруты из таблицы. Команду нужно вводить в виде `route del <destination> [<param1> <value1> [<paramN> <valueN>]]`.

```
# Удалить маршрут для адреса 1.1.1.1 из таблиц маршрутизации rt11 и main
wsc> route del 1.1.1.1 table rt11
wsc> route del 1.1.1.1 table main
# Удалить статический маршрут для сети 172.16.0.0/16 через 10.120.9.1
wsc> route del 172.16.0.0/16 dev eth-ext1 via 10.120.9.1 proto static
```

route rule

Команды секции `route rule` позволяют управлять правилами маршрутизации. Указанная секция является также подсекцией `route`, поэтому вход в нее может быть выполнен как из корневой секции, так и из секции `route`.

route rule list

Секционная команда `route rule list` позволяет вывести список правил маршрутизации.

```
# Вывести список правил маршрутизации
wsc> route rule list
```

Команда `route rule list` с аргументов `system` позволяет вывести правила маршрутизации системной конфигурации.

```
# Вывести системную конфигурацию правил
wsc> route rule list system
```

route rule add

Секционная команда `route rule add` позволяет создать правило маршрутизации с заданными параметрами. Вы можете настроить один параметр или несколько параметров правила одновременно:

```
# Добавить правило маршрутизации с приоритетом 444 и адресом отправителя
10.10.0.10/32. При соответствии правилу будет проверяться таблица маршрутизации
mytable
wsc> route rule add eth-ext1 from 10.10.0.10/32 pref 444 table mytable
```

Команда `route rule add` с параметром `from` позволяет указать IP-адреса отправителей трафика, соответствующего правилу маршрутизации.

```
# Добавить правило маршрутизации с адресом отправителя 10.120.9.77. При соответствии
правилу будет проверяться таблица маршрутизации wan
wsc> route rule add eth-ext1 from 10.120.9.77 table wan
```

Команда `route rule add` с параметром `fwmark` позволяет указать метку трафика, соответствующего правилу маршрутизации.

```
# Добавить правило маршрутизации с адресом отправителя 10.120.9.145 и меткой трафика
0x40. При соответствии правилу будет проверяться таблица маршрутизации wan
wsc> route rule add eth-mgmt from 10.120.9.145 table wan fwmark 0x40
```

Команда `route rule add` с параметром `iif` позволяет указать входящий интерфейс трафика, соответствующего правилу маршрутизации.

```
# Добавить правило маршрутизации с адресом получателя 10.120.9.77 и интерфейсом eth-
ext1. При соответствии правилу будет проверяться таблица маршрутизации wan
wsc> route rule add eth-ext1 to 10.120.9.77 iif eth-ext1 table wan
```

Команда `route rule add` с параметром `oif` позволяет указать исходящий интерфейс трафика, соответствующего правилу маршрутизации.

```
# Добавить правило маршрутизации с адресом получателя 10.120.9.77 и интерфейсом eth-
ext1. При соответствии правилу будет проверяться таблица маршрутизации wan
wsc> route rule add eth-ext1 to 10.120.9.77 oif eth-ext1 table wan
```

Команда `route rule add` с параметром `pref` позволяет указать приоритет правила. Если параметр не указан, значение будет сгенерировано автоматически.

Примечание. Значение параметра `pref` каждого правила должно быть уникальным.

```
# Создать правило маршрутизации с приоритетом 101 и адресом отправителя
10.10.0.10/32. При соответствии правилу будет проверяться таблица маршрутизации
mytable
wsc> route rule add eth-ext1 from 10.10.0.10/32 pref 101 table mytable
```

Команда `route rule add` с параметром `table` позволяет указать таблицу, которая будет использоваться для маршрутизации трафика, соответствующего настраиваемому правилу.

```
# Добавить правило маршрутизации с адресом отправителя 10.1.1.77. При соответствии
правилу будет проверяться таблица маршрутизации wan
wsc> route rule add eth-mgmt from 10.1.1.77 table wan
```

Команда `route rule add` с параметром `to` позволяет указать IP-адреса получателей трафика, соответствующего правилу маршрутизации.

```
# Добавить правило маршрутизации с адресом получателя 10.120.9.77. При соответствии
правилу будет проверяться таблица маршрутизации wan
wsc> route rule add eth-ext1 to 10.120.9.77 table wan
```

Команда `route rule add` с параметром `tos` позволяет указать тип сервиса (ToS) трафика, соответствующего правилу маршрутизации.

```
# Добавить правило маршрутизации с адресом отправителя 10.120.9.77 и ToS 0x4. При
соответствии правилу будет проверяться таблица маршрутизации wan
wsc> route rule add eth-ext1 from 10.120.9.77 tos 0x4 table wan
```

route rule del

Секционная команда `route rule del` позволяет удалить одно или несколько правил маршрутизации с указанным значением параметра `pref`. Вы можете просмотреть `pref`, используя команду `route rule list`.

```
# Удалить правило маршрутизации с приоритетом 444
wsc> route rule del 444
# Удалить правила маршрутизации с приоритетами 10, 11, 34
wsc> route rule del 10 11 34
```

route table

Команды секции `route table` позволяют управлять таблицами маршрутизации. Указанная секция является подсекцией `route`, поэтому вход в нее может быть выполнен как из корневой секции, так и из секции `route`.

route table add

Команда `route table` с аргументом `add` позволяет создать таблицы маршрутизации с именем `<name>` и номером `<id>`. Если номер таблицы не указан, он будет назначен автоматически.

Примечание. Таблицы маршрутизации с номерами 0—126 и 250 зарезервированы в системных целях.

```
# Создать таблицу маршрутизации с именем mytable и номером 128
wsc> route table add mytable 128
```

route table del

Команда `route table` с аргументом `del` позволяет удалить одну или несколько таблиц маршрутизации.

```
# Удалить таблицу маршрутизации
wsc> route table del mytable
# Удалить таблицы маршрутизации lan и wan
wsc> route table del wan lan
```

route table list

Команда `route table list` позволяет вывести список всех таблиц маршрутизации.

```
# Вывести список таблиц маршрутизации
wsc> route table list
```

Команда `route table list` с аргументом `system` позволяет вывести таблицы маршрутизации трафика.

```
# Вывести таблицы маршрутизации
wsc> route table list system
```

См. также

Особенности маршрутизации исходящего трафика (см. раздел 17.12)

A.10. Команды настройки виртуальных IP-адресов

Команды секции `vip` позволяют выбрать балансировщик нагрузки, а также настроить виртуальные IP-адреса (VIP-адреса) и порты, которые анонсируются внутренним балансировщиком для сервисов кластера Kubernetes. После развертывания PT AF вы можете настраивать виртуальные IP-адреса на любом узле кластера.

Примечание. Настраивать маршруты не требуется, если трафик поступает с устройства (например, обратного прокси-сервера), которое находится с PT AF в одной сети на уровне L3. Если устройство находится в другой подсети или используется NGFW, который перенаправляет трафик без использования SNAT, необходимо настроить маршрут по умолчанию или маршрут к сетям, в которых находится устройство (если их количество ограничено).

vip

Команда используется для входа в секцию `vip`.

vip list

Команда выводит тип используемого балансировщика нагрузки, а также VIP-адреса и порты, которые анонсируются внутренним балансировщиком.

vip set

Команда позволяет выбрать балансировщик нагрузки, а также настроить VIP-адреса и порты, которые анонсируются внутренним балансировщиком. Для применения изменений необходимо после настройки выполнить команду `config commit`.

Параметры команды:

— **load_balancer.** Тип балансировщика нагрузки: `metallb` — внутренний балансировщик MetalLB (по умолчанию), `external` — внешний балансировщик.

— **border.** Виртуальный IP-адрес и порт для взаимодействия сервиса Border с агентами.

Примечание. Если вы измените IP-адрес и порт, связь между PT AF и агентом прервется. Для ее восстановления потребуется обновить строку подключения на агенте (строку можно получить в веб-интерфейсе PT AF).

— **manage.** Виртуальный IP-адрес и порт для доступа к веб-интерфейсу PT AF и взаимодействия с REST API.

— **monitoring.** Виртуальный IP-адрес и порт для доступа к веб-интерфейсу Grafana.

Вы можете не указывать номера портов. В этом случае будут использованы порты по умолчанию: 443 — для доступа к веб-интерфейсу PT AF, 3000 — для доступа к веб-интерфейсу Grafana, 8443 — для взаимодействия PT AF с агентами. Вы можете настраивать как один параметр, так и несколько параметров одновременно.

Примеры:

```
wsc> vip set load_balancer external
wsc> vip set border 192.0.2.171
wsc> vip set load_balancer metallb border 192.0.2.171:151 manage 192.0.2.52:423
monitoring 192.0.2.89:128
```

A.11. Часто задаваемые вопросы о работе с WSC

В этом разделе даны ответы на часто задаваемые вопросы, связанные с использованием оболочки WSC.

Как просмотреть журнал событий WSC

Общий журнал событий WSC хранится в файле `/var/log/ptaf/wsc-daemon.log`.

Журнал, который PT AF ведет при выполнении команд применения конфигурации, например таких, как `config commit` или `config commit force`, хранится в файле `/var/log/ptaf/wsc-config-commit.log`.

Как запустить команды без входа в WSC

Если требуется выполнить команды без входа в WSC, вы можете воспользоваться параметром `-c` или `--command`, указав в кавычках нужную команду. Например:

```
$ sudo wsc -c "inventory node add <hostname>"
```

Также для выполнения команды без входа в WSC вы можете использовать конвейер Linux. Например:

```
$ sudo echo "inventory node add <hostname>" | wsc
```

Как запустить скрипт в WSC

WSC поддерживает чтение переданного файла, в котором описаны команды. Например, вы можете создать файл `add_routes.wsc`, содержащий описание следующих команд:

```
# Add routes and commit
route add default via 10.120.9.1 dev eth-ext1 table wan
config commit
```

Вы можете применить созданный файл в WSC следующим способом:

```
$ sudo wsc add_routes.wsc
```

При использовании шебанга указанный скрипт `add_routes.wsc` можно представить в виде:

```
#!/usr/local/bin/wsc
# Add routes and commit
route add default via 10.120.9.1 dev eth-ext1 table wan
config commit
```

Вы можете запустить созданный скрипт в WSC следующим способом:

```
$ chmod +x add_routes.wsc
$ ./add_routes.wsc
```

Как в WSC изменить формат выводимых данных на JSON

Вы можете изменить формат всех выводимых данных на JSON в запускаемой оболочке WSC с помощью параметра `--json`:

```
$ sudo wsc --json
```

Приложение Б. Справочник по языку пользовательских правил

В общем случае пользовательское правило состоит из двух частей: секции для определения локальных переменных и секции с логикой обработки HTTP-запроса или HTTP-ответа.



Рисунок 18. Структура пользовательского правила

Секция для определения локальных переменных (см. приложение Б.1) начинается с ключевого слова `with` и содержит одно или несколько выражений для определения переменных. Секция является необязательной.



Рисунок 19. Пример секции для определения локальных переменных

Секция с логикой обработки HTTP-запроса (ответа) начинается с ключевого слова `if` и содержит условие, которое формируется из одного или нескольких логических выражений (предикатов), объединяемых с помощью логических операторов `and`, `or`, `not` и круглых скобок.



Рисунок 20. Пример секции с логикой обработки HTTP-запроса (ответа)

Результатом вычисления условия является логическая истина или ложь. Если условие истинно, правило считается сработавшим и система выполнит действия, связанные с правилом, согласно его приоритету. Если условие ложно, правило не сработает и никаких действий, связанных с правилом, выполняться не будет.

Предикат состоит из контекстной переменной (см. приложение Б.1) (или ссылки на нее через локальную переменную), набора преобразований (см. приложение Б.2) над переменной, оператора сравнения (см. приложение Б.3) и аргумента.

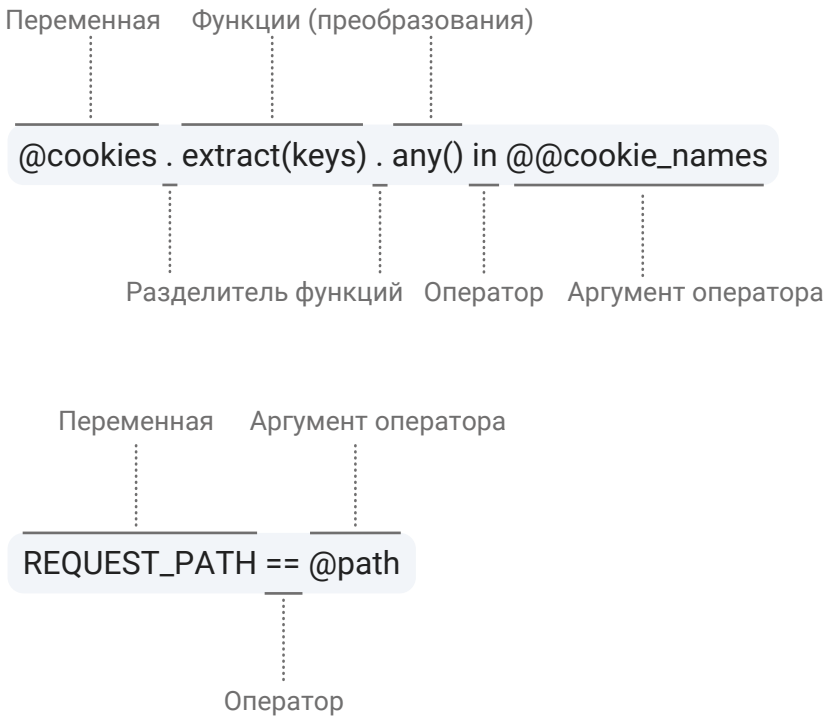


Рисунок 21. Примеры предикатов

При вычислении предиката выбирается часть HTTP-запроса (ответа), при необходимости последовательно преобразуется с помощью функций и сравнивается с аргументом оператора. Результатом вычисления предиката является логическая истина или ложь. Функции и аргумент необязательны и могут отсутствовать в предикате.

В этом разделе

Переменные (см. приложение Б.1)

Функции (см. приложение Б.2)

Операторы (см. приложение Б.3)

Типы данных (см. приложение Б.4)

Прочие элементы языка (см. приложение Б.5)

Б.1. Переменные

В языке пользовательских правил переменные можно разделить по размерности значений и по способу определения.

По размерности значений переменные делятся на скалярные и векторные. Скалярные переменные могут иметь только одно значение, векторные содержат множество однотипных значений.

По способу определения переменные делятся на локальные, контекстные и параметры правила.

В этом разделе

Локальные переменные (см. приложение Б.1.1)

Параметры правила (см. приложение Б.1.2)

Контекстные переменные (см. приложение Б.1.3)

Б.1.1. Локальные переменные

Определяются в коде правила в секции `with` с помощью выражения:

```
@<Имя переменной> = <Значение переменной>
```

В имени локальной переменной можно указывать только цифры, латинские буквы и знак подчеркивания. Имя регистрозависимое и не должно начинаться с цифры.

В значении переменной можно указывать литералы доступных типов (см. приложение Б.4), а также можно ссылаться на другие локальные или контекстные переменные. Поскольку обработка выражений выполняется в порядке их следования, значение локальной переменной, на которую ссылается выражение, должно быть уже определено в предыдущем выражении. Выражения нужно разделять запятой.

Примеры определения локальных переменных:

```
with
  @path = "/test.php",
  @status_code = 200,
  @client_ip = 192.0.2.7,
  @list_auth = ["/v1/authenticate", "/v2/authenticate", "/v3/auth"],
  @regex = ~"\\.(?:bat|exe|scr|vbs|htm|php|asp)",
  @context_var = REQUEST_GET,
  @other_list = @list_auth
```

Б.1.2. Параметры правила

Определяются в карточке правила (см. раздел 10.9) в блоке параметров **Конфигурация правила**.

В имени параметра можно указывать только цифры, латинские буквы и знак подчеркивания. Имя регистрозависимое и не должно начинаться с цифры. В значении параметра можно указывать строку, целое число, булево значение, список строк или целых чисел, а также глобальный список.

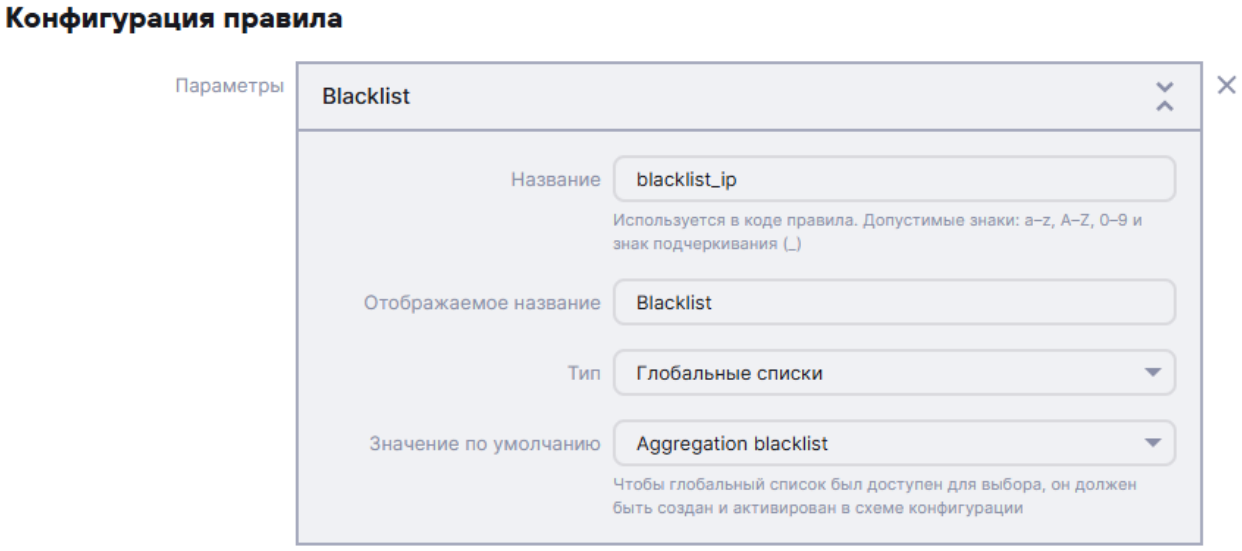


Рисунок 22. Пример определения параметра через глобальный список

Параметр используется в коде правила в секции `if`, перед его названием указывается префикс `@@`.

Пример использования параметров правила в коде:

```
if @cookies.extract(keys).any() in @@cookie_names and not CLIENT_IP in @@blacklist_ip
```

Б.1.3. Контекстные переменные

Перечень переменных формируется производителем системы. Значения определяются на основе HTTP-запроса и HTTP-ответа.

Некоторые векторные контекстные переменные содержат набор элементов, каждый из которых состоит из двух или трех строк: «ключ — значение» или «ключ — значение — имя файла». Такие переменные (словарь строк) имеют размерность (ранк), отличную от остальных переменных: равную двум для набора «ключ — значение», трем — для «ключ — значение — имя файла». Остальные векторные контекстные переменные и все скалярные имеют ранк, равный единице.

Ниже приведено описание контекстных переменных.

CLIENT_BROWSER_NAME

Название браузера клиента.

Определяется на основе заголовка User-Agent. Если система не определила название браузера, переменной присваивается значение `Other`.

Скалярная переменная, тип данных — строковый.

Пример заголовка:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36 Edge/115.101.1901.188
```

Значение переменной:

```
Edge
```

CLIENT_BROWSER_VERSION

Версия браузера клиента.

Определяется на основе заголовка User-Agent.

Скалярная переменная, тип данных — строковый.

Пример заголовка:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36 Edge/115.101.1901.188
```

Значение переменной:

```
115.101
```

CLIENT_CITY

Название города.

Определяется на основе IP-адреса клиента и базы GeoIP-данных.

> **Примечание.** Для определения страны, региона и города в PT AF, начиная с версии 4.1.8, используется база GeoIP от российского Главного радиочастотного центра.

Скалярная переменная, тип данных — строковый.

Пример:

```
Vladivostok
```

CLIENT_COUNTRY

Двухбуквенный код страны.

Определяется на основе IP-адреса клиента и базы GeoIP-данных.

> **Примечание.** Для определения страны, региона и города в PT AF, начиная с версии 4.1.8, используется база GeoIP от российского Главного радиочастотного центра.

Скалярная переменная, тип данных — строковый.

Пример:

```
RU
```

Пример предиката:

```
# Клиент не из России
CLIENT_COUNTRY != "RU"
```

CLIENT_IP

IP-адрес клиента.

Скалярная переменная, тип данных — IP-адрес.

Пример:

```
192.0.2.45
```

Примеры предикатов:

```
CLIENT_IP in [10.0.0.1, 8.8.8.8]
CLIENT_IP == 8.8.8.8

# Не поддерживается указание подсети в формате 10.0.0.0/8. Нужно использовать
статический список, содержащий подсеть 10.0.0.0/8
CLIENT_IP in @@static_list
```

CLIENT_OS_NAME

Семейство операционной системы рабочей станции клиента.

Определяется на основе заголовка User-Agent.

Скалярная переменная, тип данных — строковый.

Пример заголовка:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36 Edge/115.101.1901.188
```

Значение переменной:

```
Windows
```

CLIENT_PROTO

Протокол соединения.

Скалярная переменная, тип данных — строковый.

Возможные значения: `HTTP` и `HTTPS`.

CLIENT_REGION

Регион клиента внутри страны.

Определяется на основе IP-адреса клиента и базы GeoIP-данных.

> **Примечание.** Для определения страны, региона и города в PT AF, начиная с версии 4.1.8, используется база GeoIP от российского Главного радиочастотного центра.

Скалярная переменная, тип данных — строковый.

Пример:

```
Primorye
```

REQUEST_BODY

Тело запроса.

Скалярная переменная, тип данных — строковый.

Пример:

```
grant_type=authorization_code&redirect_uri=http://localhost/&code=NSfkD2aJBpcS-YU5NSErE1-4U_TKeWrlo45H5GZUAqP13tHUrUkawPMk_cF3Vbrr7hbypqc_TgBkdsnL2A9uSkzBKDeovvd4X6y2Kwr8kwU
```

REQUEST_COOKIES

Сессионные куки запроса.

Определяется на основе заголовка Cookie и содержит набор пар «ключ — значение».

Векторная переменная, тип данных — строковый.

Пример заголовка:

```
Cookie: PHPSESSID=486zf09hf012fh2; csrftoken=d89t4o3tb3gg43
```

Значение переменной:

```
[("PHPSESSID", "486zf09hf012fh2"), ("csrftoken", "d89t4o3tb3gg43")]
```

Примеры предикатов:

```
REQUEST_COOKIES . select(~"(?i:user_id)") . extract(values) . map(base64_decode) .
any() matches ~"(ping)"

# Значение куки Authorization содержит Basic (независимо от регистра)
REQUEST_COOKIES . select(~"(?i:authorization)") . extract(values) . map(lowercase) .
any() matches "basic"
```

REQUEST_FILES

Информация о файлах в составных (multipart) запросах.

Определяется на основе заголовка Content-Disposition и содержит набор данных «ключ — значение — имя файла».

Векторная переменная, тип данных — строковый.

Пример заголовков:

```
Content-Disposition: form-data; name="AttachedFile1"; filename="logo.svg"
Content-Type: application/svg

<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
...
----------------------65487651324676543
Content-Disposition: form-data; name="AttachedFile2"; filename="wallet.txt"
Content-Type: text/plain

1GXPWTNnVC8boQeX6HEiaimGNf374iJZmj
----------------------65487651324676543
...
```

Значение переменной:

```
[("AttachedFile1", "<?xml version="1.0" standalone="no"?><!DOCTYPE...", "logo.svg"),
("AttachedFile2", "1GXPWTNnVC8boQeX6HEiaimGNf374iJZmj", "wallet.txt"), ...]
```

REQUEST_GET

Параметры запроса, передаваемые в URI (GET-параметры запроса).

Определяется на основе URI в стартовой строке запроса и содержит набор пар «ключ — значение».

Векторная переменная, тип данных — строковый.

Пример стартовой строки запроса:

```
GET /shop/catalog?page=2&items=15 HTTP/1.1
```

Значение переменной:

```
[("page", "2"), ("items", "15")]
```

REQUEST_HEADERS

Заголовки запроса.

Определяется на основе заголовков запроса и содержит набор пар «ключ — значение».

Векторная переменная, тип данных — строковый.

Пример заголовков:

```
Authorization: Basic dGVzdF93YW...
Host: example.com
Content-Length: 173
Content-Type: application/x-www-form-urlencoded
...
```

Значение переменной:

```
[("Authorization", "Basic dGVzdF93YW..."), ("Host", "example.com"), ("Content-
Length", "173"), ("Content-Type": "application/x-www-form-urlencoded"), ...]
```

Примеры предикатов:

```
#Заголовок User-Agent содержится в запросе. Название заголовка ищется без учета
регистра
REQUEST_HEADERS . select(~"(?i:User-Agent)") . exists()


#Значение заголовка Referer содержит .php. Название заголовка ищется без учета
регистра, значение — приводится к нижнему регистру
REQUEST_HEADERS . select(~"(?i:Referer)") . extract(values) . map(lowercase) . any()
matches ".php"


#Значение заголовка Host равно example.com(точно совпадает). Название заголовка
ищется без учета регистра
REQUEST_HEADERS . select(~"(?i:host)") . extract(values) . map(lowercase) . any() ==
"example.com"


#Значение заголовка Accept равно text/html(точно совпадает). Название заголовка
ищется без учета регистра
REQUEST_HEADERS . select(~"(?i:Accept)") . extract(values) . any() == "text/html"


#Значение заголовка Authorization содержит Basic (с учетом регистра)
REQUEST_HEADERS . select("Authorization") . extract(values) . any() matches "Basic"
```

```
#Значение заголовка Authorization содержит basic. Название заголовка ищется без учета регистра, значение — приводится к нижнему регистру
REQUEST_HEADERS . select(~"(?i:authorization)") . extract(values) . map(lowercase) . any() matches "basic"
```

REQUEST_HTTP_VERSION

Версия HTTP.

Определяется на основе стартовой строки запроса.

Скалярная переменная, тип данных — строковый.

Пример стартовой строки запроса:

```
GET /shop/catalog?page=2&items=15 HTTP/1.1
```

Значение переменной:

```
HTTP/1.1
```

REQUEST_METHOD

Метод запроса.

Определяется на основе стартовой строки запроса.

Скалярная переменная, тип данных — строковый.

Пример стартовой строки запроса:

```
GET /shop/catalog?page=2&items=15 HTTP/1.1
```

Значение переменной:

```
GET
```

Примеры предикатов:

```
REQUEST_METHOD == "GET"
REQUEST_METHOD in ["GET","POST"]
```

REQUEST_PATH

Путь к ресурсу.

Определяется на основе стартовой строки запроса.

Скалярная переменная, тип данных — строковый.

Пример стартовой строки запроса:

```
GET /shop/catalog?page=2&items=15 HTTP/1.1
```

Значение переменной:

```
/shop/catalog
```

Примеры предикатов:

```
REQUEST_PATH matches "flogout.aspx"
REQUEST_PATH matches ~"\\.git"

# Значения /bitrix/access_user.php и /bitrix/accesson.php нужно указывать в нижнем регистре, поскольку применяется преобразовани map(lowercase)
REQUEST_PATH . map(lowercase) in ["/bitrix/access_user.php", "/bitrix/accesson.php"]
```

REQUEST_POST

Параметры запроса в теле (POST-параметры).

Определяется на основе тела запроса и содержит набор пар «ключ — значение».

Векторная переменная, тип данных — строковый.

Пример тела запроса:

```
login=user&password=P@ssw0rd
```

Значение переменной:

```
[("login", "user"), ("password", "P@ssw0rd")]
```

REQUEST_QUERY

Строка с параметрами запроса.

Определяется на основе стартовой строки запроса.

Скалярная переменная, тип данных — строковый.

Пример стартовой строки запроса:

```
GET /shop/catalog?page=2&items=15 HTTP/1.1
```

Значение переменной:

```
page=2&items=15
```

Пример предиката:

```
REQUEST_QUERY . map(lowercase) matches "cmd=read"
```

REQUEST_SIZE

Размер запроса в байтах.

Скалярная переменная, тип данных — целочисленный.

Пример:

```
429
```

REQUEST_URI

URI запроса.

Определяется на основе стартовой строки запроса.

Скалярная переменная, тип данных — строковый.

Пример стартовой строки запроса:

```
GET /shop/catalog?page=2&items=15 HTTP/1.1
```

Значение переменной:

```
/shop/catalog?page=2&items=15
```

RESPONSE_BODY

Тело ответа.

Скалярная переменная, тип данных — строковый.

Пример:

```
<html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The
requested URL was not found on this server.</p><hr><address>Apache/2.4.54 (Debian)
Server at example.com Port 8181</address></body></html>
```

RESPONSE_HEADERS

Заголовки ответа.

Определяется на основе заголовков ответа и содержит набор пар «ключ — значение».

Векторная переменная, тип данных — строковый.

Пример заголовков:

```
Content-Type: text/html; charset=iso-8859-1
Content-Length: 290
Connection: close
...
```

Значение переменной:

```
[("Content-Type", "text/html; charset=iso-8859-1"), ("Content-Length", "290"),
("Connection", "close"), ...]
```

RESPONSE_SIZE

Размер ответа в байтах.

Скалярная переменная, тип данных — целочисленный.

Пример:

```
115
```

RESPONSE_STATUS_CODE

Код ответа.

Определяется на основе стартовой строки ответа.

Скалярная переменная, тип данных — целочисленный.

Пример стартовой строки ответа:

```
HTTP/1.1 200 OK
```

Значение переменной:

```
200
```

Б.2. Функции

Функции предназначены для выбора определенной части HTTP-запроса (ответа) и (или) ее преобразования. Каждая функция получает входные данные, определенной размерности (см. приложение Б.1) и ранка (см. приложение Б.1.3), преобразует и передает их следующей функции для обработки или оператору для сравнения с аргументом.

Применение функции может изменить размерность и ранк преобразуемых данных (текущего контекста), которые в начале вычисления предиката равны размерности и ранку контекстной переменной. Несоответствие размерности или ранка входных данных со спецификацией функции приведет к ошибке в работе правила. Особенно это нужно учитывать в том случае, когда предикат состоит из нескольких функций.

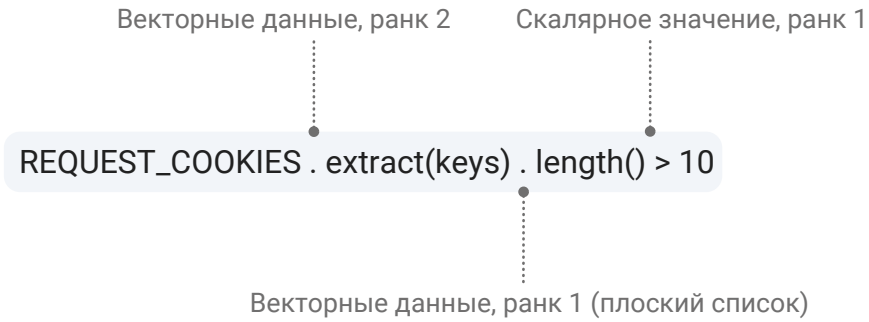


Рисунок 23. Изменение текущего контекста

Ниже описаны функции языка пользовательских правил.

all

Определяет логику применения оператора, следующего за функцией. Результатом сравнения будет логическая истина, если сравнение аргумента с каждым элементом списка возвращает истину. В ином случае результатом сравнения будет логическая ложь.

Применяется только к плоскому списку (с единичным ранком) и указывается последней функцией в предикате. Не имеет аргументов.

> **Примечание.** При обработке пустого множества функция `all` всегда возвращает `False` независимо от оператора, следующего за ней. Если такой логический результат затем инвертируется в правиле (что приводит к его срабатыванию), в карточке события будет отсутствовать блок с совпадшими переменными.

```
# Примеры предикатов
REQUEST_COOKIES . select("Example cookie name") . extract(values) . map(length) . all() > 0
REQUEST_GET . extract(values) . all() matches ~"[\\s\\S]?"
REQUEST_POST . select("page") . extract(values) . all() matches ~\\d
# Правило сработает на запрос, в котором хотя бы один GET-параметр не соответствует регулярному выражению или в котором вовсе отсутствуют GET-параметры
if NOT REQUEST_GET . extract(values) . all() matches ~"[\\s\\S]?"
# Если требуется, чтобы правило не срабатывало на запрос без GET-параметров, нужно добавить через AND дополнительное условие.
if NOT REQUEST_GET . extract(values) . all() matches ~"[\\s\\S]?"
AND
REQUEST_GET . extract(values) . length() > 0
# Правило сработает на запрос, в котором хотя бы один POST-параметр "page" не содержит цифры или в котором вовсе отсутствует POST-параметр "page".
if NOT REQUEST_POST . select("page") . extract(values) . all() matches ~"\\d"
# Если требуется, чтобы правило не срабатывало на запрос без POST-параметра "page", нужно добавить через AND дополнительное условие
if NOT REQUEST_POST . select("page") . extract(values) . all() matches ~"\\d"
   AND
   REQUEST_POST . select("page") . extract(values) . length() > 0
```

any

Определяет логику применения оператора, следующего за функцией. Результатом сравнения будет логическая истина, если сравнение аргумента с хотя бы одним элементом списка возвращает истину. В ином случае результатом сравнения будет логическая ложь.

Применяется только к плоскому списку (с единичным ранком) и указывается последней функцией в предикате. Не имеет аргументов.

> **Примечание.** При обработке пустого множества функция `any` всегда возвращает `False` независимо от оператора, следующего за ней. Если такой логический результат затем инвертируется в правиле (что приводит к его срабатыванию), в карточке события будет отсутствовать блок с совпадшими переменными.

```
# Примеры предикатов
REQUEST_HEADERS . select("x-app-version") . extract(values) . any() == "6.1.0"
REQUEST_GET . extract(values) . any() matches ~"[\\s\\S]?"
REQUEST_POST . select("page") . extract(values) . any() matches ~\\d
# Правило сработает при отсутствии в запросе POST-параметра "page"
if NOT REQUEST_POST . select("page") . extract(values) . map(length) . any() < 0
```

```
# Правило сработает на запрос, в котором значение хотя бы одного GET-параметра равно "pass" или в котором вовсе отсутствуют GET-параметры
if NOT REQUEST_GET . extract(values) . any() == "pass"
# Если требуется, чтобы правило не срабатывало на запрос без GET-параметров, нужно добавить через AND дополнительное условие
if NOT REQUEST_GET . extract(values) . any() == "pass"
   AND
   REQUEST_GET . extract(values) . length() > 0
```

first

Возвращает первый элемент списка (скалярное значение). Если список не содержит элементов, возвращает пустое значение.

Функция `first` позволяет применять другие функции. Например, позволяет применять функцию `json_path` для обработки GET-параметров, а также других векторных значений в запросе. Поскольку элементы списка не упорядочены, для корректного применения функции `first` нужно предварительно преобразовать список таким образом, чтобы в списке остался один элемент.

```
# Пример предиката
REQUEST_HEADERS . select("Host") . extract(values) . first()
# Результат преобразования
[("Authorization","Basic dGVzdF93YW..."),("Host","example.com"),...] →
[("Host","example.com")] → [("example.com")] → "example.com"
```

json_path

Извлекает значения из строки с данными в формате JSON. Аргумент функции — выражение на языке запросов JSONPath. Результат функции — строка.

Если входные данные не соответствуют формату JSON, функция возвращает пустое значение. Если результат функции содержит данные разной структуры (например, и строки, и объекты), они упорядочиваются в массив.

Особенности и ограничения функции:

— Валидация выражения на языке JSONPath не выполняется. Если в выражении допущена опечатка, при обработке трафика правило не сработает, и пользователь не получит об этом уведомлений. Перед применением правила внимательно проверьте синтаксис выражения и убедитесь, что оно синтаксически корректно и соответствует тем конструкциям JSON, для которых оно предназначено.

— При обработке JSONPath-выражений не поддерживается обращение к узлу, который находится после условия фильтрации `[?(@...)]` (например, обращение к узлу `id` в выражении `$.items[?(@.price == 10)].id`). Рекомендуется разделять такие выражения на несколько частей, каждая из которых может содержать не более одного условия в конце, и последовательно обрабатывать каждую часть с помощью функции `json_path`.

  Например:

`json_path("$.items[?(@.price == 10)].id")` → `json_path("$.items[?(@.price == 10)]") . json_path("$.id")`.

— Поскольку результат функции `json_path` сериализуется библиотекой стороннего производителя, для поиска объектов лучше использовать сравнение с подстрокой или с регулярным выражением, а не точное совпадение. В текущей версии языка все незначащие пробельные символы удаляются из результата функции `json_path`.

```
# Тело запроса
{
  "items": [
    {"id": 1, "name": "A", "price": 10},
    {"id": 2, "name": "B", "price": 5}
  ]
}

# Пример предиката
REQUEST_BODY . json_path("$.items[?(@.price == 10)]")
# Результат
{"id":1,"name":"A","price":10}

# Пример предиката
REQUEST_BODY . json_path("$.items[0].name")
# Результат
A

# Пример предиката
REQUEST_BODY . json_path("$.items[?(@.price>1)]")
# Результат
[{"id":1,"name":"A","price":10},{"id":2,"name":"B","price":5}]

# Пример предиката
REQUEST_BODY . json_path("$.items[?(@.price<6)]") . json_path("$.name")
# Результат
B

# Пример предиката
REQUEST_BODY . json_path("$..name")
# Результат
["A","B"]
```

extract

Преобразует список с ранком больше единицы (словарь строк) к «плоскому» списку (с единичным ранком).

Входными данными функции являются наборы элементов «ключ — значение» и «ключ — значение — имя файла». Аргументы функции определяют извлекаемую проекцию: `keys` — извлекаются ключи, `values` — значения, `filenames` — имена файлов. Можно указывать более одного аргумента.

```
# Пример предиката
REQUEST_HEADERS . extract(keys)
# Результат преобразования
[("Authorization","Basic dGVzdF93YW..."),("Host","example.com"),...] →
["Authorization","Host",...]
# Пример предиката
REQUEST_HEADERS . extract(keys,values)
# Результат преобразования
[("Authorization","Basic dGVzdF93YW..."),("Host","example.com"),...] →
["Authorization","Basic dGVzdF93YW...","Host","example.com",...]
```

length

Вычисляет длину строки (для скалярных значений) или количество элементов в списке (для векторных данных).

Результат вычисления — целое число. Не имеет аргументов.

```
# Примеры предикатов
# Проверка количества символов в пути к ресурсу
REQUEST_PATH . length() > 10
# Проверка количества POST-параметров
REQUEST_POST . length() > 10
# Количество заголовков больше одного
REQUEST_HEADERS . length() gt 1
# В URI больше 30 GET-параметров
REQUEST_GET . length() gt 30
# Длина пути к ресурсу больше одного символа
REQUEST_PATH . length() gt 1
```

map

Преобразует строковые данные: в зависимости от аргумента функция может декодировать их, приводить к нижнему или верхнему регистру, а также вычислять длину строки. Возможные аргументы:

— **base64_decode.** Декодирует данные, закодированные по стандарту Base64.

— **hex_decode.** Декодирует данные, закодированные шестнадцатеричным кодом.

— **html_entity_decode.** Декодирует HTML-сущности.

— **url_decode.** Декодирует URL.

— **lowercase.** Приводит строку к нижнему регистру.

— **uppercase.** Приводит строку к верхнему регистру.

— **lenght.** Вычисляет длину строки или количество элементов в списке.

```
# Примеры предикатов
REQUEST_PATH . map(length) > 10
REQUEST_GET . extract(values) . map(length) > 5


# Можно указать несколько аргументов. В этом случае преобразование выполняется последовательно в порядке перечисления аргументов слева направо
REQUEST_GET . extract(values) . map(html_entity_decode, base64_decode) . map(hex_decode, url_decode) . any() == "Example string"


# Сработает на заголовках Host: example.com, Host: Example.com, host: example.com и hOst: example.com
# Не сработает на заголовках host: eexample.com и host: eexample.coms
REQUEST_HEADERS . map(lowercase) . select(~"(?i:Host)") . extract(values) . any() == "example.com"
REQUEST_HEADERS . map(lowercase) . select(~"(?i:Host)") . extract(values) . any() matches ~"^(?i)(example\.com)$"


# Не сработает, поскольку значение, преобразованное функцией map(lowercase) в нижний регистр, сравнивается с "Example.com" в верхнем регистре
REQUEST_HEADERS . map(lowercase) . select(~"(?i:Host)") . extract(values) . any() == "Example.com"


# Функция map(lowercase)преобразует значение переменной REQUEST_URI в нижний регистр, чтобы не указывать регистрозависимое регулярное выражение
REQUEST_URI . map(lowercase) matches ~"(ftp://|http://|https://|{.+include.+exit.+})"
```

select

Фильтрует список с ранком больше единицы (словарь строк) по точному совпадению со строкой или по регулярному выражению.

В результате фильтрации возвращается список, составные элементы которого обязательно соответствуют аргументу функции (содержат строку или соответствуют регулярному выражению). При этом ранк списка остается прежним.

```
# Пример предиката
REQUEST_HEADERS . select("Host")
# Результат преобразования
[("Authorization","Basic dGVzdF93YW..."),("Host","example.com"),...] →
[("Host","example.com")]


# Пример предиката
REQUEST_HEADERS . select(~"(?i:Host)") . extract(values) . any() matches "example.com"


# Заголовок Referer имеет пустое значение
```

```
REQUEST_HEADERS . select(~"Referer") . length() == 0

# Список разрешенных значений заголовков
REQUEST_HEADERS . select(~"(?i:client_version)") . extract(values) . any() in
["3.6.0", "3.7.0", "3.7.1" , "3.7.2", "3.8.0"]
```

Б.3. Операторы

Операторы проверяют текущий контекст предиката на соответствие аргументу. В языке пользовательских правил доступны следующие операторы.

Реляционные операторы

Таблица 28. Реляционные операторы

Оператор	Значение	Тип данных	Пример фильтра
`>` `gt`	Больше	Целое число	`RESPONSE_STATUS_CODE > 400`
`<` `lt`	Меньше	Целое число	`RESPONSE_SIZE lt 500`
`>=` `ge`	Больше или равно (не меньше)	Целое число	`REQUEST_SIZE ge 1000`
`<=` `le`	Меньше или равно (не больше)	Целое число	`RESPONSE_STATUS_CODE <= 500`
`==` `eq`	Равно	Целое число, строка	`REQUEST_PATH eq "/shop/catalog"` `RESPONSE_STATUS_CODE == 404`
`!=` `ne`	Не равно (не совпадает)	Целое число, строка	`REQUEST_PATH ne "/shop/catalog"` `RESPONSE_STATUS_CODE != 200`

between

Проверяет, содержится ли целочисленное значение из текущего контекста в диапазоне значений, определяемом аргументами оператора.

Аргументы оператора — два целочисленных значения. Сначала указывается нижняя граница, затем верхняя.

```
# Пример предиката
REQUEST_GET . length() between 1 and 10
```

contains

Проверяет список, указанный в аргументе, на вхождение в список из текущего контекста.

Аргумент оператора — список. Типы данных текущего контекста и аргумента должны совпадать.

```
# Пример предиката
REQUEST_HEADERS . extract(keys) contains ["Host", "Content-Length", "Content-Type"]
```

exists

Проверяет наличие значений в текущем контексте. Применим только к векторному контексту. Не имеет аргументов.

```
# Примеры предикатов
REQUEST_METHOD = "POST" and REQUEST_POST . select("address.mobile") . exists()
REQUEST_HEADERS . map(lowercase) . select(~"bounty") . exists()
```

in

Проверяет скалярное значение на вхождение в плоский список. Аргументы оператора — список или параметр правила, указывающий на глобальный список.

```
# Примеры предикатов
REQUEST_PATH in ["/shop", "/catalog","/shop/catalog"]
REQUEST_GET . extract(values) . map(length) in [5, 10, 15]
CLIENT_IP in @@allowed_ip_list
```

is_empty

Проверяет наличие значения в текущем контексте:

— если значение пустое (`""`) или не существует (`null`) — возвращает `True`;

— если значение не пустое — возвращает `False`.

Применим только к скалярному контексту, допустимый тип контекста — строка. Не имеет аргументов.

```
# Примеры предикатов
# Правило сработает на запрос с пустым телом (null или "")
if REQUEST_BODY . is_empty()
# Правило сработает на запрос с не пустым телом
if NOT REQUEST_BODY . is_empty()
```

```
# Правило сработает на запрос, в котором отсутствует GET-параметр с ключом "page" или GET-параметр с ключом "page" не имеет значения
if REQUEST_GET . select("page") . extract(values) . first() . is_empty()
# Правило сработает на запрос, в котором отсутствует заголовок "Header" или заголовок "Header" не имеет значения
if REQUEST_HEADERS . select("Header") . extract(values) . first() . is_empty()
```

is_set

Проверяет наличие значения в текущем контексте:

— если значение не пустое или пустое ("") — возвращает `True`;

— если значение не существует (`null`) — возвращает `False`.

Применим только к скалярному контексту. Не имеет аргументов.

```
# Примеры предикатов
# Правило сработает на запрос, в котором присутствует GET-параметр с ключом "page" и значение этого параметра можно преобразовать из hex-кода
if REQUEST_GET . select("page") . extract(values) . first() . map(hex_decode) . is_set()
# Правило сработает на запрос, в котором отсутствует GET-параметр с ключом "page"
IF NOT REQUEST_GET . select("page") . extract(values) . all() . is_set()
```

matches

Проверяет соответствие текущего контекста регулярному выражению или наличие в текущем контексте строки, указанной в аргументе.

```
# Примеры предикатов
REQUEST_PATH matches "/shop/catalog"
REQUEST_HEADERS . extract(keys) . any() matches ~"\\d"
```

Б.4. Типы данных

В языке для написания пользовательских правил используются следующие типы данных.

Строка

Заключается в двойные кавычки ("). Если строка содержит двойные кавычки или обратную косую черту, их необходимо экранировать обратной косой чертой.

Примеры строк:

```
"POST"
"/v1/authenticate"
```

Целое число без знака

Последовательность цифр, допустимы незначащие начальные нули.

Примеры целых чисел:

```
0056
401
```

IP-адрес

Поддерживаются адреса IPv4, IPv6 и диапазоны адресов в формате CIDR. Не поддерживается смешанный формат IPv6.

Примеры IP-адресов:

```
192.0.2.7
198.51.100.0/24
2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d
```

Список

Множество однотипных значений (строки, целые числа или IP-адреса), перечисленных через запятую. Список заключается в квадратные скобки.

Примеры списков:

```
["/v1/authenticate", "/v2/authenticate", "/v3/auth"]
[400, 500, 503]
[192.0.2.7, 198.51.100.0/24, 2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d]
```

Регулярное выражение

Выражение заключается в двойные кавычки (`"`), перед первыми кавычками добавляется тильда. Синтаксис выражения — PCRE (библиотека Hyperscan).

Следующие метасимволы в регулярном выражении не требуют экранирования: `\a`, `\b`, `\f`, `\n`, `\r`, `\t`, `\v`, `\\`, `\"` и `\'`. В остальных случаях обратную косую черту и двойные кавычки необходимо экранировать обратной косой чертой.

Примеры регулярных выражений:

```
~"^/bitrix/admin/.*$"
~"\\.(?:bat|exe|scr|vbs|htm|php|asp)"
```

Б.5. Прочие элементы языка

Комментарии

Делятся на однострочные и многострочные. Однострочный комментарий начинается с символа `#`, многострочный заключаются между символами `/*` и `*/`. Комментариями можно заменять пробелы и переносы строк, чтобы отделять другие виды литералов друг от друга.

```
# Примеры комментариев
# Секция определения локальных переменных начинается с ключевого слова with
```

```
with @path/*Это локальная переменная*/= "/test.php"
# Секция с логикой обработки HTTP-запроса (ответа) начинается с ключевого слова if
if CLIENT_IP in @@parameter_list/*Это параметр правила*/and REQUEST_PATH/*Это
контекстная переменная*/== @path
```

Разделители

Предусмотрены следующие разделители:

— **Пробелы, знаки табуляции и переносы строки.** Можно использовать для разделения любых элементов языка между собой, если такое разделение не меняет синтаксис элемента. Например, недопустимо указывать `wi th` вместо ключевого слова `with`.

— **Запятая «,».** Разделяет выражения для определения локальных переменных, а также элементы в списке.

— **Точка «.».** Разделяет функции (преобразования) в предикате.

Скобки

Круглые скобки «( )» изменяют приоритет при выполнении логических операций с предикатами.

Квадратные скобки «[ ]» используются для определения списка.

Приложение В. Конструктор исключений для запуска правила

Конструктор исключений позволяет построить логическое выражение для проверки условий отмены запуска правила (см. раздел 10.7). Логическое выражение строится из групп условий. Группы объединяются логическим оператором `OR`. Проверка не будет запущена, если выполняются условия хотя бы одной группы.

Каждая группа состоит минимум из одного условия. Условия внутри группы объединяются логическим оператором `AND`. Если все условия группы выполняются (логическое выражение истинно), то проверка не запускается и действия, указанные в правиле, не срабатывают.

> **Примечание.** Для определения страны, региона и города в PT AF, начиная с версии 4.1.8, используется база GeoIP от российского Главного радиочастотного центра.

Результат логического выражения определяется логикой работы операторов (условий), конструкции из которых позволяют проверить значения параметров в HTTP-запросе клиента.

Регулярные выражения поддерживают синтаксис шаблонов Lua и библиотеки HyperScan.

Таблица 29. Параметры HTTP-запроса для настройки исключения

Параметр	Имя	Условие	Описание
`IP-адрес`	—	Возможные условия: — равно; — не равно; — входит в список	IPv4-адрес клиента
`Страна`	—	Возможные условия: — равно; — не равно	Название страны
`Регион`	—	Возможные условия: — равно; — не равно; — соответствует регулярному выражению	Название региона

Параметр	Имя	Условие	Описание
Город	—	Возможные условия: — равно; — не равно; — соответствует регулярному выражению	Название города
Заголовок	+	Возможные условия: — существует; — равно; — не равно; — соответствует регулярному выражению; — пустое значение	Заголовок HTTP-запроса
GET-параметр	+	Возможные условия: — существует; — равно; — не равно; — соответствует регулярному выражению; — пустое значение	Параметры строки GET-запроса
POST-параметр	+	Возможные условия: — существует; — равно; — не равно; — соответствует регулярному выражению; — пустое значение	Параметры тела POST-запроса

Параметр	Имя	Условие	Описание
Куки	+	Возможные условия: — существует; — равно; — не равно; — соответствует регулярному выражению; — пустое значение	Параметр заголовка Cookie в HTTP-запросе. Содержит пары «ключ — значение», разделенные точкой с запятой
Путь	—	Возможные условия: — равно; — не равно; — соответствует регулярному выражению	Путь к ресурсу (path HTTP-запроса)
URI	—	Возможные условия: — равно; — не равно; — соответствует регулярному выражению	Относительный URI. Значение должно включать path, query и fragment
Метод	—	Возможные условия: — равно; — не равно	Название метода, исключаемого из проверки правилом. Возможные значения: GET, POST, HEAD, PUT, OPTIONS, DELETE, PATCH
Данные по WebSocket от клиента	-	Возможные условия: — равно; — не равно; — соответствует регулярному выражению (Lua); — соответствует регулярному выражению (Hyperscan)	Данные, передаваемые по протоколу WebSocket от клиента к веб-приложению

Приложение Г. Справочник по языку фильтрации событий безопасности

Условие фильтрации содержит параметр события (см. приложение Г), оператор (см. приложение Г) и значение для сравнения. С помощью логических операторов `and`, `or` и `not` и круглых скобок `( )` вы можете объединять несколько простых условий в более сложное условие.

Параметры события безопасности

С помощью параметров событий безопасности вы можете прописать условия фильтрации событий. Ниже описаны параметры события безопасности и приведены примеры фильтров.

Таблица 30. Параметры события безопасности

Параметр	Значение	Тип данных	Пример
`app_id`	Идентификатор веб-приложения	Идентификатор в формате RFC 4122 (UUID)	`app_id == 529a8a33-3dd0-4df7-abfb-7d739bbabc23`
`app_name`	Название веб-приложения	Строка	`app_name == "Example profile"`
`client_browser_name`	Название браузера клиента	Строка	`client_browser_name == "Firefox"`
`client_browser_version`	Версия браузера клиента	Строка	`client_browser_version == "66.0"`
`client_country`	Двухбуквенный код страны клиента согласно ISO 3166-1	Предопределенный список значений	`client_country == RU`
`client_ip`	IP-адрес клиента	IP-адрес [29]	`client_ip == 192.0.2.56` `client_ip in 192.0.2.0/24`

29 В зависимости от оператора IP-адрес нужно указывать с префиксом маски (в формате CIDR) или без префикса.

Параметр	Значение	Тип данных	Пример
client_os_name	Семейство операционной системы рабочей станции клиента	Строка	client_os_name == "Linux"
client_username	Логин пользователя	Строка	client_username == "admin"
event_severity	Уровень опасности события: — high — высокий; — medium — средний; — low — низкий; — none — нет	Предопределенный список значений	event_severity == medium
matched_names	Имя совпавшей переменной	Строка	matched_names == "REQUEST_HEADERS"
matched_values	Значение совпавшей переменной. Доступны операторы ~=, regex и ==. При использовании ~= или regex требуется добавление дополнительного параметра, например matched_names либо request_uri	Строка	matched_values == "text/css" matched_names == "REQUEST_GET" and matched_values ~= "(vd|abc)" matched_values regex "script" and request_uri == "/fonts/font.woff"
request_cookies	Ключ и значение куки запроса. Доступны операторы contains и ==	Строка	request_cookies["PHPSESSID"] == "12345678901234567890" request_cookies.key == "PHPSESSID"

Параметр	Значение	Тип данных	Пример
			`request_cookies.value contains "12345678901234567890"`

`request_get`	Ключ и значение параметра GET-запроса. Доступны операторы `contains` и `==`	Строка	`request_get["_id"] == "12345678901234567890"`
			`request_get.key contains "_id"`
			`request_get.value contains "mysql.user"`

`request_headers`	Имя и значение заголовка запроса. Доступны операторы `contains` и `==`	Строка	`request_headers["User-Agent"] contains "citrix"`
			`request_headers.key == "Authorization"`
			`request_headers.value == "test.com"`

`request_post`	Ключ и значение параметра POST-запроса. Доступны операторы `contains` и `==`	Строка	`request_post["type"] == "authorization"`
			`request_post.key contains "par"`
			`request_post.value contains "java.rmi.server"`

`request_method`	Метод запроса	Строка	`request_method == "GET"`
`request_path`	Путь к ресурсу	Строка	`request_path == "/shop/catalog"`
`request_size`	Размер запроса в байтах	Целое число	`request_size < 811`

Параметр	Значение	Тип данных	Пример
`request_uri`	URI запроса	Строка	`request_uri == "/shop/catalog?page=2&items=15"`

`response_headers`	Имя и значение заголовка ответа.Доступны операторы `contains` и `==`	Строка	`response_headers["Etag"] == "1234a567-4f"`
			`response_headers.key == "X-Powered-By"`
			`response_headers.value contains "1234a567-4f"`

`response_size`	Размер ответа в байтах	Целое число	`response_size <> 384`
`response_status_code`	Код ответа (от 100 до 599 включительно)	Целое число	`response_status_code > 200`
`rule_id`	Псевдоним системного правила	Строка	`rule_id == jwt_alg_none_attack`
	Идентификатор пользовательского правила	Идентификатор в формате RFC 4122 (UUID)	`rule_id == ce8352bf-2205-4baa-a9b6-bdcd6a999e4a`
`rule_phase`	Фаза срабатывания правила: — `on_request` — на запросе; — `on_response` — на ответе; — `on_transaction_complete` — при окончании транзакции; — `on_transaction_start` — при начале транзакции;	Предопределенный список значений	`rule_phase == on_request`

Параметр	Значение	Тип данных	Пример
	— `on_websocket_downstream` — при получении данных от сервера по WebSocket; — `on_websocket_upstream` — при передаче данных серверу по WebSocket		
`transaction_id`	Идентификатор транзакции	Идентификатор в формате RFC 4122 (UUID)	`transaction_id == e0d3e136-c0b6-484c-9bfa-3e15642767e1`

Операторы в фильтрах

С помощью операторов вы можете задать значения для параметров событий безопасности и объединить несколько параметров в условии фильтрации. Ниже описаны операторы для фильтрации и приведены примеры фильтров.

Таблица 31. Операторы в фильтрах

Оператор	Значение	Тип данных	Пример фильтра
Операторы сравнения			
`>`	Больше	Целое число	`response_status_code > 400`
`<`	Меньше	Целое число	`response_size < 500`
`>=`	Больше или равно (не меньше)	Целое число	`request_size >= 1000`
`<=`	Меньше или равно (не больше)	Целое число	`response_status_code <= 500`
`=`	Равно (без учета регистра)	Строка	`client_username = "admin"`

Оператор	Значение	Тип данных	Пример фильтра
`==`	Равно (точное совпадение)	Целое число, строка, UUID, IP-адрес без префикса маски или предопределенный список значений	`request_path == "/shop/catalog"`
`<>` `!=`	Не равно (не совпадает)	Целое число, строка, UUID	`response_status_code <> 200` `client_username != "admin"`
`~=` `regex`	Соответствует регулярному выражению	Строка	`client_browser_version ~= "6\d\.\d"` `client_browser_version regex "6\d\.\d"`
Логические операторы			
`and`	Логическое И	—	`client_username == "operator" and client_ip in [192.0.2.0/24, 198.51.100.0/24]`
`or`	Логическое ИЛИ	—	`client_browser_name == "Firefox" or client_browser_name == "Chrome"`
`not`	Логическое НЕ (отрицание)	—	`not client_os_name == "Windows"`
Прочие операторы			
`between n and m`	Входит в указанный промежуток (от `n` до `m`), где `n` и `m` — целые числа	Целое число	`response_status_code between 300 and 399`
`contains`	Содержит строку	Строка, бинарные данные	`request_path contains "/shop"`
`exists`	Параметр имеет непустое значение	—	`client_username exists`

Оператор	Значение	Тип данных	Пример фильтра
`in [x,y,z]`	Равно (точное совпадение) одному из перечисленных в скобках значений	Предопределенный список значений	`event_severity in [low, medium]`

`in <Подсеть>`
`in [<Подсеть 1>, <Подсеть 2...>]`
`in [<IP-адрес 1>, <IP-адрес 2>...]`
	IP-адрес клиента входит в подсеть или в список IP-адресов	IP-адрес подсети в формате CIDR, список IP-адресов подсетей в формате CIDR или список IP-адресов без префикса маски	`client_ip in 192.0.2.0/24`
			`client_ip in [198.51.100.0/24, 203.0.113.0/24]`
			`client_ip in [198.51.100.89, 203.0.113.120]`

См. также

Страница События безопасности (см. раздел 7.2)

Приложение Д. Индикаторы состояния PT AF в Grafana

Ниже описаны причины срабатывания индикаторов, а также приведены действия по диагностике и решению проблем.

В этом разделе

Индикатор ClickHouse (см. приложение Д.1)

Индикатор Consul (см. приложение Д.2)

Индикатор CPU (см. приложение Д.3)

Индикатор DISK (см. приложение Д.4)

Индикатор ETCD (см. приложение Д.5)

Индикатор K8S (см. приложение Д.6)

Индикатор Minio (см. приложение Д.7)

Индикатор Network (см. приложение Д.8)

Индикатор Nodes (см. приложение Д.9)

Индикатор PG SQL (см. приложение Д.10)

Индикатор PTAF Backend (см. приложение Д.11)

Индикатор RabbitMQ (см. приложение Д.12)

Индикатор RAM (см. приложение Д.13)

Индикатор RPS / app errors (см. приложение Д.14)

Д.1. Индикатор ClickHouse

Таблица 32. Индикатор ClickHouse

Причина	Диагностика
Желтые индикатор и рамка	
Задержка репликации данных составляет от одной до пяти минут	Определите проблемный узел: 1. Нажмите на индикатор **ClickHouse** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbClickHouseAsyncMetrics** с указанием имени узла
Красные индикатор и рамка	
Задержка репликации данных составляет более пяти минут	Определите проблемный узел: 1. Нажмите на индикатор **ClickHouse** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbClickHouseAsyncMetrics** с указанием имени узла
Одна из реплик находится в состоянии «только чтение»	Определите проблемный узел: 1. Нажмите на индикатор **ClickHouse** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbClickHouseReadonlyReplica** с указанием имени узла

Д.2. Индикатор Consul

Таблица 33. Индикатор Consul

Причина	Диагностика
Желтая рамка	
Один из сервисов, отслеживаемых в кластере Consul, находится в статусе `critical`	Определите проблемные сервис и узел: 1. Нажмите на индикатор **Consul** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **ConsulServiceStatusCritical** с указанием имени сервиса и узла
Красный индикатор	
Кластер Consul неработоспособен	Определите проблемный узел: 1. Нажмите на индикатор **Consul** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **ConsulUp** с указанием имени узла
Кластер Consul не имеет «лидера»	Определите проблемный узел: 1. Нажмите на индикатор **Consul** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **ConsulRaftLeader** с указанием имени узла

Причина	Диагностика
Один из узлов кластера Consul находится в статусе `critical`	Определите проблемный узел: 1. Нажмите на индикатор **Consul** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **ConsulNodeStatusCritical** с указанием имени узла

Д.3. Индикатор CPU

Таблица 34. Индикатор CPU

Причина	Диагностика
Желтый индикатор	
Для одного из узлов утилизация ядер ЦП находится в диапазоне 75—86%	Определите узел с повышенной утилизацией ядер: 1. На виджете **CPU utilization / LA** выберите точку с максимальным значением на непрерывном графике. Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **UTIL**. 2. Нажмите на индикатор **CPU** и по ссылке откройте дашборд **Nodes**. 3. Выберите узел, найденный на первом шаге, и проанализируйте графики на виджете **CPU**
Для одного из узлов средняя загрузка ЦП находится в диапазоне 64—73%	Определите узел с повышенной загрузкой ЦП: 1. На виджете **CPU utilization / LA** выберите точку с максимальным значением на прерывистом графике.

Причина	Диагностика
	Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **LA**. 2. Нажмите на индикатор **CPU** и по ссылке откройте дашборд **Nodes**. 3. Выберите узел, найденный на первом шаге, и проанализируйте графики на виджете **Load**
Для одного из узлов «украденное» время ЦП[31] находится в диапазоне 0,86—0,95%	Определите узел с «украденным» временем ЦП: на виджете **CPU IO wait / Stolen by other VMs / k8s provisioning** выберите любую точку на графике — откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **STOLEN CPU**
Красный индикатор	
Для одного из узлов утилизация ядер ЦП превышает 86%	Определите узел с высокой утилизацией ядер: 1. На виджете **CPU utilization / LA** выберите точку с максимальным значением на непрерывном графике. Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **UTIL**. 2. Нажмите на индикатор **CPU** и по ссылке откройте дашборд **Nodes**. 3. Выберите узел, найденный на первом шаге, и проанализируйте графики на виджете **CPU**
Для одного из узлов средняя загрузка ЦП превышает 73%	Определите узел с высокой загрузкой ЦП: 1. На виджете **CPU utilization / LA** выберите точку с максимальным значением на прерывистом графике.

31 В следствии избыточного выделения ресурсов.

Причина	Диагностика
	Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **LA**. 2. Нажмите на индикатор **CPU** и по ссылке откройте дашборд **Nodes**. 3. Выберите узел, найденный на первом шаге, и проанализируйте графики на виджете **Load**
Для одного из узлов «украденное» время ЦП[31] превышает 0,95%	Определите узел с «украденным» временем ЦП: на виджете **CPU IO wait / Stolen by other VMs / k8s provisioning** выберите любую точку на графике — откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **STOLEN CPU**
Желтая рамка	
Для одного из узлов загрузка ЦП для обработки запросов подов Kubernetes находится в диапазоне 80—90%	Определите узел с повышенной загрузкой ЦП: 1. На виджете **CPU IO wait / Stolen by other VMs / k8s provisioning** выберите точку с максимальным значением на прерывистом графике. Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **k8s provisioning**. 2. Нажмите на индикатор **CPU** и по ссылке откройте дашборд **Cluster overview**. 3. Выберите узел, найденный на первом шаге, и проанализируйте графики на виджете **k8s CPU requests**, чтобы определить количество и тип подов, которые может дополнительно поддержать узел
Красная рамка	
Для одного из узлов загрузка ЦП для обработки запросов подов Kubernetes превышает 90%	Определите узел с высокой загрузкой ЦП: 1. На виджете **CPU IO wait / Stolen by other VMs / k8s provisioning** выберите точку с максимальным значением на прерывистом графике.

Причина	Диагностика
	Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **k8s provisioning**. 2. Нажмите на индикатор **CPU** и по ссылке откройте дашборд **Cluster overview**. 3. Выберите узел, найденный на первом шаге, и проанализируйте графики на виджете **k8s CPU requests**, чтобы определить количество и тип подов, которые может дополнительно поддержать узел

Д.4. Индикатор DISK

Таблица 35. Индикатор DISK

Причина	Диагностика
Желтый индикатор	
На одном из узлов раздел [32] заполнен на 80—90%	Определите заполненный раздел: 1. На виджете **Disks fill** выберите точку на графике. Откроется всплывающая подсказка, в которой отобразятся имена узлов и разделов, а также процент их заполнения в выбранной точке. Записи о наиболее заполненных разделах размещены выше остальных. 2. Нажмите на индикатор **DISK** и по ссылке откройте дашборд **Nodes**. 3. Проанализируйте графики на виджете **Disk Space Used**

32 Учитываются физические и логические разделы, смонтированные к любому каталогу, за исключением разделов, смонтированных к `/boot` и `/boot/efi`.

Причина	Диагностика
	Красный индикатор
На одном из узлов раздел[32] заполнен на 90% или более	Определите заполненный раздел: 1. На виджете **Disks fill** выберите точку на графике. Откроется всплывающая подсказка, в которой отобразятся имена узлов и разделов, а также процент их заполнения в выбранной точке. Записи о наиболее заполненных разделах размещены выше остальных. 2. Нажмите на индикатор **DISK** и по ссылке откройте дашборд **Nodes**. 3. Проанализируйте графики на виджете **Disk Space Used**
На одном из узлов раздел[32] смонтирован в режиме «только для чтения»	Запись о таком узле и разделе отображается с подписью **READONLY !!!** как на самом виджете **Disks fill**, так и на всплывающей подсказке к виджету
	Желтая рамка
На одном из узлов раздел[32] будет полностью заполнен[33] через 24—72 часа	Определите заполняемый раздел: В раскрывающемся списке **Depth of disks filling prediction (hours)** выберите 72 часа. На виджете **Disks fill** записи о таком узле и разделе отображаются с подписью **WILL FULL IN 72 HOURS** как на самом виджете, так и на всплывающей подсказке к нему

33 Текущая скорость заполнения диска вычисляется как производная (простая линейная регрессия) на отрезке последних пяти минут.

Причина	Диагностика
	Красная рамка
На одном из узлов раздел [32] будет полностью заполнен [33] через 24 часа или менее	Определите заполняемый раздел: В раскрывающемся списке **Depth of disks filling prediction (hours)** выберите 24 часа. На виджете **Disks fill** записи о таком узле и разделе отображаются с подписью **WILL FULL IN 24 HOURS** как на самом виджете, так и на всплывающей подсказке к нему

Д.5. Индикатор ETCD

Таблица 36. Индикатор ETCD

Причина	Диагностика
	Красные индикатор и рамка
Один из узлов хранилища etcd не находит «лидера»	Определите проблемный узел: 1. Нажмите на индикатор **ETCD** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sEtcdLeader** с указанием имени узла
В течение последних пяти минут 99 перцентиль длительности запросов к etcd превышает 10 секунд	Определите проблемный узел: 1. Нажмите на индикатор **ETCD** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sEtcdRequestDelay** с указанием имени узла

Причина	Диагностика
За последнюю минуту произошло больше трех смен «лидера» хранилища etcd	Определите проблемный узел: 1. Нажмите на индикатор **ETCD** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sEtcdLeaderChange** с указанием имени узла

Д.6. Индикатор K8S

Таблица 37. Индикатор K8S

Причина	Диагностика
Желтые индикатор и рамка	
Один из подов узла находится в статусе `Pending`	Определите под в статусе `Pending`: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sPodStatusPending** с указанием имени пода
Доля ресурсов ЦП, используемых для обработки запросов подов Kubernetes, усредненная по всем узлам, находится в диапазоне 80—90%	Определите узлы с повышенной загрузкой ЦП: 1. На виджете **CPU IO wait / Stolen by other VMs / k8s provisioning** выберите точки с максимальными значениями на прерывистом графике.

Причина	Диагностика
	Откроется всплывающая подсказка, в которой отобразятся имена узлов как значения параметра **k8s provisioning**. 2. Нажмите на индикатор **CPU** и по ссылке откройте дашборд **Cluster overview**. 3. Выберите узлы, найденные на первом шаге, и проанализируйте графики на виджете **k8s CPU requests**, чтобы определить количество и тип подов, которые дополнительно могут поддержать узлы
Доля ресурсов ОЗУ, используемых для обработки запросов подов Kubernetes, усредненная по всем узлам, находится в диапазоне 80—90%	Определите узлы с повышенной загрузкой ОЗУ: 1. На виджете **RAM utilization / k8s provisioning** выберите точки с максимальными значениями на прерывистом графике. Откроется всплывающая подсказка, в которой отобразятся имена узлов как значения параметра **k8s provisioning**. 2. Нажмите на индикатор **RAM** и по ссылке откройте дашборд **Cluster overview**. 3. Выберите узлы, найденные на первом шаге, и проанализируйте графики в виджете **k8s Memory requests**, чтобы определить количество и тип подов, которые могут поддержать узлы дополнительно к текущим
Для одного из веб-приложений соотношение планируемого количества реплик к максимальному количеству, достигнутому при автомасштабировании, превышает 90%	Определите проблемный объект с типом Deployment: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sHpaReplicas** с указанием имени объекта

Причина	Диагностика
Для одного из веб-приложений соотношение фактического количества реплик к максимальному количеству, достигнутому при автомасштабировании, превышает 90%	Определите проблемный объект с типом Deployment: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sHpaDesiredReplicas** с указанием имени объекта
Красные индикатор и рамка	
Один из контейнеров в Kubernetes перегружался чаще одного раза за последние 10 минут	Определите проблемный контейнер: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sContainerStatusRestart** с указанием имени контейнера
Один из контейнеров в Kubernetes находится в статусе `CrashLoopBackOff`	Определите проблемный контейнер: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sContainerStatusCrashLoopBackOff** с указанием имени контейнера
Один из объектов с типом DaemonSet содержит хотя бы один недоступный под	Определите проблемный объект с типом DaemonSet: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sDaemonsetUnavailable** с указанием имени объекта

Причина	Диагностика
Один из объектов с типом Deployment содержит хотя бы один недоступный под	Определите проблемный объект с типом Deployment: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sReplicasUnavailable** с указанием имени объекта
Один из объектов с типом StatefulSet содержит хотя бы один недоступный под	Определите проблемный объект с типом StatefulSet: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sStatefulset** с указанием имени объекта
Один из узлов находится в состоянии MemoryPressure	Определите проблемный узел: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sNodeMemory** с указанием имени узла
Один из узлов находится в состоянии DiskPressure	Определите проблемный узел: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sNodeDisk** с указанием имени узла
Один из узлов находится в состоянии NetworkUnavailable	Определите проблемный узел: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sNetworkUnavailable** с указанием имени узла

Причина	Диагностика
Запросы к API-серверу Kubernetes, отправленные в течение последних пяти минут, завершались с ошибками 5xx более 10 раз	Определите проблемный узел: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sApiserverCode5xx** с указанием имени узла
Один из запросов к API-серверу Kubernetes, отправленный в течение последних пяти минут, длился более одной минуты	Определите тип проблемного запроса: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sApiserverRequest** с указанием названия типа запроса
На одном из узлов размещено максимальное разрешенное количество подов для узла	Определите проблемный узел: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sRunningPods** с указанием имени узла
Один из системных подов Kubernetes (kube-apiserver, kube-controller-manager или kube-scheduler) не имеет статуса **Ready**	Определите проблемный под: 1. На виджете **K8S Components Health** найдите системный под, показатель здоровья которого менее 100%. 2. Уточните его имя и время, с которого началось снижение показателя. 3. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Pods**.

Причина	Диагностика
	4. В верхней части дашборда в раскрывающемся списке **pod** поочередно выберите системные поды с именем, определенным в первом шаге инструкции, но расположенные на разных узлах. 5. Определите под со сниженным показателем здоровья: на виджете **Pod status** на диаграмме **Running** такой под будет иметь одно или несколько нулевых значений
Для одного из узлов загрузка ЦП для обработки запросов подов Kubernetes превышает 90%	Определите узел с высокой загрузкой ЦП. Вариант 1: 1. На виджете **CPU IO wait / Stolen by other VMs / k8s provisioning** выберите точку с максимальным значением на прерывистом графике. Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **k8s provisioning**. 2. Нажмите на индикатор **CPU** и по ссылке откройте дашборд **Cluster overview**. 3. Выберите узел, найденный на первом шаге, и проанализируйте графики в виджете **k8s CPU requests**, чтобы определить количество и тип подов, которые дополнительно может поддержать узел. Вариант 2: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sSumCpuUsage** с указанием имени узла
Для одного из узлов загрузка ОЗУ для обработки запросов подов Kubernetes превышает 90%	Определите узел с высокой загрузкой ОЗУ.

Причина	Диагностика
	Вариант 1: 1. На виджете **RAM utilization / k8s provisioning** выберите точку с максимальным значением на прерывистом графике. Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **k8s provisioning**. 2. Нажмите на индикатор **RAM** и по ссылке откройте дашборд **Cluster overview**. 3. Выберите узел, найденный на первом шаге, и проанализируйте графики в виджете **k8s Memory requests**, чтобы определить количество и тип подов, которые дополнительно может поддержать узел. Вариант 2: 1. Нажмите на индикатор **K8S** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **K8sSumMemoryUsage** с указанием имени узла

Д.7. Индикатор Minio

Таблица 38. Индикатор Minio

Причина	Диагностика
Красные индикатор и рамка	
Один из узлов в кластере Minio недоступен	Определите недоступный узел: 1. Нажмите на индикатор **Minio** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbMinioNodesOffline** с указанием имени узла
Один из «дисков» в кластере Minio недоступен	Определите узел с недоступным «диском»: 1. Нажмите на индикатор **Minio** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbMinioDisksOffline** с указанием имени узла

Д.8. Индикатор Network

Таблица 39. Индикатор Network

Причина	Диагностика и решение проблем
	Желтые индикатор и рамка
Утилизация физического (псевдофизического) сетевого адаптера находится в диапазоне 86—95%	Определите сетевые адаптеры с высокой утилизацией. Вариант 1: На виджете **Max Network utilization** выберите точку на графике с максимальным значением. Откроется всплывающая подсказка, в которой отобразится имя узла и название адаптера. Вариант 2: 1. Нажмите на индикатор **Network** и по ссылке откройте дашборд **Network**. 2. На виджете **Network Traffic** определите максимально нагруженные адаптеры, последовательно выбирая узлы и их сетевые адаптеры в верхней части дашборда. Для решения проблемы рекомендуется: — Заменить сетевые адаптеры на более скоростные, (например, со скоростью 10 Гбит/с), что возможно потребует увеличения вычислительной мощности узлов. — Увеличить количество узлов, обрабатывающих трафик
Доля ошибок для физического (псевдофизического) сетевого адаптера или сетевой подсистемы ядра ОС находится в диапазоне 0,86—0,95%	Доля ошибок отображается на виджете **Max Network Errors**. Для всех ненулевых значений под диаграммами отображается описание ошибки с указанием максимального значения за наблюдаемый период.

Причина	Диагностика и решение проблем
	Ошибки делятся на следующие типы: — **RC ERRORS** — ошибки приема; — **TR ERRORS** — ошибки передачи; — **RC DROPS** — ошибки сброса при приеме; — **TR DROPS** — ошибки сброса при передаче; — **CPU BACKLOG DROPS** — ошибки сброса вследствие переполнения очереди `netdev_max_backlog` ядра ОС; — **CPU LIMIT DROPS** — ошибки сброса вследствие превышения лимита времени, выделяемого ЦП на обработку очереди в ядре ОС. Кроме того, основную сетевую статистику можно посмотреть на дашборде **Infrastructure** → **Network**. Более подробные сетевые метрики по умолчанию не собираются, поскольку это может привести к дополнительной нагрузке на узел. Вы можете включить детальный сбор метрик на несколько минут для выполнения временной диагностики: 1. На узле создайте файл `/opt/ptaf/conf/collect_node_network_socket_stats` для сбора метрик. 2. После диагностики удалите файл, чтобы остановить сбор метрик.

Причина	Диагностика и решение проблем

	Общие ошибки RC ERRORS и TR ERRORS. Для диагностики ошибок и получения статистики драйвера сетевого адаптера выполните команду:
	`ethtool -S eth-ext1`
	Названия счетчиков зависят от драйвера, что может потребовать уточнения в документации производителя для разделения общих ошибок на конкретные типы.
	Чаще всего ошибки вызваны проблемами адаптера, кабеля или оборудования внешней сети.
	Ошибки сброса RC DROPS и TR DROPS. Ошибки сброса обычно вызваны переполнением буферов или превышением лимитов:
	— Проверьте текущие и максимальные значения для буферов и увеличьте их при возможности:
	`ethtool -g eth-ext1`
	`ethtool -g eth-ext1 rx 4096`
	`ethtool -g eth-ext1 tx 4096`
	Пример вывода команды `ethtool -g eth-ext1`:
	`Ring parameters for eth-ext1:`
	`Pre-set maximums:`
	`RX: 4096`
	`RX Mini: n/a`
	`RX Jumbo: n/a`
	`TX: 4096`
	`Current hardware settings:`
	`RX: 256`
	`RX Mini: n/a`
	`RX Jumbo: n/a`

Причина	Диагностика и решение проблем

	TX: 256
	— Для предотвращения переполнения включите приостановку отсылки кадров (требуется поддержка коммутатором):
	`ethtool -a eth-ext1`
	`ethtool -a eth-ext1 autoneg on`
	`ethtool -a eth-ext1 rx on`
	`ethtool -a eth-ext1 tx on`
	Пример вывода команды `ethtool -a eth-ext1`:
	`Pause parameters for eth-ext1:`
	`Autonegotiate: on`
	`RX: off`
	`TX: off`
	— Проверьте распределение прерываний:
	`egrep "CPU0|eth-ext1" /proc/interrupts`
	Пример вывода:
	`CPU0 CPU1 CPU2 CPU3 CPU4 CPU5 CPU6 CPU7`
	`31: 0 0 0 0 0 1 0 0 IR-PCI-MSI 1048576-edge eth-ext1`
	`32: 0 8818955 0 0 0 0 27 0 IR-PCI-MSI 1048577-edge eth-ext1-TxRx-0`
	`33: 0 0 7363245 0 0 0 0 32 IR-PCI-MSI 1048578-edge eth-ext1-TxRx-1`
	`34: 5573688 0 0 0 0 0 0 0 IR-PCI-MSI 1048579-edge eth-ext1-TxRx-2`
	`35: 0 5852035 0 0 0 0 0 0 IR-PCI-MSI 1048580-edge eth-ext1-TxRx-3`

Причина	Диагностика и решение проблем

	36: 0 0 5738363 0 0 0 0
	0 IR-PCI-MSI 1048581-edge eth-ext1-TxRx-4
	37: 0 0 0 5573741 0 0 0
	0 IR-PCI-MSI 1048582-edge eth-ext1-TxRx-5
	38: 0 0 5576699 0 30 0 0
	0 IR-PCI-MSI 1048583-edge eth-ext1-TxRx-6
	39: 0 0 0 5823076 0 26 0
	0 IR-PCI-MSI 1048584-edge eth-ext1-TxRx-7
	
	На скоростях от 100 Мбит/с системные прерывания, привязанные к очередям сетевого адаптера, должны распределяться между разными ядрами ЦП. Убедитесь, что разные прерывания (строки вывода команды) равномерно распределены между ядрами ЦП (имеют ненулевые счетчики в разных столбцах `CPUx`).
	
	Убедитесь в наличии достаточного количества очередей ввода-вывода: серверные сетевые адаптеры со скоростью 10 Гбит/с, необходимые для нормального функционирования кластера под нагрузкой, имеют от 100 или более очередей на каждом сетевом адаптере (количество строк вывода команды).
	
	Ошибки сброса CPU BACKLOG DROPS. Проверьте наличие ошибок:
	
	`cat /proc/net/softnet_stat`
	
	Пример вывода:
	
	`2011e8ef 003b8226 00003511 00000000 ... 00000000`
	
	`060d102b 000021af 0000364d 00000000 ... 00000000`
	
	`06f72be1 000019ad 00003808 00000000 ... 00000000`
	
	`0602bbd3 00001437 0000379e 00000000 ... 00000000`

Причина	Диагностика и решение проблем

	`0527c356 00001590 000035d8 00000000 ... 00000000`
	`05ca38d8 00002254 0000384d 00000000 ... 00000000`
	Во втором столбце отобразится количество ошибок с момента последней перезагрузки сервера. Если это количество увеличивается более чем на 10 за сутки:
	1. Узнайте текущий максимальный размер очереди входящих пакетов, которые ожидают обработки ядром:
	`sysctl net.core.netdev_max_backlog`
	2. Увеличьте размер очереди в два раза:
	`sysctl -w net.core.netdev_max_backlog=<Новое значение>`
	3. Через сутки проверьте, на сколько увеличивается количество ошибок.
	Ошибки сброса CPU LIMIT DROPS. Проверьте наличие ошибок:
	`cat /proc/net/softnet_stat`
	Пример вывода:
	`2011e8ef 003b8226 00003511 00000000 ... 00000000`
	`060d102b 000021af 0000364d 00000000 ... 00000000`
	`06f72be1 000019ad 00003808 00000000 ... 00000000`
	`0602bbd3 00001437 0000379e 00000000 ... 00000000`
	`0527c356 00001590 000035d8 00000000 ... 00000000`
	`05ca38d8 00002254 0000384d 00000000 ... 00000000`

Причина	Диагностика и решение проблем

	Во третьем столбце отобразится количество ошибок с момента последней перезагрузки сервера. Если это количество увеличивается более чем на 10 за сутки:
	1. Узнайте текущее максимальное количество пакетов, которое ядро может обработать за одно прерывание:
	`sysctl net.core.netdev_budget`
	2. Увеличьте лимит в два раза:
	`sysctl -w net.core.netdev_budget=<Новое значение>`
	3. Через сутки проверьте, на сколько увеличивается количество ошибок

Красные индикатор и рамка	
Утилизация физического (псевдофизического) сетевого адаптера превышает 95%	Определите сетевые адаптеры с высокой утилизацией. Вариант 1: На виджете **Max Network utilization** выберите точку на графике с максимальным значением. Откроется всплывающая подсказка, в которой отобразится имя узла и название адаптера. Вариант 2: 1. Нажмите на индикатор **Network** и по ссылке откройте дашборд **Network**. 2. На виджете **Network Traffic** определите максимально нагруженные адаптеры, последовательно выбирая узлы и их сетевые адаптеры в верхней части дашборда.

Причина	Диагностика и решение проблем
	Для решения проблемы рекомендуется: — Заменить сетевые адаптеры на более скоростные, (например, со скоростью 10 Гбит/с), что возможно потребует увеличения вычислительной мощности узлов. — Увеличить количество узлов, обрабатывающих трафик
Доля ошибок для физического (псевдо-физического) сетевого адаптера или сетевой подсистемы ядра ОС превышает 0,95%	Доля ошибок отображается на виджете **Max Network Errors**. Для всех ненулевых значений под диаграммами отображается описание ошибки с указанием максимального значения за наблюдаемый период. Ошибки делятся на следующие типы: — **RC ERRORS** — ошибки приема; — **TR ERRORS** — ошибки передачи; — **RC DROPS** — ошибки сброса при приеме; — **TR DROPS** — ошибки сброса при передаче; — **CPU BACKLOG DROPS** — ошибки сброса вследствие переполнения очереди `netdev_max_backlog` ядра ОС; — **CPU LIMIT DROPS** — ошибки сброса вследствие превышения лимита времени, выделяемого ЦП на обработку очереди в ядре ОС. Кроме того, основную сетевую статистику можно посмотреть на дашборде **Infrastructure** → **Network**. Более подробные сетевые метрики по умолчанию не собираются, поскольку это может привести к дополнительной нагрузке на узел.

Причина	Диагностика и решение проблем

	Вы можете включить детальный сбор метрик на несколько минут для выполнения временной диагностики:
	1. На узле создайте файл `/opt/ptaf/conf/collect_node_network_socket_stats` для сбора метрик.
	2. После диагностики удалите файл, чтобы остановить сбор метрик.
	Общие ошибки RC ERRORS и TR ERRORS. Для диагностики ошибок и получения статистики драйвера сетевого адаптера выполните команду:
	`ethtool -S eth-ext1`
	Названия счетчиков зависят от драйвера, что может потребовать уточнения в документации производителя для разделения общих ошибок на конкретные типы.
	Чаще всего ошибки вызваны проблемами адаптера, кабеля или оборудования внешней сети.
	Ошибки сброса RC DROPS и TR DROPS. Ошибки сброса обычно вызваны переполнением буферов или превышением лимитов:
	— Проверьте текущие и максимальные значения для буферов и увеличьте их при возможности:
	`ethtool -g eth-ext1`
	`ethtool -g eth-ext1 rx 4096`
	`ethtool -g eth-ext1 tx 4096`
	Пример вывода команды `ethtool -g eth-ext1`:
	`Ring parameters for eth-ext1:`
	`Pre-set maximums:`
	`RX: 4096`
	`RX Mini: n/a`
	`RX Jumbo: n/a`

Причина	Диагностика и решение проблем

	TX: 4096
	Current hardware settings:
	RX: 256
	RX Mini: n/a
	RX Jumbo: n/a
	TX: 256
	— Для предотвращения переполнения включите приостановку отсылки кадров (требуется поддержка коммутатором):
	`ethtool -a eth-ext1`
	`ethtool -a eth-ext1 autoneg on`
	`ethtool -a eth-ext1 rx on`
	`ethtool -a eth-ext1 tx on`
	Пример вывода команды `ethtool -a eth-ext1`:
	Pause parameters for eth-ext1:
	Autonegotiate: on
	RX: off
	TX: off
	— Проверьте распределение прерываний:
	`egrep "CPU0|eth-ext1" /proc/interrupts`
	Пример вывода:
	CPU0 CPU1 CPU2 CPU3 CPU4 CPU5 CPU6 CPU7
	31: 0 0 0 0 0 1 0 0 IR-PCI-MSI 1048576-edge eth-ext1
	32: 0 8818955 0 0 0 0 27 0 IR-PCI-MSI 1048577-edge eth-ext1-TxRx-0

Причина	Диагностика и решение проблем

```
  33:          0          0    7363245          0          0          0          0
        32  IR-PCI-MSI 1048578-edge      eth-ext1-TxRx-1
  34:    5573688          0          0          0          0          0          0
         0  IR-PCI-MSI 1048579-edge      eth-ext1-TxRx-2
  35:          0    5852035          0          0          0          0          0
         0  IR-PCI-MSI 1048580-edge      eth-ext1-TxRx-3
  36:          0          0    5738363          0          0          0          0
         0  IR-PCI-MSI 1048581-edge      eth-ext1-TxRx-4
  37:          0          0          0    5573741          0          0          0
         0  IR-PCI-MSI 1048582-edge      eth-ext1-TxRx-5
  38:          0          0    5576699          0         30          0          0
         0  IR-PCI-MSI 1048583-edge      eth-ext1-TxRx-6
  39:          0          0          0    5823076          0         26          0
         0  IR-PCI-MSI 1048584-edge      eth-ext1-TxRx-7
```

На скоростях от 100 Мбит/с системные прерывания, привязанные к очередям сетевого адаптера, должны распределяться между разными ядрами ЦП. Убедитесь, что разные прерывания (строки вывода команды) равномерно распределены между ядрами ЦП (имеют ненулевые счетчики в разных столбцах `CPUx`).

Убедитесь в наличии достаточного количества очередей ввода-вывода: серверные сетевые адаптеры со скоростью 10 Гбит/с, необходимые для нормального функционирования кластера под нагрузкой, имеют от 100 или более очередей на каждом сетевом адаптере (количество строк вывода команды).

Ошибки сброса CPU BACKLOG DROPS. Проверьте наличие ошибок:

```
cat /proc/net/softnet_stat
```

Пример вывода:

Причина	Диагностика и решение проблем

	`2011e8ef 003b8226 00003511 00000000 ... 00000000`
	`060d102b 000021af 0000364d 00000000 ... 00000000`
	`06f72be1 000019ad 00003808 00000000 ... 00000000`
	`0602bbd3 00001437 0000379e 00000000 ... 00000000`
	`0527c356 00001590 000035d8 00000000 ... 00000000`
	`05ca38d8 00002254 0000384d 00000000 ... 00000000`
	Во втором столбце отобразится количество ошибок с момента последней перезагрузки сервера. Если это количество увеличивается более чем на 10 за сутки:
	1. Узнайте текущий максимальный размер очереди входящих пакетов, которые ожидают обработки ядром:
	`sysctl net.core.netdev_max_backlog`
	2. Увеличьте размер очереди в два раза:
	`sysctl -w net.core.netdev_max_backlog=<Новое значение>`
	3. Через сутки проверьте, на сколько увеличивается количество ошибок.
	Ошибки сброса CPU LIMIT DROPS. Проверьте наличие ошибок:
	`cat /proc/net/softnet_stat`
	Пример вывода:
	`2011e8ef 003b8226 00003511 00000000 ... 00000000`
	`060d102b 000021af 0000364d 00000000 ... 00000000`

Причина	Диагностика и решение проблем

	`06f72be1 000019ad 00003808 00000000 ... 00000000`
	`0602bbd3 00001437 0000379e 00000000 ... 00000000`
	`0527c356 00001590 000035d8 00000000 ... 00000000`
	`05ca38d8 00002254 0000384d 00000000 ... 00000000`
	Во третьем столбце отобразится количество ошибок с момента последней перезагрузки сервера. Если это количество увеличивается более чем на 10 за сутки:
	1. Узнайте текущее максимальное количество пакетов, которое ядро может обработать за одно прерывание:
	`sysctl net.core.netdev_budget`
	2. Увеличьте лимит в два раза:
	`sysctl -w net.core.netdev_budget=<Новое значение>`
	3. Через сутки проверьте, на сколько увеличивается количество ошибок

Д.9. Индикатор Nodes

Таблица 40. Индикатор Nodes

Причина	Диагностика
Красный индикатор	
Неработоспособен один из узлов кластера PT AF	Найдите проблемное веб-приложение: 1. Нажмите на индикатор **Nodes** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещений **HostNotReady** или **K8sNodeNotReady** с указанием имени недоступного узла. Выполните стандартную диагностику причин недоступности узла: — Проверьте работоспособность узла; — Проверьте настройку сети для узла (связность нижнего уровня, адресацию, маршрутизацию, межсетевой экран ОС, DNS). — Проверьте сетевую доступность узла с других узлов по IP-адресам и DNS-имени, доступность TCP-портов и UDP-портов, необходимых для работы кластера PT AF, настройку межсетевого экрана между узлами (при его наличии)

Причина	Диагностика
	Желтая рамка
На одном из узлов не синхронизировано системное время	Порядок диагностики: 1. На дашборде **System status** на виджете **Time Sync** найдите узлы с несинхронизированным временем. 2. На каждом узле выполните диагностику службы chrony: • проверьте работоспособность службы — `systemctl status chrony`; • получите статус источников времени — `chronyc sources`; • выполните ручную синхронизацию — `chronyc waitsync 30`. 3. Проанализируйте полученные сообщения
	Красная рамка
На одном из узлов неработоспособна служба ОС	Определите проблемные узел и службу. Вариант 1: 1. Нажмите на индикатор **Nodes** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **HostNodeSystemdStateFailed** с указанием узла и неработоспособной службы. Вариант 2: 1. Нажмите на индикатор **Nodes** и по ссылке откройте дашборд **Systemd units**.

Причина	Диагностика
	В панели **Top 5 failed units** отобразятся пять последних неработоспособных служб. 2. Выберите узел, службу и период для просмотра журнала службы. 3. На виджете **Target unit logs** проанализируйте журналы службы

Д.10. Индикатор PG SQL

Таблица 41. Индикатор PG SQL

Причина	Диагностика
Красный индикатор	
Один из узлов в кластере PostgreSQL неработоспособен	Определите проблемный узел: 1. Нажмите на индикатор **PG SQL** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbPgExporterUP** с указанием имени узла
Количество активных подключений к БД PostgreSQL достигло порогового значения (доступно менее 10 новых подключений)	Определите проблемный узел: 1. Нажмите на индикатор **PG SQL** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbPgLimitConnections** с указанием имени узла

Причина	Диагностика
За последние 5 минут в БД PostgreSQL возникла ситуация взаимной блокировки (deadlock)	Определите проблемный узел: 1. Нажмите на индикатор **PG SQL** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbPgDeadlocks** с указанием имени узла
Желтая рамка	
Один из узлов кластера stolon-keeper сообщает о необходимости перезагрузки (или самого узла, или его конфигурации)	Определите проблемный узел: 1. Нажмите на индикатор **PG SQL** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещений **DbStolonKeeperNeedsRestart** или **DbStolonKeeperNeedsReload** с указанием имени узла
Красные индикатор и рамка	
В кластере stolon-sentinel нет «лидера»	Определите проблемный узел: 1. Нажмите на индикатор **PG SQL** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbStolonSentinelNotLeader** с указанием имени узла
В кластере stolon-keeper нет «мастера»	Определите проблемный узел: 1. Нажмите на индикатор **PG SQL** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **DbStolonNotActiveMaster** с указанием имени узла

Д.11. Индикатор PTAF Backend

Таблица 42. Индикатор PTAF Backend

Причина	Диагностика
Красные индикатор и рамка	
За последнюю минуту более 3% запросов от сервисов пространства ptaf-backend к сервису управления Kubernetes завершились с ошибкой	Определите проблемное приложение: 1. Нажмите на индикатор **PTAF Backend** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **PtafK8sManagerCallsErrors** с указанием имени приложения
За последние пять минут более 3% вызовов клиентов сервиса ptaf_rpc завершились с ошибкой	Определите проблемное приложение: 1. Нажмите на индикатор **PTAF Backend** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **PtafRpcClientCallsFailed** с указанием имени приложения
За последние пять минут более 3% попыток обработки сервисных сообщений ptaf_rpc завершились с ошибкой	Определите проблемное приложение: 1. Нажмите на индикатор **PTAF Backend** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **PtafRpcServiceHandlingErrMsg** с указанием имени приложения
За последние пять минут более 3% сервисных сообщений ptaf_rpc были отброшены	Определите проблемное приложение: 1. Нажмите на индикатор **PTAF Backend** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **PtafRpcServiceRejectedMsg** с указанием имени приложения

Причина	Диагностика
За последние пять минут более 3% сообщений между сервисами ptaf-backend завершились с ошибкой	Определите проблемное приложение: 1. Нажмите на индикатор **PTAF Backend** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **PtafRpcTransportPublicationsFail** с указанием имени приложения

Д.12. Индикатор RabbitMQ

Таблица 43. Индикатор RabbitMQ

Причина	Диагностика
Красные индикатор и рамка	
Количество файловых дескрипторов, используемых брокером сообщений RabbitMQ, достигло порогового значения	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqLimit** с указанием имени узла
Дисковое пространство, используемое брокером сообщений RabbitMQ, достигло порогового значения	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqFreeDiskSpace** с указанием имени узла

Причина	Диагностика
Объем ОЗУ, используемый брокером сообщений RabbitMQ, достиг 1500 МБ (1 500 000 000 байт). Публикация новых сообщений остановлена	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqMemoryUsedWatermark** с указанием имени узла
Брокер сообщений RabbitMQ использует более 90% отведенного ему объема ОЗУ	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqMemoryUsed** с указанием имени узла
Брокер сообщений RabbitMQ использует более 90% отведенного ему количество файловых дескрипторов	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqFds** с указанием имени узла
Лимит свободного дискового пространства почти достигнут (осталось менее 10% до лимита)	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqDiskSpace** с указанием имени узла
Один из узлов кластера RabbitMQ недоступен	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqUnreachableClusterPeersCount** с указанием имени узла

Причина	Диагностика
Одна из очередей в RabbitMQ содержит более 30 000 необработанных сообщений	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqQueueMessagesReady** с указанием имени узла
Одна из очередей в RabbitMQ содержит более 3000 сообщений, обработка которых начата, но не закончена	Определите проблемный узел: 1. Нажмите на индикатор **RabbitMQ** и по ссылке откройте дашборд **Alerts status**. 2. В панели **Firing alerts** проверьте наличие оповещения **RabbitmqQueueMessagesUnacknowledged** с указанием имени узла

Д.13. Индикатор RAM

Таблица 44. Индикатор RAM

Причина	Диагностика
Желтый индикатор	
Для одного из узлов утилизация ОЗУ находится в диапазоне 85—95%	Определите узел с повышенной утилизацией ОЗУ: 1. На виджете **RAM utilization / k8s provisioning** выберите точку с максимальным значением на непрерывном графике.

Причина	Диагностика
	Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **UTIL**. 2. Нажмите на индикатор **RAM** и по ссылке откройте дашборд **Nodes**. 3. Выберите узел, найденный на первом шаге, и проанализируйте диаграммы на виджете **Memory**
Красный индикатор	
Для одного из узлов утилизация ОЗУ превышает 95%	Определите узел с высокой утилизацией ОЗУ: 1. На виджете **RAM utilization / k8s provisioning** выберите точку с максимальным значением на непрерывном графике. Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **UTIL**. 2. Нажмите на индикатор **RAM** и по ссылке откройте дашборд **Nodes**. 3. Выберите узел, найденный на первом шаге, и проанализируйте диаграммы на виджете **Memory**
Желтая рамка	
Для одного из узлов загрузка ОЗУ для обработки запросов подов Kubernetes находится в диапазоне 80—90%	Определите узел с повышенной загрузкой ОЗУ: 1. На виджете **RAM utilization / k8s provisioning** выберите точку с максимальным значением на прерывистом графике.

Причина	Диагностика
	Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **k8s provisioning**. 2. Нажмите на индикатор **RAM** и по ссылке откройте дашборд **Cluster overview**. 3. Выберите узел, найденный на первом шаге, и проанализируйте диаграммы на виджете **k8s Memory requests**, чтобы определить количество и тип подов, которые может дополнительно поддержать узел
Красная рамка	
Для одного из узлов загрузка ОЗУ для обработки запросов подов Kubernetes превышает 90%	Определите узел с высокой загрузкой ОЗУ: 1. На виджете **RAM utilization / k8s provisioning** выберите точку с максимальным значением на прерывистом графике. Откроется всплывающая подсказка, в которой отобразится имя узла как значение параметра **k8s provisioning**. 2. Нажмите на индикатор **RAM** и по ссылке откройте дашборд **Cluster overview**. 3. Выберите узел, найденный на первом шаге, и проанализируйте диаграммы на виджете **k8s Memory requests**, чтобы определить количество и тип подов, которые может дополнительно поддержать узел

Д.14. Индикатор RPS / app errors

Таблица 45. Индикатор RPS / app errors

Причина	Диагностика
Желтый индикатор	
Суммарное значение RPS за последнюю минуту меньше порога **Minimum mark for Total RPS** или больше порога **Maximum mark for Total RPS**	Проанализируйте распределение RPS по веб-приложениям: 1. Нажмите на индикатор **RPS** и по ссылке откройте дашборд **Tenants**. 2. В панели **Webapp RPS** в каждом изолированном пространстве для каждого его веб-приложения просмотрите значение RPS
Желтая рамка	
Количество ответов с кодами 50x, получаемых PT AF от защищаемых серверов, находится в пределах от одного до двух процентов от общего количества запросов, отправляемых к защищаемым серверам	Просмотрите журналы защищаемых серверов, проанализируйте их трафик. Также проверьте корректность настройки PT AF
Красная рамка	
Количество ответов с кодами 50x, получаемых PT AF от защищаемых серверов, равно двум или более процентам от общего количества запросов, отправляемых к защищаемым серверам	Просмотрите журналы защищаемых серверов, проанализируйте их трафик. Также проверьте корректность настройки PT AF

Предметный указатель

B

bond-интерфейс
- время задержки 229
- настройка 228
- политика передачи пакетов 229
- создание 226
- состав 229

W

WSC 219, 243

A

агенты
- лицензирование 24
- развертывание 15

Д

действия с трафиком 75
- add IP address to list 77
- log to DB 77
- send custom response 77
- send to syslog 77
- skip 77
- записывать событие в базу данных 102

K

кластер
- лицензирование 24
- пропускная способность 24
- развертывание 24, 25
- роли узлов 233

команды оболочки WSC
- admin 220
- border 224
- border generate_token 224
- border list 224
- border renew_certs 224
- border set token 225
- config 220
- config accept 222
- config commit 221
- config commit force 221
- config commit network 221
- config reset 221
- config try 221
- dhcp 225
- dhcp list 225
- dhcp set 225
- exit 222
- help 222
- history 222
- hostname 223
- if 226
- if bond 226
- if del 226
- if list 226
- if mode 226

if set 227
if vlan 230
info 223
inventory 230
inventory check 233
inventory node 230
inventory node add 231
inventory node del 231
inventory node list 230
inventory node set 231
inventory render 233
inventory service 234
inventory service add 234
inventory service del 234
inventory service list 234
inventory service set 234
keys 235
keys generate 235
ntp 235
ntp add 236
ntp del 236
ntp list 236
ntp list system 236
route 236
route add 237
route del 239
route list 236
route rule 239
route rule add 240
route rule del 241
route rule list 240
route table 241
route table add 241
route table del 242
route table list 242
snapshot 223
snapshot restore 223
timezone 223
vip 242
vip list 243
vip set 243

Л

лицензия
- активация 151
- номер 26
- ошибки 195
- приобретение 23
- просмотр 151, 194
- срок действия 26

М

маршрутизация
- добавление статических маршрутов в таблицу 237
- создание правила маршрутизации 240
- удаление правил маршрутизации 241
- удаление статических маршрутов из таблицы 239

П

правила обработки трафика
- группы 67
- действия при срабатывании 102
- исключения 70, 268
- отключение 70
- параметры 69
- условия запуска 70

Глоссарий

Apache Wicket

Фреймворк с открытым исходным кодом для создания веб-приложений.

Django

Фреймворк для создания веб-приложений на языке программирования Python.

Ghostscript

Набор утилит, позволяющий конвертировать файлы PostScript в файлы различных графических форматов. Используется во многих популярных CMS.

Grafana

Система с открытым исходным кодом для построения графиков мониторинга и анализа метрик.

Grails

Программа для создания веб-приложений, написанная на языке Groovy. Работает на платформе Java.

ImageMagick

Кроссплатформенный консольный редактор изображений, используемый во многих популярных CMS. Некоторые его версии являются уязвимыми для внедрения вредоносного кода через имена файлов или посредством обработки файлов.

Jetty

Контейнер сервлетов, который может быть использован как HTTP-сервер или в паре со специализированным HTTP-сервером.

Jolokia

Программный продукт с открытым кодом, который предоставляет HTTP API для технологии JMX.

Joomla

Система управления содержимым (CMS) с открытым исходным кодом, написанная на языках PHP и JavaScript.

Kubernetes

Открытое программное обеспечение для автоматизации развертывания, масштабирования и управления контейнеризированными приложениями. Используется в качестве системы оркестрации микросервисов.

Spring Boot

Универсальная программная платформа с открытым исходным кодом на Java, используемая для создания микросервисов.

WSC

Web Server Console — оболочка для базовой конфигурации системы, представляющая собой интерфейс командной строки.

зона доступности

Свойство узла кластера, определяющее, трафик каких изолированных пространств будет на нем обрабатываться.

необработанные данные

Исходный HTTP-запрос и ответ, не подвергнутые обработке.

политика безопасности

Набор правил, предназначенный для защиты отдельного веб-приложения. Формируется при помощи механизма наследования на основе пользовательского шаблона политики безопасности. Параметры правил, входящих в набор, могут быть переопределены пользователем.

правило

Проверка, которая срабатывает при соблюдении определенного условия в контексте защищаемого приложения для обнаружения угрозы безопасности или атаки.

событие безопасности

Факт обнаружения трафика с определенными характеристиками при помощи правила.

транзакция

Группа последовательных операций для получения, проверки и передачи HTTP-запроса и ответа между клиентом и защищаемым веб-приложением, а также для прерывания передачи данных при обнаруженном нарушении, с подменой ответа. Индентификатор транзакции указывается в свойствах записей о событиях безопасности, регистрируемых в результате проверки.

фингерпринт

Отпечаток аппаратных характеристик сервера, который используется, например, для создания файла лицензии.



positive technologies

Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.