ООО «Веб-Сервер», ОГРН 1227700436578, ИНН 9704151517
ул. Вятская, д. 27, стр. 7, г. Москва, 127015



Описание функциональных характеристик

версия 1.3

ООО «Веб-Сервер»

нояб. 13, 2026

Оглавление

1 Аннотация **1**

2 Обзор решения и возможности **2**
2.1 Функциональность Angie ADC . . . 2

3 Управление трафиком и сервисы балансировки **4**
3.1 Балансировщик нагрузки . . . 4
3.1.1 Настройка конфигурации . . . 5
3.1.1.1 Общая информация . . . 6
3.1.1.2 Текстовый конфигуратор . . . 7
3.1.1.3 Визуальный конфигуратор . . . 7
3.1.1.4 Перезапуск балансировщика . . . 8
3.1.1.5 Логи балансировщика . . . 8
3.1.1.6 Принцип конфигурации . . . 8
3.1.1.7 Использование портов . . . 9
3.1.1.8 Настройка простого прокси-сервера . . . 9
3.1.1.9 Настройка балансировки нагрузки . . . 10
3.1.2 Управление резервными конфигурациями . . . 11
3.1.2.1 Просмотр списка сохраненных конфигураций . . . 11
3.1.2.2 Изменение рабочего статуса хранимой конфигурации . . . 11
3.1.2.3 Восстановление последней рабочей версии конфигурации . . . 11
3.1.2.4 Восстановление конфигурации из резервной копии . . . 11
3.1.2.5 Выбор репозитория для хранения конфигураций . . . 12
3.1.3 Методы балансировки . . . 13
3.1.3.1 Примеры HTTP-балансировки нагрузки . . . 14
3.1.3.2 Примеры TCP/UDP-балансировки нагрузки . . . 18
3.1.4 Предоставление доступов на работу с конфигурацией . . . 21
3.1.4.1 Предоставление прав на просмотр и редактирование . . . 21
3.1.4.2 Просмотр выданных доступов . . . 22
3.1.4.3 Редактирование выданных доступов . . . 22
3.1.4.4 Удаление выданных доступов . . . 22
3.1.5 Проверки работоспособности серверов . . . 22
3.1.5.1 Пассивные проверки . . . 22
3.1.5.2 Активные проверки . . . 23
3.1.6 Резервирование проксируемых серверов и групп . . . 25
3.1.6.1 Запасные серверы (spare-серверы) . . . 26
3.1.6.2 Резервные группы серверов (backup-группы) . . . 26
3.1.7 Управление сертификатами . . . 27
3.1.8 Аутентификация клиентов . . . 28
3.1.8.1 Настройка аутентификации клиентов . . . 29
3.1.8.2 Изменение параметров портала аутентификации . . . 30

3.1.8.3 Выбор домена маршрутизации для портала . . . 30
3.1.8.4 Удаление портала аутентификации . . . 31
3.1.9 Режим отладки . . . 31
3.1.9.1 Отладочный лог . . . 31
3.1.9.2 Расположение директивы . . . 32
3.1.9.3 Лог для отдельных адресов . . . 33
3.2 Глобальная балансировка . . . 33
3.2.1 Настройка GSLB . . . 34
3.2.2 Типы глобальной балансировки . . . 36
3.2.2.1 Балансировка round-robin . . . 36
3.2.2.2 Балансировка weighted round-robin . . . 36
3.2.2.3 Балансировка failover . . . 36
3.2.2.4 Балансировка ip-hash . . . 36
3.2.2.5 Балансировка geo-affinity . . . 37
3.2.2.6 Балансировка least connection . . . 37
3.2.2.7 Закрепление бэкенда за клиентом (Persistence) . . . 38
3.2.3 Включение и выключение глобальной балансировки . . . 39
3.2.4 Использование EDNS Client Subnet . . . 39
3.2.5 Настройка IP-адресов ADNS . . . 39
3.2.6 Определение доступности дата-центров . . . 41
3.2.6.1 Рекомендации . . . 41
3.2.6.2 Состояния монитора . . . 41
3.2.6.3 Пример . . . 41
3.2.7 Добавление доменов и записей . . . 43
3.2.8 Балансировка по географическому положению . . . 49
3.2.8.1 Настройка географических площадок . . . 49
3.2.8.2 Настройка групп клиентских подсетей . . . 50
3.2.8.3 Настройка баз GeoIP . . . 51
3.2.8.4 Настройка балансировки по географическому положению . . . 52
3.3 Типовые задачи и примеры . . . 53
3.3.1 Сеть и адресация . . . 53
3.3.2 TLS и сертификаты . . . 53
3.3.3 Балансировка и отказоустойчивость . . . 53
3.3.4 Безопасность и контроль доступа . . . 53
3.3.5 Доставка контента . . . 53
3.3.6 Администрирование и наблюдаемость . . . 53
3.3.6.1 Сеть и адресация . . . 53
3.3.6.2 TLS и сертификаты . . . 67
3.3.6.3 Балансировка и отказоустойчивость . . . 83
3.3.6.4 Безопасность и контроль доступа . . . 86
3.3.6.5 Доставка контента . . . 92
3.3.6.6 Администрирование и наблюдаемость . . . 93

4 Отказоустойчивость и маршрутизация 97
4.1 Пара высокой доступности . . . 97
4.1.1 Обзор работы . . . 98
4.1.1.1 Режим Active / Standby . . . 98
4.1.1.2 Развертывание . . . 99
4.1.1.3 Обновление конфигурации и синхронизация . . . 99
4.1.2 Создание пары высокой доступности . . . 99
4.1.2.1 Требования . . . 99
4.1.2.2 Предварительные действия . . . 99
4.1.2.3 Создание пары высокой доступности в режиме Active / Standby . . . 100
4.1.3 Настройка высокой доступности в паре . . . 101
4.1.3.1 VRRP . . . 101
4.1.3.2 Динамическая маршрутизация в паре высокой доступности . . . 104
4.1.3.3 OSPF . . . 105
4.1.3.4 BGP . . . 108

4.1.4 Управление парой . . . 112
4.1.4.1 Просмотр информации о паре . . . 112
4.1.4.2 Обновление конфигурации и синхронизация . . . 113
4.1.4.3 Настройка протокола опроса доступности узлов . . . 114
4.1.4.4 Удаление пары . . . 114
4.1.5 Привязка клиентских сессий . . . 115
4.2 IP-маршрутизация . . . 116
4.2.1 VRRP . . . 116
4.2.1.1 Где настраивается VRRP . . . 117
4.2.1.2 Ограничения . . . 117
4.2.2 Настройка динамической маршрутизации . . . 140
4.2.2.1 Просмотр . . . 140
4.2.3 BGP-маршрутизация . . . 140
4.2.3.1 Резервирование с помощью протокола BGP (Active-Standby) . . . 141
4.2.3.2 Распределение нагрузки с помощью протокола BGP (Active-Active) . . . 148
4.2.4 OSPF-маршрутизация . . . 159
4.2.4.1 Резервирование с помощью протокола OSPF (Active-Standby) . . . 159
4.2.4.2 Распределение нагрузки с помощью протокола OSPF (Active-Active) . . . 166
4.2.5 Статическая маршрутизация . . . 172
4.2.5.1 Пример . . . 172
4.2.6 Использование протокола BFD для уменьшения времени реакции . . . 173
4.2.6.1 Введение . . . 173
4.2.6.2 Настройка с OSPF . . . 173
4.2.6.3 Настройка с BGP . . . 175
4.2.6.4 Настройка с VRRP . . . 176
4.2.6.5 Настройка со статическими маршрутами . . . 176
4.2.6.6 Настройка независимого пира . . . 177
4.2.6.7 Профиль . . . 178
4.2.7 Настройка RHI . . . 179
4.2.7.1 Как это работает . . . 179
4.2.7.2 Настройка балансировщика нагрузки . . . 179
4.2.7.3 Привязка префиксов к апстримам . . . 180
4.2.7.4 Анонс по BGP . . . 181
4.2.7.5 Анонс по OSPF . . . 181
4.2.7.6 Возврат отозванного префикса . . . 183
4.2.8 Настройка ECMP . . . 183
4.2.8.1 Распределение трафика между несколькими Angie ADC . . . 183
4.2.8.2 Внешнее хранилище sticky . . . 185
4.2.8.3 Распределение трафика между несколькими маршрутизаторами . . . 187
4.2.8.4 UCMP-балансировка . . . 188

5 Мониторинг и диагностика 191
5.1 Метрики и статистика . . . 191
5.1.1 Статистика балансировщика нагрузки . . . 191
5.1.1.1 Виджет "Серверные зоны" . . . 192
5.1.1.2 Виджет "Зоны апстримов" . . . 193
5.1.2 Статистика глобальной балансировки . . . 194
5.1.2.1 Запрошенные имена . . . 195
5.1.2.2 Состояния записей . . . 195
5.1.3 Мониторинг состояния системы . . . 196
5.1.3.1 Сводная инфографика . . . 196
5.1.3.2 Центральный процессор . . . 197
5.1.3.3 Обработка данных . . . 197
5.1.3.4 Сетевые интерфейсы . . . 197
5.1.3.5 ОЗУ . . . 197
5.1.3.6 Файловая система . . . 198
5.1.3.7 Накопители (ROM) . . . 198
5.1.3.8 S.M.A.R.T. атрибуты диска . . . 198

5.1.3.9 Датчики . . . 199
5.1.4 Мониторинг в Console Light . . . 199
5.1.4.1 Переход в Console Light . . . 199
5.1.4.2 Интерфейс . . . 200
5.1.4.3 Вкладка "Angie" . . . 200
5.1.4.4 Вкладка "HTTP-зоны" . . . 203
5.1.4.5 Вкладка "HTTP-апстримы" . . . 205
5.1.4.6 Вкладка "TCP/UDP-зоны" . . . 206
5.1.4.7 Вкладка "TCP/UDP-апстримы" . . . 208
5.1.4.8 Вкладка "Кэши" . . . 209
5.1.4.9 Вкладка "Общие зоны" . . . 210
5.1.4.10 Вкладка "DNS-резолверы" . . . 211
5.1.4.11 Виджет "Настройки" . . . 211
5.1.4.12 Панель управления консолью . . . 212
5.1.5 Экспорт метрик . . . 212
5.1.5.1 Экспорт метрик Node Exporter . . . 212
5.1.5.2 Экспорт метрик балансировщика нагрузки . . . 212
5.1.5.3 Экспорт системных метрик Angie ADC . . . 213
5.1.6 SNMP . . . 213
5.1.6.1 Настройка для SNMPv3 . . . 214
5.1.6.2 Настройка для SNMPv2c . . . 215
5.1.6.3 Настройка домена маршрутизации . . . 216
5.1.6.4 Метрики операционной системы . . . 216
5.1.6.5 Собственные метрики Angie ADC . . . 217
5.2 Доступность . . . 218
5.2.1 Датчики . . . 219
5.2.2 Мониторы . . . 219
5.2.3 Применение . . . 219
5.2.3.1 Настройка датчиков и мониторов . . . 220
5.2.3.2 Мониторинг доступности . . . 223
5.3 Диагностика и логирование . . . 225
5.3.1 Диагностика сети . . . 225
5.3.2 Диагностика через CLI . . . 226
5.3.3 Аварийная диагностика . . . 227
5.3.4 Журналы событий и экспорт . . . 228
5.3.4.1 Просмотр журналов событий . . . 228
5.3.4.2 Экспорт логов . . . 230
5.3.5 Техническая поддержка . . . 231

6 Администрирование и безопасность 232
6.1 Настройка системы . . . 232
6.1.1 Смена имени устройства . . . 232
6.1.1.1 Изменение имени устройства . . . 233
6.1.1.2 CLI . . . 233
6.1.1.3 Мастер настройки . . . 233
6.1.2 Настройка HTTPS . . . 233
6.1.2.1 Загрузка сертификата управления и включение защищенного соединения . . . 233
6.1.3 Управление сертификатами . . . 233
6.1.3.1 Загрузка сертификата данных . . . 234
6.1.3.2 Загрузка доверенного сертификата . . . 235
6.1.3.3 Удаление сертификатов . . . 235
6.1.3.4 Управление через CLI . . . 235
6.1.4 Настройка NTP . . . 235
6.1.4.1 Настройка конфигурации NTP . . . 236
6.1.4.2 Статусы . . . 236
6.1.4.3 CLI . . . 237
6.1.5 Базы GeoIP . . . 237

6.1.5.1 Загрузка и замена базы . . . 238
6.1.5.2 Удаление базы . . . 239
6.2 Управление кластером . . . 239
6.2.1 Мониторинг состояния кластера . . . 240
6.2.1.1 Информация о текущем узле кластера . . . 240
6.2.1.2 Подсистема управления конфигурацией . . . 241
6.2.1.3 Подсистема обмена метриками . . . 241
6.2.1.4 Узлы кластера . . . 242
6.2.2 Применение, отмена и откат изменений . . . 243
6.2.2.1 Применение изменений . . . 244
6.2.2.2 Отмена изменений . . . 244
6.2.2.3 Откат изменений . . . 244
6.2.3 Управление составом узлов в кластере . . . 244
6.2.3.1 Добавление узлов . . . 244
6.2.3.2 Включение и выключение узлов . . . 244
6.2.3.3 Исключение узлов . . . 245
6.3 Сеть и домены маршрутизации . . . 245
6.3.1 Примеры сетевых схем . . . 246
6.3.1.1 Настройка сетевых интерфейсов . . . 246
6.3.1.2 Настройка маршрутизации . . . 250
6.3.1.3 Настройка DNS-резолверов . . . 252
6.3.1.4 Настройка доменов маршрутизации . . . 252
6.4 Управление пользователями и доступами . . . 254
6.4.1 Пользователи и роли . . . 254
6.4.1.1 Локальные пользователи . . . 254
6.4.1.2 Внешние пользователи . . . 254
6.4.1.3 Роли . . . 254
6.4.2 Управление локальными пользователями . . . 255
6.4.2.1 Добавление локального пользователя . . . 255
6.4.2.2 Изменение учетных данных и статуса локального пользователя . . . 256
6.4.2.3 Сброс пароля локального пользователя . . . 256
6.4.2.4 Сброс настроек двухфакторной аутентификации локального пользователя . . . 257
6.4.2.5 Удаление локального пользователя . . . 257
6.4.2.6 Восстановление удаленного локального пользователя . . . 257
6.4.3 Управление пользовательскими сессиями . . . 257
6.4.3.1 Просмотр сессий . . . 258
6.4.3.2 Завершение сессии . . . 258
6.4.3.3 Завершение всех сессий текущего узла . . . 258
6.4.4 Подключение внешних пользователей . . . 259
6.4.4.1 Режим цепочек аутентификации и авторизации . . . 259
6.4.4.2 Профили серверов . . . 262
6.4.4.3 Настройка режима цепочек . . . 268
6.4.4.4 Аутентификация (режим без цепочек) . . . 273
6.4.4.5 Авторизация (режим без цепочек) . . . 275
6.4.5 Парольная политика . . . 280
6.4.5.1 Настройка парольной политики . . . 281
6.4.5.2 Сброс истории паролей для пользователей . . . 282
6.4.5.3 Сброс пароля локального пользователя . . . 282
6.4.5.4 Сброс настроек двухфакторной аутентификации локального пользователя . . . 282
6.4.6 Настройка учетной записи . . . 283
6.4.6.1 Смена пароля учетной записи . . . 284
6.4.6.2 Включение двухфакторной аутентификации . . . 284
6.4.6.3 Отключение двухфакторной аутентификации . . . 285
6.4.7 Аудит действий пользователей . . . 285
6.5 Резервное копирование и восстановление системы . . . 286
6.5.1 Создание резервной копии . . . 287

6.5.2 Обновление резервной копии . . . 287
6.5.3 Скачивание резервной копии . . . 288
6.5.4 Восстановление текущего узла из резервной копии . . . 288
6.5.5 Перенос резервной копии на новый узел . . . 288

7 Мастер настройки по SSH 290
7.1 Меню мастера . . . 291
7.2 Настройка сети узла . . . 291
7.2.1 Первоначальная настройка . . . 292
7.2.2 Настройка сетевых интерфейсов . . . 292
7.2.3 Выделение сети управления . . . 293
7.2.4 Создание домена маршрутизации . . . 293
7.2.5 Создание бондов . . . 293
7.2.6 Создание VLAN-интерфейсов . . . 293
7.2.7 Настройка DNS-серверов . . . 294
7.3 Просмотр конфигурации Angie ADC и сетевых настроек . . . 294
7.4 Смена портов для веб-интерфейса Angie ADC . . . 294
7.5 Изменение имени устройства Angie ADC . . . 294
7.6 Изменение часового пояса . . . 294
7.7 Проверка доступности узла . . . 295
7.8 Аварийная диагностика . . . 295
7.9 Просмотр журнала восстановления из резервной копии . . . 295

8 Создание и масштабирование кластера 296
8.1 Создание точки входа в кластер . . . 296
8.2 Добавление узлов в кластер . . . 297

9 Интерфейс командной строки (CLI) Angie ADC 299
9.1 Поддерживаемые команды . . . 299
9.2 Синтаксис . . . 301
9.3 certificates . . . 301
9.3.1 list . . . 302
9.3.2 info . . . 302
9.3.3 upload . . . 302
9.3.4 remove . . . 303
9.4 configuration . . . 303
9.4.1 end . . . 304
9.4.2 no ha standby . . . 304
9.4.3 routing . . . 304
9.4.4 set . . . 306
9.4.5 unset . . . 307
9.4.6 vrrp . . . 307
9.5 diagnostics . . . 307
9.5.1 arping . . . 308
9.5.2 diag . . . 308
9.5.3 nslookup . . . 308
9.5.3.1 Разовый запрос . . . 308
9.5.3.2 Интерактивный режим . . . 309
9.5.4 ping . . . 310
9.5.5 pingc . . . 310
9.5.6 ss . . . 310
9.5.6.1 Параметры . . . 310
9.5.6.2 Примеры . . . 311
9.5.6.3 Фильтрация по state . . . 311
9.5.6.4 Фильтрация по критериям . . . 311
9.5.7 ssldump . . . 312
9.5.8 tcpdump . . . 313
9.5.9 traceroute . . . 313
9.6 firewall . . . 314

9.6.1 list . . . 314
9.6.2 no open . . . 315
9.6.3 open . . . 315
9.6.4 save . . . 316
9.7 ip . . . 316
9.8 logs . . . 316
9.8.1 Фильтрация вывода . . . 318
9.8.1.1 grep . . . 318
9.8.1.2 include . . . 318
9.8.1.3 exclude . . . 319
9.8.1.4 head . . . 319
9.8.1.5 tail . . . 319
9.9 modules . . . 319
9.9.1 info . . . 320
9.9.2 list . . . 320
9.10 ps . . . 320
9.11 settings . . . 321
9.11.1 angie debug . . . 321
9.11.2 no angie debug . . . 322
9.11.3 reload . . . 322
9.11.4 sysctl . . . 322
9.11.5 syslog . . . 322
9.12 show . . . 324
9.13 system . . . 324
9.13.1 bond . . . 324
9.13.2 hostname . . . 324
9.13.3 ntp . . . 325
9.13.4 reboot . . . 325
9.13.5 stat . . . 326
9.13.6 time . . . 326
9.13.7 timezone . . . 326
9.13.8 upgrade . . . 326
9.13.9 version . . . 326
9.14 transfer . . . 327
9.14.1 edit . . . 327
9.14.2 ls . . . 327
9.14.3 rm . . . 327
9.14.4 view . . . 327
9.15 trusted-ca . . . 327
9.15.1 upload . . . 328
9.15.2 list . . . 328
9.15.3 info . . . 328
9.15.4 remove . . . 329
9.16 web . . . 329
9.16.1 upload . . . 329
9.16.2 tls . . . 330

10 Права на интеллектуальную собственность 331

ГЛАВА 1

Аннотация

Настоящий документ содержит описание функциональных характеристик Angie ADC.

Angie ADC — программное обеспечение класса "контроллер доставки приложений", которое представляет собой систему балансировки, включающее DNS-балансировку, а также позволяющее маршрутизировать и балансировать сетевые запросы, используя протоколы маршрутизации внешнего и внутреннего шлюза.

ГЛАВА 2

Обзор решения и возможности

Angie ADC — комплексное программное решение для балансировки нагрузки и управления сетевым трафиком, включающее балансировку на уровнях L4-L7, интеллектуальную доставку приложений и маршрутизацию, а также глобальную DNS-балансировку (GSLB) и решения для обеспечения высокой доступности.

Angie ADC поддерживает мониторинг и управление через веб-интерфейс и командную строку (CLI), а также предоставляет API для интеграции с внешними системами.

Решение Angie ADC поставляется в виде аппаратного балансировщика и виртуального устройства (Virtual Appliance) и развертывается в *кластере*.

2.1 Функциональность Angie ADC

В таблице ниже приведены основные функции и возможности Angie ADC, а также ссылки на соответствующие разделы документации.

Функции	Документация
Локальная балансировка нагрузки	*Балансировщик нагрузки*
Глобальная балансировка нагрузки (GSLB)	*Глобальная балансировка*
Кластеризация	*Кластер Angie ADC для администрирования нескольких устройств*
Решения для обеспечения высокой доступности и маршрутизации	*Пара высокой доступности*: развертывание высокодоступного решения на базе двух Angie ADC *IP-маршрутизация*: настройки высокой доступности для standalone-устройств Angie ADC
Инструменты для мониторинга и диагностики	*Мониторинг работы балансировщика нагрузки и глобальной балансировки* *Мониторинг системных метрик Angie ADC* *Мониторинг доступности узлов и бэкендов* *Диагностика сети* *Syslog*, *SNMP*
Инструменты для управления и безопасности	Управление через веб-интерфейс и *CLI* *Настройка сетевых интерфейсов* *Управление сертификатами* *Резервное копирование и восстановление системы* *Ролевое разграничение доступа к системе* *Управление пользовательскими сессиями* *Внешняя аутентификация и авторизация RADIUS, LDAP и TACACS+* *Парольная политика* *Настройка учетной записи* *Аудит действий пользователей*
Поддерживаемые протоколы и механизмы	*BGP*, *OSPF*, *VRRP*, *RHI*, *BFD*

ГЛАВА 3

Управление трафиком и сервисы балансировки

Здесь описывается настройка балансировщика нагрузки L4-L7 и глобальной DNS-балансировки (GSLB), а также приведены примеры решения типовых задач.

В этом разделе:

- *Балансировщик нагрузки*
- *Глобальная балансировка*
- *Типовые задачи и примеры*

3.1 Балансировщик нагрузки

В этом разделе:

- *Настройка конфигурации*
- *Управление резервными конфигурациями*
- *Методы балансировки*
- *Предоставление доступов на работу с конфигурацией*
- *Проверки работоспособности серверов*
- *Резервирование проксируемых серверов*
- *Аутентификация клиентов*
- *Управление сертификатами*
- *Режим отладки*

См. также *Типовые задачи и примеры*.

Балансировка

Балансировщик нагрузки позволяет распределять клиентские запросы по серверам на основании выбранного алгоритма балансировки, данных статистики или обратной связи от сервера (см. *Методы балансировки*). В идеале клиентские запросы равномерно распределяются по всем серверам, что увеличивает совокупную производительность системы. Доступна балансировка на двух уровнях: L7 (протокол HTTP) и L4 (TCP и UDP).

Высокая доступность

Высокая доступность при балансировке обеспечивается за счет *проверок работоспособности апстрим-серверов* и *резервирования проксируемых серверов и групп*.

> **Примечание**
>
> Отказоустойчивость самого балансировщика нагрузки обеспечивается отдельно, например с помощью *пары высокой доступности*.

Дополнительная настройка

Помимо алгоритмов распределения запросов, в HTTP- и TCP/UDP-балансировке могут использоваться смежные модули:

- Модуль `queue` создает очередь запросов. Если балансировщик не смог выбрать апстрим-сервер для обработки, то запрос попадает в очередь ожидания. Также можно задать приоритизацию запросов в очереди. Приоритетные запросы будут обрабатываться в первую очередь, что позволит в условиях критической перегрузки сохранить обслуживание наиболее важных клиентов, отсекая второстепенные запросы и повышая устойчивость к DDoS-атакам.
- Модуль `keepalive` позволяет держать открытые неактивные соединения с апстрим-серверами, т. е. не закрывать соединения при завершении обработки запроса.
- Директива `bind_conn`, реализованная в модуле `keepalive`, позволяет привязать клиентское соединение к серверному соединению.
- Модуль `sticky` также позволяет привязывать клиентское соединение к апстрим-серверу, но на основе информации, содержащейся в самом запросе.
- Модуль `zone` обеспечивает доступ с использованием REST API. API позволяет получать набор метрик, в том числе относящихся к балансировке.
- Модуль `upstream_probe` позволяет обеспечить активные проверки апстрим-серверов.

Подробнее см. в справочнике HTTP-модуля Upstream и потокового модуля Upstream.

Хранение версий конфигурации

Все версии конфигурации балансировщика нагрузки сохраняются. Вы можете просмотреть историю изменений, а также *восстановить конфигурацию* из резервной копии.

Разделение доступа к конфигурации

Администратор может выдать ограниченный доступ к конфигурации пользователям Angie ADC с ролью **Оператор**. Подробнее см. *Предоставление доступов на работу с конфигурацией* и *Делегирование сервиса оператору*.

Справочная информация

В разделе adc_lb-reference представлены сведения о встроенных и сторонних модулях, примеры их настройки, а также поддерживаемые ими директивы и переменные.

3.1.1 Настройка конфигурации

В этой статье:

- *Общая информация*;
- *Текстовый конфигуратор*;
- *Визуальный конфигуратор*;
- *Перезапуск балансировщика*;
- *Логи балансировщика*;
- *Принцип конфигурации*;

- *Использование портов*;
- *Настройка простого прокси-сервера*;
- *Настройка балансировки нагрузки*.

3.1.1.1 Общая информация

Конфигурацию балансировщика нагрузки можно просмотреть и отредактировать в веб-интерфейсе Angie ADC (`Управление трафиком` → `Балансировщик нагрузки`).

В левой части экрана отображается список файлов конфигурации, к которым есть *доступ* пользователя. В правой части экрана отображается конфигурация каждого файла. Поддерживаются *текстовый* и *визуальный* конфигураторы, между ними можно переключаться.

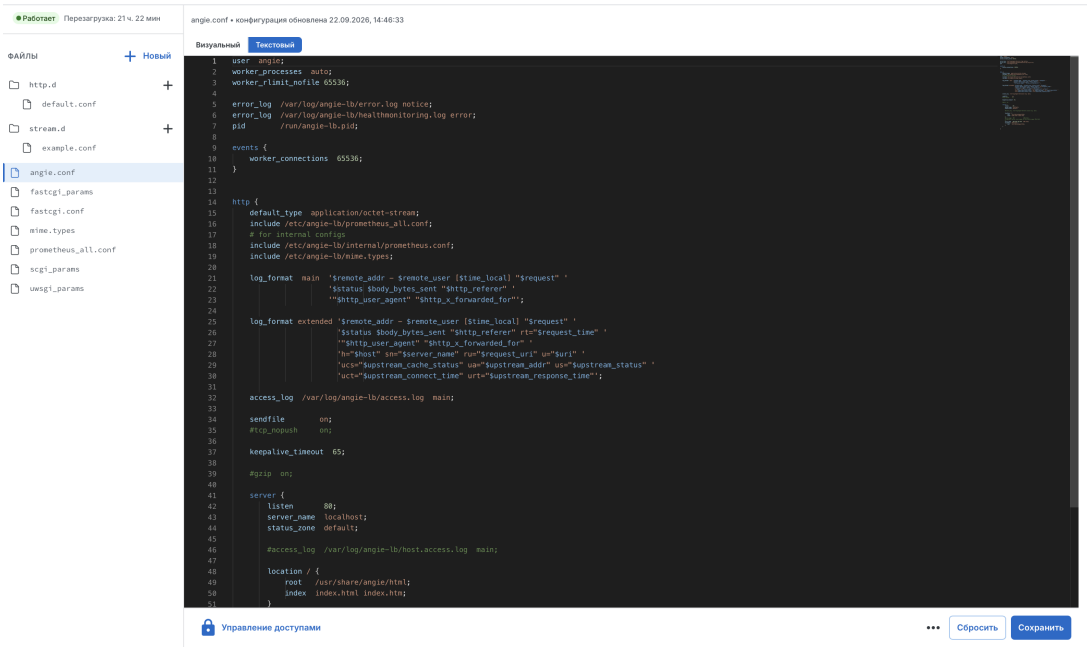
По умолчанию конфигурация балансировщика содержит следующие файлы и папки:

- папка `http.d` — содержит конфигурации веб-сайтов и веб-приложений, работающих по протоколам HTTP/HTTPS:
  - файл `default.conf` — пример настройки виртуального хоста; этот файл не используется.
- папка `stream.d` — настройки проксирования трафика на уровне транспортного протокола (TCP и UDP):
  - файл `example.conf` — пример настройки потокового (TCP/UDP) проксирования; этот файл не используется.
- файл `angie.conf` — главный конфигурационный файл веб-сервера; запускает процессы, определяет пути к логам и подключает все остальные папки и файлы;
- файл `fastcgi.conf` — настройки для работы с PHP (через PHP-FPM) и другими FastCGI-приложениями;
- файл `fastcgi_params` — аналог fastcgi.conf, содержащий базовые переменные окружения для FastCGI;
- файл `mime.types` — карта соответствия расширений файлов и их типов данных (например .html → text/html, .jpg → image/jpeg);
- файл `prometheus_all.conf` — файл настройки экспорта метрик в формате Prometheus для мониторинга (например, в Grafana);
- файл `scgi_params` — параметры для работы по протоколу SCGI;
- файл `uwsgi_params` — параметры для интеграции с приложениями на Python.

Администратор может добавлять новые файлы в папки `http.d` и `stream.d`, нажав на значок добавления напротив соответствующей папки, и удалять любые существующие файлы, нажав на три точки в нижней части экрана соответствующего файла и выбрав пункт `Удалить файл`.

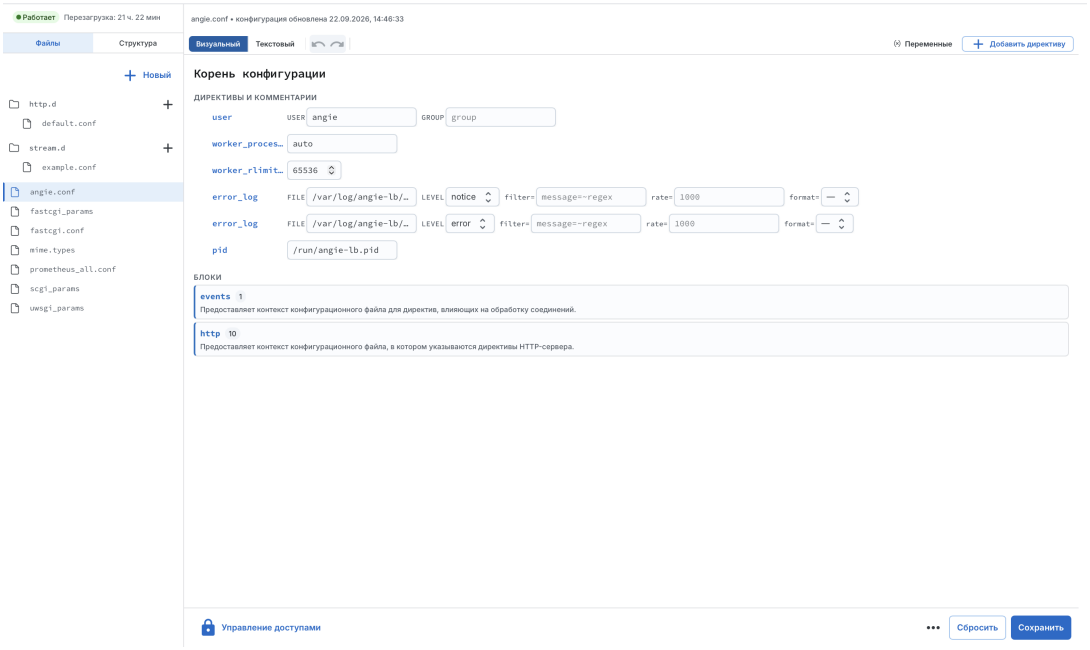
При сохранении изменений конфигурация обновляется и применяется сразу. Если при сохранении файла возникает конфликт (другой пользователь уже внес изменения в файл), то система подсвечивает те места, где правки конфликтуют, и предлагает выбрать, какую версию файла сохранить: пользовательскую (`Сохранить мою версию`) или серверную (`Принять серверную версию`).

3.1.1.2 Текстовый конфигуратор



В текстовом конфигураторе конфигурация редактируется как обычный текст: директивы Angie вводятся и изменяются вручную. Содержимое выбранного файла отображается с подсветкой синтаксиса и нумерацией строк.

3.1.1.3 Визуальный конфигуратор



Визуальный конфигуратор позволяет задать конфигурацию, выбирая директивы и параметры из меню, а не вводя их вручную. На основе заданных значений конфигуратор формирует итоговую конфигурацию балансировщика; просмотреть и при необходимости отредактировать ее вручную можно, переключившись в текстовый режим.

3.1.1.4 Перезапуск балансировщика

В верхней части экрана отображается статус балансировщика:

- `Работает` — балансировщик запущен;
- `Не работает` — балансировщик не запустился после перезагрузки конфигурации.

Также отображается время, прошедшее с последней перезагрузки (`Перезагрузка`) и количество перезагрузок при наведении на время (`Поколение`).

> **Совет**
>
> Если у балансировщика отображается статус `Не работает`, необходимо проверить журнал ошибок балансировщика (см. ниже) и устранить ошибки.
>
> Также можно попробовать перезапустить балансировщик вручную. Для этого откройте любой файл конфигурации балансировщика и сохраните его без внесения изменений.

3.1.1.5 Логи балансировщика

В веб-интерфейсе можно просмотреть журнал ошибок балансировщика нагрузки. Для этого перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки` и в нижней части экрана щелкните многоточие (`...`) и выберите `Логи`.

Также см. *Журналы событий и экспорт* и *diagnostics*.

3.1.1.6 Принцип конфигурации

Для настройки балансировщика нагрузки используется декларативная конфигурация. Балансировщик нагрузки состоит из модулей, которые настраиваются директивами, заданными в конфигурации. Директивы могут быть простыми и блочными. Простая директива состоит из имени и параметров, разделенных пробелами, и оканчивается точкой с запятой `;`. В блочной директиве вместо точки с запятой после имени и параметров следует набор дополнительных инструкций внутри фигурных скобок `{` и `}`. Блочные директивы называются контекстами.

Примеры:

- контекст events (общая обработка соединений);
- контекст http (конфигурация HTTP-балансировки);
- контекст stream (конфигурация TCP/UDP-балансировки).

Контексты `events`, `http`, `stream` располагаются в контексте main. Другие директивы, размещенные вне контекстов `events`, `http`, `stream`, считаются также находящимися в контексте `main`.

В контекстах http и stream размещаются:

- блоки `server`, в которых настраивается проксирование трафика;
- блоки `upstream`, в которых настраиваются группы upstream-серверов для балансировки нагрузки.

В конфигурации в веб-интерфейсе Angie ADC уже предустановлены некоторые общие параметры. Вам необходимо дополнить конфигурацию с учетом ваших целей.

Подробнее о конфигурации и обработке соединений см. adc__configfile и adc__processing.

> **Предупреждение**
>
> Строки конфигурации, приведенные ниже, нельзя удалять или менять (они используются для обеспечения работы соответствующего функционала Angie ADC).
>
> Контекст `main`:

```
error_log  /var/log/angie-lb/healthmonitoring.log error;
pid        /run/angie-lb.pid;
```

Контекст `http`:

```
include /etc/angie-lb/prometheus_all.conf;
include /etc/angie-lb/internal/prometheus.conf;
```

3.1.1.7 Использование портов

Если вы планируете использовать в конфигурации другие порты помимо 80/443, вы можете открыть их с помощью команды *open* через CLI Angie ADC.

Предупреждение

При настройке конфигурации не занимайте следующие порты (используются внутренними сервисами Angie ADC):

TCP: 22, 199, 2222, 2601, 2602, 2603, 2604, 2605, 2606, 2615, 2616, 2617, 2619, 2623, 3050, 3051, 3053, 3054, 3060, 3111, 3122, 3123, 3301, 3302, 3380, 3391, 4460, 5044, 5355, 5432, 8010, 8080, 8443, 9090, 9100, 9120, 9600, 9633, 9898, 9900, 60080

- Порты 8080 и 8443 можно использовать, если у вас выделен отдельный *интерфейс управления*.

UDP: 53, 123, 161, 323, 546, 3784, 3785, 4784, 5355, 7784

3.1.1.8 Настройка простого прокси-сервера

Angie ADC можно использовать в качестве прокси-сервера, который принимает запросы, перенаправляет их на проксируемые серверы, получает от них ответы и отправляет их клиенту.

В примере ниже настраивается базовый прокси-сервер, который будет обслуживать запросы изображений из локального каталога и отправлять все остальные запросы на проксируемый сервер.

1. Создайте сервер, который будет использоваться в качестве бэкенда для прокси (проксируемый сервер), добавив блок `server` в контекст `http`:

   ```
   server {
       listen 8081;
       root /static/www;

       location / {
       }
   }
   ```

   Здесь сервер слушает на порту `8081` и сопоставляет URI запросов с файлами в каталоге `/static/www` (как настроить загрузку и раздачу статических файлов, см. *Загрузка и раздача статических файлов*). Директива root находится в контексте `server` и будет использоваться, если директива location, выбранная для выполнения запроса, не содержит собственной директивы `root`.

   Примечание

   В общем случае конфигурационный файл может содержать несколько блоков `server`, отличающихся портами, на которых они слушают (listen), и именами сервера (server_name). Определив, какой `server` будет обрабатывать запрос, Angie ADC сравнивает URI запроса с параметрами location, заданными в блоке `server`, и принимает решение.

2. Добавьте конфигурацию прокси-сервера:

```
server {
    listen 80;
    location / {
        proxy_pass http://localhost:8081/;
    }

    location ~ \.(gif|jpg|png)$ {
        root /static/images;
    }
}
```

В первом блоке `location` добавлена директива adc__proxy_pass с указанием протокола, имени и порта проксируемого сервера. Во втором блоке `location` задано регулярное выражение для всех URI, оканчивающихся на `.gif`, `.jpg` или `.png`. Соответствующие запросы будут обслуживаться из каталога `/static/images`.

> **Примечание**
>
> При выборе блока `location`, который будет обслуживать запрос, сначала проверяются директивы `location`, задающие префиксы, и запоминается `location` с самым длинным подходящим префиксом. Затем проверяются блоки `location`, заданные регулярными выражениями, в порядке их объявления в конфигурации и используется первое совпадение. Иначе берется `location`, сохраненный до этого.

3. Сохраните изменения в конфигурации, нажав на кнопку `Сохранить`.

Получившийся прокси-сервер будет обслуживать запросы к файлам `.gif`, `.jpg` или `.png` из каталога `/static/images`, а все остальные запросы будет проксировать на сервер `localhost:8081`.

3.1.1.9 Настройка балансировки нагрузки

Чтобы настроить балансировку нагрузки для HTTP-трафика, добавьте блок upstream в контекст `http` и укажите в нем бэкенд-серверы, которые будут использоваться для балансировки нагрузки. Затем настройте проксирование запросов на эту группу серверов в блоке `server` с помощью директивы location.

Пример:

```
upstream backend {
    zone backend 1m;
    server backend1.example.com;
    server backend2.example.com;
}

server {
    listen 80;
    server_name localhost;

    location /api {
        proxy_pass http://backend;
    }
}
```

В приведенном примере задана группа серверов `backend`. Все запросы на порт `80` с URI, начинающимися с `/api`, проксируются в эту группу. Метод балансировки нагрузки не указан явно, поэтому по умолчанию используется метод `round-robin` (запросы распределяются по серверам последовательно).

3.1.2 Управление резервными конфигурациями

В Angie ADC реализовано хранение всех версий конфигурационных файлов балансировщика нагрузки. При сохранении изменений в любом файле конфигурации балансировщика Angie ADC автоматически применяет новую конфигурацию и сохраняет предыдущую версию в репозитории. Можно просмотреть список сохраненных версий конфигурации и применить нужную версию. Также поддерживается *выбор внутреннего или внешнего репозитория* для хранения конфигураций.

3.1.2.1 Просмотр списка сохраненных конфигураций

Чтобы просмотреть список сохраненных конфигураций:

1. Откройте веб-интерфейс Angie ADC.
2. Выберите `Управление трафиком` → `Балансировщик нагрузки`.
3. В нижней части экрана щелкните многоточие (`...`) и выберите `История`.

Откроется таблица со списком сохраненных конфигураций. Для каждой конфигурации указано время ее создания, версия Angie ADC, статус (рабочая или нерабочая конфигурация), пользовательский комментарий, теги (`angie-lb` и UUID) и дата последнего изменения.

3.1.2.2 Изменение рабочего статуса хранимой конфигурации

Чтобы пометить конфигурацию как рабочую или нерабочую:

1. Откройте веб-интерфейс Angie ADC.
2. Выберите `Управление трафиком` → `Балансировщик нагрузки`.
3. В нижней части экрана щелкните многоточие (`...`) и выберите `История`.

   Откроется таблица со списком сохраненных конфигураций.
4. Щелкните многоточие (`...`) напротив конфигурации, статус которой вы хотите изменить, и нажмите `Пометить как нерабочую` или `Пометить как рабочую`.
5. Если вы устанавливаете нерабочий статус, укажите причину поломки и нажмите `Сохранить`.

   Статус конфигурации будет изменен.

3.1.2.3 Восстановление последней рабочей версии конфигурации

Чтобы применить последнюю рабочую версию конфигурации:

1. Откройте веб-интерфейс Angie ADC.
2. Выберите `Управление трафиком` → `Балансировщик нагрузки`.
3. В нижней части экрана щелкните многоточие (`...`) и выберите `Применить последнюю рабочую версию`.

   Будет применена последняя рабочая конфигурация.

3.1.2.4 Восстановление конфигурации из резервной копии

Чтобы применить произвольную конфигурацию из резервной копии:

1. Откройте веб-интерфейс Angie ADC.
2. Выберите `Управление трафиком` → `Балансировщик нагрузки`.
3. В нижней части экрана щелкните многоточие (`...`) и выберите `История`.

   Откроется таблица со списком сохраненных конфигураций.
4. Щелкните многоточие (`...`) напротив конфигурации, которую вы хотите использовать, и нажмите кнопку `Применить`.

   Конфигурация будет применена сразу.

3.1.2.5 Выбор репозитория для хранения конфигураций

В Angie ADC поддерживается два типа репозитория для хранения *резервных копий конфигурации балансировщика нагрузки*, локальный (`filesystem`) и внешний (S3). Для надежного хранения данных рекомендуется использовать внешний репозиторий. Резервная копия в любом репозитории обновляется автоматически при внесении изменений и сохранении новой конфигурации балансировщика нагрузки.

Локальный репозиторий `filesystem` подключен по умолчанию. При использовании локального репозитория резервные копии хранятся в файловой системе внутри Angie ADC.

> **Примечание**
>
> При подключении нового репозитория (локального или внешнего) резервная копия в локальном репозитории автоматически удаляется.

Внешний репозиторий подключается по протоколу S3. Мы рекомендуем использовать внешний S3-совместимый репозиторий для хранения резервных копий конфигурации. В отличие от локального репозитория, при отключении внешнего репозитория резервные копии в нем сохраняются.

Просмотр информации о текущем репозитории:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки` → многоточие (`...`) → `История` → `Управление резервным копированием`.

   Откроется страница с информацией о текущем репозитории.

Подключение локального репозитория:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки` → многоточие (`...`) → `История` → `Управление резервным копированием`.

   Откроется страница с информацией о текущем репозитории.

2. Перейдите на вкладку `Filesystem`.
3. Нажмите `Подключить`.

Будет подключен локальный репозиторий и создана резервная копия конфигурации балансировщика.

> **Примечание**
>
> Если у вас до этого уже была сохранена резервная копия в `filesystem`, она будет удалена.

Подключение внешнего репозитория (S3):

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки` → многоточие (`...`) → `История` → `Управление резервным копированием`.

   Откроется страница с информацией о текущем репозитории.

2. Перейдите на вкладку `S3`.
3. Заполните поля для подключения репозитория:

   - `Конечная точка`
   - `Имя корзины`
   - `Домен маршрутизации` — *домен маршрутизации*, через который доступен S3-репозиторий. Значение `По умолчанию` означает, что используется общая сеть.

- `Ключ доступа`
- `Секретный токен`

4. Нажмите `Подключить`.

   Если вы подключаете репозиторий, в котором уже была резервная копия конфигурации, то будет использована эта копия. Если подключается новый репозиторий, будет создана резервная копия текущей конфигурации балансировщика.

> **Примечание**
>
> Если у вас до этого уже была сохранена резервная копия в `filesystem`, она будет удалена.

3.1.3 Методы балансировки

> **Примечание**
>
> Для каждой upstream-группы можно задать только один метод балансировки.

Каждый метод поддерживает свой набор параметров директивы `server`; какие из них допустимы, показано в таблице. Если указать параметр, который метод не поддерживает, конфигурация не будет загружена, а в журнал будет записана ошибка `balancing method does not support parameter`.

Алго-ритм	Описание	HTT	TCP, `weight`	`slow_s`	`backup`
`round-rc`	Запросы распределяются по серверам последовательно (используется по умолчанию).				
`hash`	Задает метод балансировки нагрузки для группы, при котором соответствие клиента серверу определяется при помощи хэшированного значения ключа. Подробнее см. TCP/UDP, HTTP.				
`ip_hash`	Сервер выбирается с помощью хэш-функции на основе IP-адреса клиента, что обеспечивает "липкость сессии". Частный случай `hash`. В качестве ключа для хэширования используются первые три октета IPv4-адреса клиента или IPv6-адрес клиента целиком. В итоге запрос конкретного клиента всегда попадает на один и тот же сервер, если он работоспособен. Подробнее см. HTTP.				
`least_cc`	Новый запрос направляется на сервер с минимальным количеством активных соединений (наименее загруженный). Подробнее см. TCP/UDP, HTTP.				
`random`	Запросы распределяются по серверам случайным образом. При большом числе запросов они будут распределяться по upstream-серверам равномерно, что хорошо подходит, например, для кластера балансировщиков. Поддерживается опциональный параметр `two` (выбор из двух случайных серверов по `least_conn`). Подробнее см. TCP/UDP, HTTP.				
`least_ti`	Балансировка нагрузки на основе наименьшего времени ответа. Запросы распределяются на те серверы, которые обрабатывают их быстрее. Уменьшает время ожидания для пользователей. Если серверы имеют разное оборудование или настройки, помогает уравновесить нагрузку. Подробнее см. TCP/UDP, HTTP.				
`feedback`	Балансировка нагрузки по обратной связи (по произвольному параметру из ответа на основной или проверочный запрос). Подробнее см. TCP/UDP, HTTP.				
`least_ba`	Балансировка на основе наименьшего потребления полосы пропускания. Режимы: upstream, downstream, both. Подробнее см. TCP/UDP, HTTP.				
`least_pa`	Балансировка на основе наименьшего числа пакетов в единицу времени. Может использоваться в случаях, когда оборудование, расположенное за балансировщиком, не способно "переварить" слишком большой поток пакетов. Режимы: upstream, downstream, both. Подробнее см. TCP/UDP.				

3.1.3.1 Примеры HTTP-балансировки нагрузки

Базовая настройка

Самая простая конфигурация для балансировки нагрузки с помощью Angie ADC может выглядеть следующим образом:

```
http {
```

```
    upstream myapp1 {

        server srv1.example.com;
        server srv2.example.com;
        server srv3.example.com;
    }
    server {

        listen 80;
        location / {

            proxy_pass http://myapp1;
        }
    }
}
```

В приведенном примере:

- Группа серверов `myapp1` содержит три сервера `srv1`, `srv2` и `srv3`.
- На этих серверах работают три экземпляра одного и того же приложения.
- Используется метод балансировки `round-robin` (по умолчанию).
- Все запросы на порт `80` перенаправляются через группу серверов `myapp1`.

least_conn

Балансировка нагрузки по наименее загруженному серверу.

Модуль балансировки нагрузки `least_conn` в модуле HTTP позволяет распределять нагрузку более равномерно, направляя новые запросы на серверы с наименьшим количеством активных соединений. Этот метод рекомендуется, если время обработки запросов может сильно варьироваться.

Пример конфигурации:

```
http {

    upstream backend {

        least_conn;

        server backend1.example.com;
        server backend2.example.com;
        server backend3.example.com;
    }

    server {

        listen 80;
        location / {

            proxy_pass http://backend;
        }
    }
}
```

В этом примере:

- Директива `least_conn` включает метод балансировки нагрузки по наименьшему числу соединений.

- Для балансировки нагрузки определены три проксируемых сервера.
- Входящие запросы к серверу проксируются в группу `backend`.

Преимущества метода:

- Динамическая балансировка: непрерывно отслеживает количество активных соединений для адаптации к текущей нагрузке на каждом сервере.
- Простота: работает без необходимости дополнительных параметров или сложных настроек.
- Совместимость: совместим с другими конфигурациями проксируемых серверов, включая веса, максимальное количество сбоев и время ожидания после сбоя.

ip_hash

Балансировка нагрузки с сохранением сессий.

Методы `round-robin` и `least_conn` не гарантируют, что запросы от одного клиента будут обрабатываться одним и тем же сервером. Если важно, чтобы клиент всегда направлялся на один сервер (например, при использовании сессионных данных), можно использовать метод `ip_hash`.

Пример конфигурации:

```
upstream myapp1 {

    ip_hash;
    server srv1.example.com;
    server srv2.example.com;
    server srv3.example.com;
}
```

Метод `ip_hash` гарантирует, что запросы от одного клиента будут попадать на один сервер, если этот сервер доступен.

weight

Взвешенная балансировка нагрузки.

С помощью директивы `weight` можно указать, какой сервер должен обрабатывать больше запросов. Этот способ рекомендуется, если серверы имеют разную производительность. По умолчанию вес сервера равен `1`.

Пример:

```
upstream myapp1 {

    server srv1.example.com weight=3;
    server srv2.example.com;
    server srv3.example.com;
}
```

В этой конфигурации каждые пять запросов будут распределены следующим образом: три запроса попадут на `srv1`, один запрос — на `srv2` и еще один — на `srv3`.

Метод `weight` может использоваться в комбинации с методами `round-robin` и `least_conn`.

least_time

Балансировка нагрузки на основе наименьшего времени ответа.

Модуль балансировки нагрузки `least_time` задает для группы метод балансировки нагрузки, при котором вероятность передачи соединения активному серверу обратно пропорциональна среднему времени его ответа; чем оно меньше, тем больше соединений будет получать сервер.

Когда использовать `least_time`?

- Переменная нагрузка: запросы распределяются на серверы, которые обрабатывают их быстрее.
- Высокая доступность: уменьшается время ожидания для пользователей.
- Гетерогенные серверы: если серверы имеют разное оборудование или настройки, `least_time` помогает уравновесить нагрузку.

Пример конфигурации:

```
http {

    upstream backend {

        least_time header;
        server backend1.example.com;
        server backend2.example.com;
        server backend3.example.com;
    }
    server {

        listen 80;
        location / {

            proxy_pass http://backend;
        }
    }
}
```

В этом примере `least_time header`: балансировка основана на времени отклика до получения заголовка ответа от сервера.

feedback

Балансировка по произвольному параметру из ответа на основной или проверочный запрос.

Модуль балансировки нагрузки `feedback` задает в `upstream` механизм балансировки нагрузки по обратной связи. Он динамически корректирует решения при балансировке, умножая вес каждого проксируемого сервера на среднее значение обратной связи, которое меняется с течением времени в зависимости от значения переменной и подчиняется необязательному условию. По умолчанию параметр `factor` равен 90.

Пример конфигурации:

```
upstream backend {

    zone backend 1m;

    feedback $feedback_value factor=80 account=$condition_value;

    server backend1.example.com;
    server backend2.example.com;
}

map $upstream_http_custom_score $feedback_value {

    "high" 100;
    "medium" 75;
    "low" 50;
    default 10;
}
```

```
map $upstream_probe $condition_value {

    "high_priority" "1";
    "low_priority" "0";
    default "1";
}
```

Эта конфигурация категоризирует ответы серверов по уровням обратной связи на основе определенных оценок из полей заголовков ответа, а также добавляет условие на `$upstream_probe`, чтобы учитывать только ответы от активной проверки `high_priority` или ответы на обычные клиентские запросы.

3.1.3.2 Примеры TCP/UDP-балансировки нагрузки

Конфигурация для TCP

```
stream {

    upstream tcp_backend {

        server 192.168.1.10:3306 weight=2;
        server 192.168.1.11:3306;
        server 192.168.1.12:3306;
    }

    server {

        listen 3306;
        proxy_pass tcp_backend;
        proxy_timeout 10s;
        proxy_connect_timeout 5s;
    }
}
```

В этой конфигурации задана группа серверов, участвующих в балансировке (`tcp_backend`). Настроен вес для серверов, чтобы более мощный сервер получал больше запросов (`weight=2`). Сервер слушает входящие соединения на порту `3306` (используется для MySQL). Трафик перенаправляется к группе серверов `tcp_backend`. Настроены тайм-ауты:

- максимальное время ожидания ответа от сервера `10s`;
- максимальное время для установления соединения с сервером `5s`.

Конфигурация для UDP

Для приложений, работающих через протокол UDP, конфигурация аналогична TCP, но с настройками для UDP-трафика.

```
stream {

    upstream udp_backend {

        server 192.168.1.20:53;
        server 192.168.1.21:53;

    }
    server {
```

```
        listen 53 udp;
        proxy_pass udp_backend;

        proxy_responses 1;
        proxy_timeout 10s;
    }
}
```

least_bandwidth

Балансировка на основе наименьшего потребления полосы пропускания.

Алгоритм периодически вычисляет среднее использование полосы пропускания для каждого апстрим-сервера, используя формулу скользящего среднего для сглаживания колебаний со временем. Когда начинается новая сессия, модуль балансировки нагрузки `least_bandwidth` выбирает проксируемый сервер с наименьшим средним использованием пропускной способности, скорректированным с учетом веса сервера, если он указан. Этот механизм гарантирует, что сессии направляются на серверы, которые в настоящее время используют меньше пропускной способности, что способствует равномерному распределению сетевой нагрузки.

Пример конфигурации:

```
stream {

    upstream backend {

        least_bandwidth both factor=80;
        server backend1.example.com:12345;
        server backend2.example.com:12345;
    }
    server {

        listen 12345;
        proxy_pass backend;
    }
}
```

В этом примере:

- В директиве `least_bandwidth` настроен учет как входящей, так и исходящей пропускной способности.
- Коэффициент сглаживания установлен равным 80, что влияет на скорость адаптации среднего значения к изменениям в использовании пропускной способности.
- Для балансировки нагрузки определены два проксируемых сервера.

Преимущества метода:

- Динамическая балансировка: непрерывно отслеживает использование пропускной способности для адаптации к текущей нагрузке на каждом сервере.
- Коэффициент сглаживания `factor` контролирует отзывчивость расчета скользящего среднего; более высокий коэффициент означает более медленную адаптацию к изменениям.
- Режимы: позволяет выбирать балансировку на основе входящей пропускной способности, исходящей пропускной способности или обоих вариантов, в зависимости от потребностей приложения.
- Совместим с другими конфигурациями проксируемых серверов, включая веса, максимальное количество сбоев и время ожидания после сбоя.

least_packets

Балансировка на основе наименьшего числа пакетов в единицу времени.

Средняя скорость пакетов для каждого проксируемого сервера периодически проверяется с использованием формулы скользящего среднего для сглаживания колебаний со временем. Когда инициируется новый сеанс, модуль балансировки нагрузки `least_packets` в потоковом модуле выбирает проксируемый сервер с наименьшей средней скоростью передачи пакетов, скорректированной с учетом веса сервера. Этот процесс гарантирует, что сеансы направляются на серверы, которые в настоящее время наименее загружены с точки зрения обработки пакетов, что способствует равномерному распределению сетевой нагрузки.

Пример конфигурации:

```
stream {

    upstream backend {

        least_packets both factor=80;
        server backend1.example.com:12345;
        server backend2.example.com:12345;
    }
    server {

        listen 12345;
        proxy_pass backend;
    }
}
```

В этом примере:

- В директиве `least_packets` настроен учет как входящих, так и исходящих пакетов.
- Коэффициент сглаживания установлен равным 80, что влияет на то, как быстро среднее значение адаптируется к изменениям скорости пакетов.
- Определены два проксируемых сервера для балансировки нагрузки.

Преимущества метода:

- Динамическая балансировка: непрерывно отслеживает скорость пакетов для адаптации к текущей нагрузке на каждом сервере.
- Параметр `factor` контролирует отзывчивость расчета скользящего среднего; более высокий коэффициент означает более медленную адаптацию к изменениям.
- Режимы: позволяет выбирать балансировку на основе числа входящих пакетов, исходящих пакетов или обоих значений.
- Совместим с другими конфигурациями проксируемых серверов, включая веса, максимальное количество сбоев и время ожидания после сбоя.

hash

Контекстное хэширование.

Поддерживается метод `hash` (например, по IP или произвольному значению). Если сервер из пула станет недоступным или будет добавлен новый сервер, минимальное количество клиентов перенаправится на другие серверы. Используется для "липких сессий", когда важно, чтобы запросы от одного клиента всегда обрабатывались одним и тем же сервером.

Пример:

```
upstream tcp_backend {
```

```
    hash $remote_addr consistent;
    server 192.168.1.10:3306;
    server 192.168.1.11:3306;
}
```

Ограничение IP

Для защиты можно использовать ограничения IP через `allow` и `deny`.

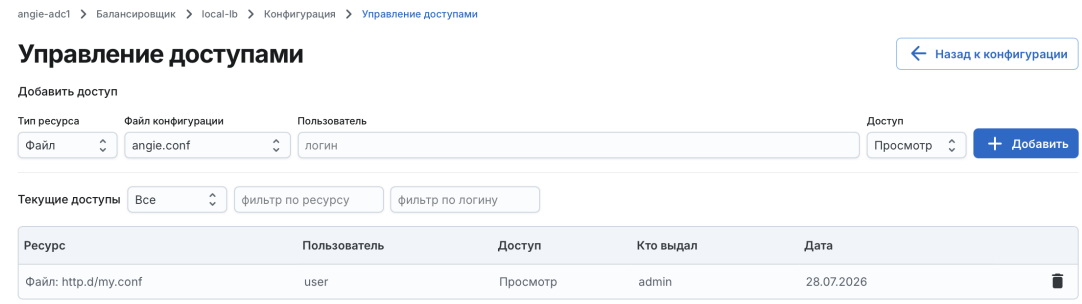
Пример:

```
server {

    listen 3306;
    allow 192.168.1.0/24;
    deny all;
    proxy_pass tcp_backend;
}
```

В этом примере разрешена только локальная сеть, остальным доступ запрещен.

3.1.4 Предоставление доступов на работу с конфигурацией



Всем пользователям Angie ADC (локальным и внешним) назначаются роли в системе, определяющие их доступ к конфигурации балансировщика нагрузки.

- **Администратор** обладает полными правами на все действия в системе, включая редактирование всех файлов конфигурации балансировщика нагрузки Angie ADC.
- **Супервизор** имеет ограниченные права: может только просматривать информацию в системе, например проводить аудит, в том числе может просматривать все файлы конфигурации балансировщика нагрузки.
- **Оператор** имеет ограниченные права: может редактировать файлы конфигурации балансировщика, к которым ему предоставлен доступ, и просматривать статистику зон, к которым ему предоставлен доступ. Доступы предоставляет администратор.

3.1.4.1 Предоставление прав на просмотр и редактирование

Чтобы *оператор мог настраивать балансировку для сервера*, ему необходимо разрешить редактирование файла конфигурации, в котором описан этот сервер. Права на просмотр и редактирование файлов предоставляет администратор через веб-интерфейс Angie ADC.

Примечание

Рекомендуется давать операторам доступ только к файлам в папках `http.d` и `stream.d`.

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки` → `Управление доступами`.
2. В открывшемся окне заполните поля формы для добавления нового доступа:
   - Чтобы предоставить доступ к файлу, выберите тип ресурса `Файл` и в выпадающем списке `Файл конфигурации` выберите нужный файл. Затем в поле `Доступ` укажите уровень доступа: `Просмотр` или `Редактирование`.
   - Чтобы предоставить доступ к зоне, выберите тип ресурса `Зона` и введите имя зоны в поле `Зона`. Для типа ресурса `Зона` всегда выдается доступ на редактирование.

   Примечание

   Зону предварительно необходимо настроить.
3. В поле `Пользователь` укажите логин пользователя, для которого настраивается доступ.
4. Нажмите `Добавить`.

Доступ будет добавлен и отобразится в таблице доступов.

3.1.4.2 Просмотр выданных доступов

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки` → `Управление доступами`.
2. В открывшемся окне в таблице `Текущие доступы` отобразится список выданных доступов.

   Для удобства поиска поддерживается фильтрация.

3.1.4.3 Редактирование выданных доступов

Редактирование записей не поддерживается.

Чтобы изменить запись, необходимо удалить старую запись и добавить новую с измененными параметрами.

3.1.4.4 Удаление выданных доступов

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки` → `Управление доступами`.
2. В открывшемся окне в таблице `Текущие доступы` отобразится список выданных доступов.
3. Нажмите на значок удаления напротив нужной записи.

Доступ будет удален.

3.1.5 Проверки работоспособности серверов

Angie ADC включает пассивные и активные проверки работоспособности серверов (health probes). Если сервер начинает отвечать с ошибками, Angie ADC временно исключает его из пула доступных серверов.

3.1.5.1 Пассивные проверки

Пассивные проверки работают автоматически на основе реальных клиентских запросов.

Пример:

```
upstream myapp1 {

   server srv1.example.com max_fails=2 fail_timeout=10s;
   server srv2.example.com;
   server srv3.example.com;
}
```

В этой конфигурации сервер помечается как недоступный после двух неудачных запросов подряд (`max_fails=2`). Через десять секунд сервер снова проверяется на доступность (`fail_timeout=10s`). Если он восстановился, запросы снова начинают отправляться на этот сервер.

3.1.5.2 Активные проверки

Активные проверки позволяют оценить доступность сервера без участия клиентов. Поддерживаются активные проверки для HTTP и TCP/UDP. Проверки задаются с помощью директивы `upstream_probe`. Для одного апстрима можно определить несколько проверок. Можно гибко настраивать поведение проверок. Поддерживается отправка ICMP echo-запросов (ping). Подробнее см. справочные материалы по активным проверкам HTTP и stream.

Пример для HTTP

```
upstream backend {
    zone backend 1m;

    server backend1.example.com;
    server backend2.example.com;
}

map $upstream_status $good {
    200     "1";
}

server {
    listen ...;

    location /backend {
        ...
        proxy_pass http://backend;

        upstream_probe backend_probe
            uri=/probe
            port=10004
            interval=5s
            test=$good
            essential
            persistent
            fails=3
            passes=3
            max_body=10m
            mode=idle;
    }
}
```

Детали работы:

- Изначально сервер не получает клиентские запросы, пока не пройдет *все* заданные для него проверки с параметром `essential` (пропуская помеченные как `persistent`, если конфигурация перезагружена и до этого сервер считался работающим). Если таких проверок нет, сервер

считается работающим.

- Сервер считается неработающим и не получает клиентские запросы, если *какая-либо* заданная для него проверка достигает своего порога `fails` или сам сервер достигает порога max_fails.
- Чтобы неработающий сервер снова мог считаться работающим, *все* заданные для него проверки должны достичь своего порога `passes`; после этого учитывается порог max_fails.

Пример для TCP/UDP

```
upstream backend {
    zone backend 1m;

    server a.example.com;
    server b.example.com;
}

map $upstream_probe_response $good {
    ~200    "1";
    default  "";
}

server {
    listen ...;

    # ...
    proxy_pass backend;
    upstream_probe_timeout 1s;

    upstream_probe backend_probe
        port=12345
        interval=5s
        test=$good
        essential
        persistent
        fails=3
        passes=3
        max_response=512k
        mode=onfail
        "send=data:GET / HTTP/1.0\r\n\r\n";
}
```

Примечание

Согласно спецификации RFC 2616 (HTTP/1.1) и RFC 9110 (HTTP Semantics), заголовки HTTP должны разделяться последовательностью CRLF (`\r\n`), а не просто `\n`.

Детали работы:

- Изначально сервер не получает клиентские запросы, пока не пройдет *все* заданные для него проверки с параметром `essential` (пропуская помеченные как `persistent`, если конфигурация перезагружена и до этого сервер считался работающим). Если таких проверок нет, сервер считается работающим.
- Сервер считается неработающим и не получает клиентские запросы, если *какая-либо* заданная для него проверка достигает своего порога `fails` или сам сервер достигает порога max_fails.
- Чтобы неработающий сервер снова мог считаться работающим, *все* заданные для него проверки должны достичь своего порога `passes`; после этого учитывается порог max_fails.

- Параметр `send` — отправляемые для проверки данные, а переменная `$upstream_probe_response` — ответ бэкенда.

Пример ICMP echo-запроса для HTTP

```
http {
    upstream u {
        zone z 1k;

        server 127.0.0.1:8081;
        server 127.0.0.1:8082;
    }

    server {
        listen ...;

        location / {
            proxy_pass http://u/;

            upstream_probe simple1
                 interval=3s
                 ping;

            upstream_probe simple2
                 interval=3s
                 ping ping_timeout=3s;
        }
    }
}
```

Детали работы:

- Используется проверка методом ICMP Echo вместо HTTP-запроса.
- ICMP-проверка проверяет доступность IP-адреса `127.0.0.1`. Порты `upstream` игнорируются.
- Сервер считается неработающим и не получает клиентские запросы, если не отвечает на запрос ICMP Echo в течение заданного таймаута. Первая проверка использует таймаут ожидания по умолчанию (1 секунда). Вторая проверка задает таймаут ожидания ответа явно (3 секунды).
- Единственным критерием прохождения проверки является успешное получение ICMP-ответа в пределах таймаута.

3.1.6 Резервирование проксируемых серверов и групп

Для повышения отказоустойчивости системы вы можете дополнительно резервировать проксируемые серверы, чтобы они включались в работу при выходе основных серверов из строя.

В Angie ADC доступно два механизма резервирования:

- *Запасные серверы* (spare-серверы).

  Запасные серверы (spare-серверы) включаются в работу при выходе из строя основных серверов в рамках одной группы. Это позволяет плавно подхватывать трафик без переключения на другую группу серверов. Запасные серверы можно использовать для поддержания производительности системы, например при выводе отдельных серверов на техническое обслуживание.

- *Резервные группы серверов* (backup-группы).

  Резервные группы (backup-группы) серверов включаются в работу при отказе всех серверов активной группы и поддерживают отказоустойчивость системы при выходе из строя групп

серверов целиком. С помощью backup-групп можно реализовать многоуровневое резервирование большой инфраструктуры.

Можно использовать оба механизма одновременно для обеспечения максимальной надежности.

Примечание

Отказоустойчивость самого балансировщика нагрузки обеспечивается отдельно, например с помощью *пары высокой доступности*.

3.1.6.1 Запасные серверы (spare-серверы)

При настройке апстрим-групп часть серверов в группе можно выделить как запасные, назначив им параметр spare в блоке `server`. Также можно объявить серверы запасными динамически с помощью API-интерфейса.

Пример:

```
http {

    upstream u {
        zone z 1m;
        server 127.0.0.1:8081 max_fails=1 fail_timeout=2s weight=2;
        server 127.0.0.1:8082 spare;
        server 127.0.0.1:8083 spare;
    }
```

По умолчанию запасные (spare) серверы находятся в режиме ожидания и имеют статус `idle`. В случае выхода из строя одного или нескольких основных серверов группы они включаются в балансировку и переходят в статус `up`. При восстановлении основных серверов замещающие spare-серверы снова переводятся в режим ожидания. При этом поддерживаются sticky-сессии: запасные серверы, выведенные из активного пула, будут по-прежнему использоваться для таких сессий. Если на запасном сервере настроены активные проверки работоспособности, то сервер не будет включаться в работу, пока проверки не будут пройдены. Неработоспособные запасные серверы будут иметь такие же статусы, как неработоспособные основные.

Решение о вводе spare-сервера в балансировку определяется разницей между совокупным весом всех серверов, используемых в группе в качестве основных `main_weight`, и совокупным весом всех активных серверов `active_weight`. Если общий вес активных серверов становится меньше веса всех основных серверов — spare-серверы вводятся в работу, если больше — spare-серверы выводятся в режим ожидания. При этом всегда используется минимально необходимое количество spare-серверов. При введении дополнительного spare-сервера будет выбран сервер с максимальным весом, а при выведении из строя лишних spare-серверов сначала будет выбран сервер с минимальным весом.

В режиме отладки через REST API доступны значения счетчиков `main_weight` и `active_weight`. Для upstream-сервера отображается поле `spare` со значением `idle` (сервер не используется) или `running` (сервер активен). Поле `spare_num` отображает количество серверов, считающихся запасными.

3.1.6.2 Резервные группы серверов (backup-группы)

Резервные группы серверов (backup-группы), в отличие от spare-серверов, представляют собой отдельные группы серверов, выделенные только для резервирования. Upstream-сервер может входить только в одну резервную группу.

Если балансировщик не может найти ни один рабочий сервер в основной группе, то он переходит к серверам backup-группы. Можно добавить одну или несколько backup-групп серверов с разным уровнем резервирования. Тогда балансировщик будет сначала переходить к backup-группе с наименьшим уровнем. Если групп много, можно указать для них произвольные уровни, например для удобства сортировки.

Уровень резервирования backup-группы можно задать с помощью директивы `backup=n`:

- `backup=1` (или просто `backup`) — группа резервных серверов первого уровня (в API отображается как `true`);
- `backup=2` — группа резервных серверов второго уровня (в API отображается как соответствующее число);
- `backup=3` — группа резервных серверов третьего уровня.

Пример:

```
upstream my_backend {
    server primary1.example.com;
    server primary2.example.com;

    server backend.example.com service=http resolve backup=prio;

    server backup1a.example.com backup;
    server backup1b.example.com backup;

    server backup2a.example.com backup=2;
    server backup2b.example.com backup=2;

    backup_switch permanent=2m;
}
```

Если upstream-сервер настраивался с помощью SRV-записи, то уровень backup-группы можно определить динамически через поле приоритета (`priority`). Для этого используется:

- Абсолютное значение приоритета (директива `backup=prio`).

  В этом случае значение приоритета `priority=n` из SRV-записи будет использовано в качестве уровня резервной группы `backup=n`.

- Относительное значение приоритета `priority=n` из SRV-записи.

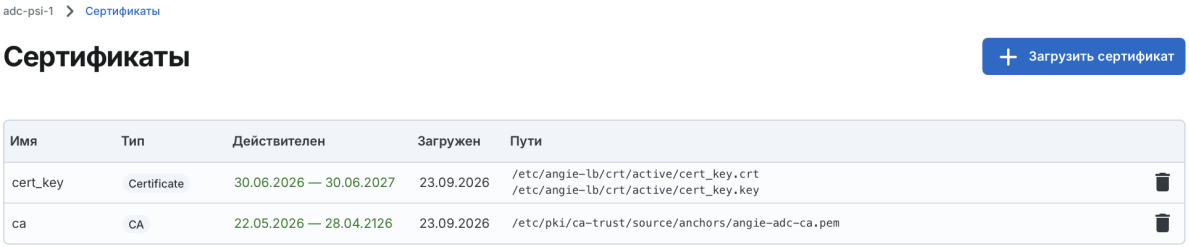
  В этом случае директива `backup=n` задает базовый уровень отсчета (например `backup=3`), а относительные уровни резервирования отсчитываются от этого уровня. Сервер с наименьшим значением `priority` получит уровень `backup=3`, следующий за ним — `backup=4`, и так далее. Если уровень отсчета `backup=n` не задан, отсчет будет идти от нуля: сервер с наименьшим значением `priority` получит `backup=0` и станет основным, за ним — `backup=1`, резервный, и так далее.

По умолчанию балансировщик всегда начинает поиск подходящего сервера с основной группы, даже если в данный момент активна резервная. Чтобы этого избежать, можно использовать директиву `backup_switch permanent`, задав для нее значение, например `permanent=2m`. В этом случае балансировщик нагрузки будет пытаться вернуться на основную группу не чаще, чем раз в две минуты, что позволит избежать избыточных переключений группы.

Если указать параметр `permanent` без значения, то выбранная backup-группа будет сохраняться в качестве активной даже после того, как серверы из основной группы снова станут доступными. В случае отказа текущей backup-группы балансировщик будет переключаться на следующую по уровню backup-группу, и, только дойдя до максимального уровня, вернется на основную группу.

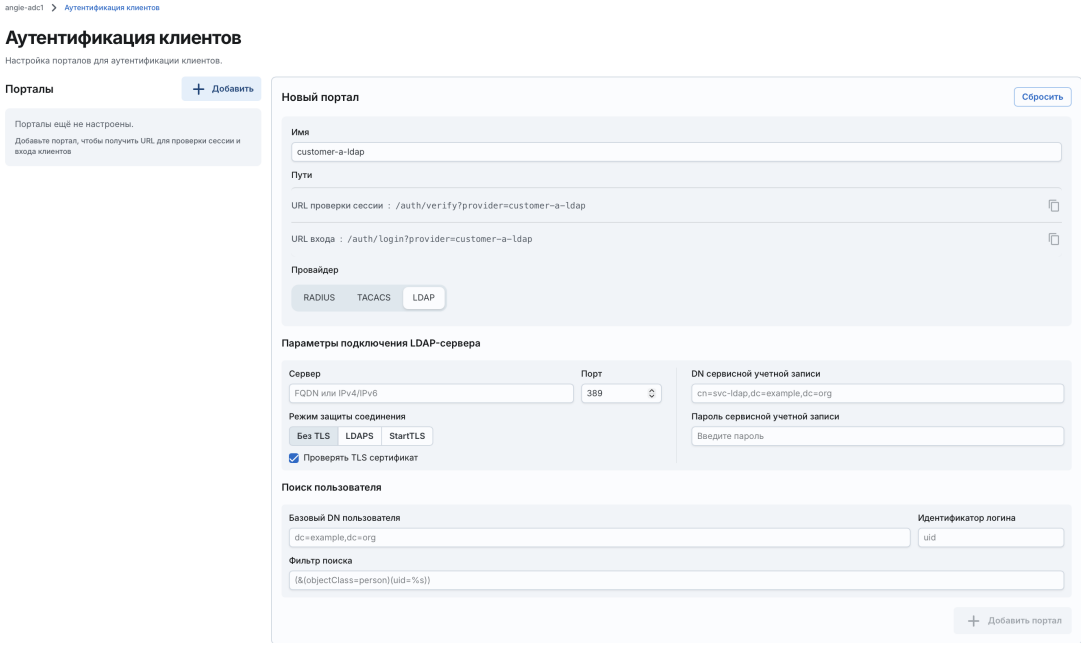
3.1.7 Управление сертификатами

В Angie ADC можно загружать сертификаты для обработки TLS-соединений балансируемого трафика и доверенные корневые и промежуточные сертификаты (`Система` → `Сертификаты`). Набор загруженных сертификатов распространяется на все узлы кластера.

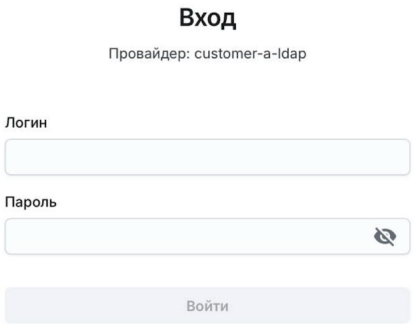


Подробнее см. *Управление сертификатами*.

3.1.8 Аутентификация клиентов



Angie ADC позволяет настроить аутентификацию клиентов при обращении к сервисам через балансировщик нагрузки. При доступе к защищенным ресурсам клиент будет попадать на страницу логина (портал аутентификации):



При успешной аутентификации клиент будет перенаправлен на запрашиваемую страницу. Для аутентификации используется внешний сервер (LDAP, TACACS+ или RADIUS). Настройки аутентификации клиентов распространяются на все узлы *кластера*.

3.1.8.1 Настройка аутентификации клиентов

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Аутентификация клиентов`.
2. В открывшемся окне нажмите `Добавить` и укажите имя нового портала для аутентификации. Имя должно быть уникальным и валидным для использования в URL: нижний регистр, начинается с буквы; допускаются буквы, цифры и дефисы, не допускаются пробелы и специальные символы.

   В блоке `Пути` отобразятся URL проверки сессии и URL входа. Эти пути необходимо в дальнейшем указать в конфигурации балансировщика нагрузки (см. пункт 5).
3. Выберите тип провайдера, LDAP, TACACS+ или RADIUS, и задайте параметры подключения к серверу:
   - Для LDAP:
     - `Сервер`: IP-адрес или доменное имя LDAP-сервера.
     - `Порт`: порт подключения к LDAP-серверу (по умолчанию `389`).
     - `Режим защиты соединения` (по умолчанию `Без TLS`, также доступны варианты `LDAPS` и `StartTLS`).
     - `DN сервисной учетной записи`: логин сервисной учетной записи, от имени которой система подключается к LDAP.
     - `Пароль сервисной учетной записи`: пароль сервисной учетной записи для подключения к LDAP-серверу.
     - `Базовый DN пользователя`: задает ветку на LDAP-сервере, в которой система будет искать пользователя, например `ou=users,dc=example,dc=com`.
     - `Идентификатор логина`: поле в LDAP, которое содержит логин, например `uid`, `sAMAccountName` или `userPrincipalName`.
     - `Фильтр поиска`: LDAP-фильтр для поиска пользователя, например `(&(objectClass=user)(sAMAccountName=%s))`.

     Примечание

     Фильтр LDAP определяет, в каком формате пользователь должен вводить логин при входе в систему:

     - если используется фильтр `(&(objectClass=user)(sAMAccountName=%s))`, то логин будет без доменного имени, например `ivanov`;
     - если используется фильтр `(&(objectClass=user)(userPrincipalName=%s))`, то логин будет полным: `ivanov@domain.com`.
   - Для RADIUS:
     - `Сервер`: IP-адрес или доменное имя RADIUS-сервера.
     - `Порт`: порт подключения к RADIUS-серверу (по умолчанию `1812`).
     - `Протокол`: протокол передачи данных: `UDP` или `TCP` (по умолчанию: `UDP`).
     - `NAS-идентификатор`: идентификатор NAS (Network Access Server), передаваемый серверу RADIUS.
     - `Метод аутентификации`: поддерживается только `PAP`.
     - `Секрет`: общий секрет для шифрования паролей.
   - Для TACACS+:
     - `Сервер`: IP-адрес или доменное имя TACACS-сервера.

- `Порт`: порт подключения к TACACS-серверу (по умолчанию `49`).
- `Секрет`: общий секрет для шифрования паролей.

4. Нажмите `Добавить портал`.
5. Перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки` и укажите пути портала аутентификации для нужного `location`, а также страницу ошибки в случае непрохождения аутентификации.

   Например:

```
include /etc/angie-lb/internal/adc-ui-portal-locations.inc;

location /app/ {
    auth_request /internal-verify;
    error_page 401 = @auth_login;
    proxy_pass http://<backend-address>;
    proxy_set_header Host              $host;
    proxy_set_header X-Forwarded-Proto <http или https>;
}

location = /internal-verify {
    internal;
    proxy_set_header X-Angie-Auth-Request 1;
    proxy_pass http://unix:/run/angie-adc-auth-dataplane/auth-dataplane.sock:/
↪auth/verify?provider=<portal-name>;
}

location @auth_login {
    return 302 /auth/portal/login?provider=<portal-name>&redirect_url=$request_
↪uri;
}
```

3.1.8.2 Изменение параметров портала аутентификации

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Аутентификация клиентов`.
2. В открывшемся окне в списке порталов выберите портал, параметры которого вы хотите изменить.
3. Внесите изменения и нажмите `Сохранить портал`.

Важно

Если портал использовался для аутентификации в конфигурации балансировщика нагрузки, не забудьте отредактировать конфигурацию соответствующим образом.

3.1.8.3 Выбор домена маршрутизации для портала

По умолчанию узел обращается к серверу аутентификации портала (RADIUS, TACACS+ или LDAP) через общую сеть. Для каждого узла можно задать *свой домен маршрутизации*, через который будет происходить обращение.

Примечание

Выбор домена маршрутизации для портала возможен только после создания портала.

Чтобы задать домен маршрутизации для портала:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Аутентификация клиентов`.
2. Выберите портал.
3. В блоке `Размещение AAA по узлам` выберите узел и домен маршрутизации для аутентификации клиентов на этом узле. Значение `По умолчанию` означает общую сеть. Домен с нужным интерфейсом должен быть заранее *добавлен на узле*.
4. Нажмите `Применить`.

3.1.8.4 Удаление портала аутентификации

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Аутентификация клиентов`.
2. В открывшемся окне в списке порталов выберите портал, который вы хотите удалить, и нажмите `Удалить`.

Портал будет удален.

Важно

Если портал использовался для аутентификации в конфигурации балансировщика нагрузки, не забудьте удалить его из конфигурации, иначе пользователи будут по-прежнему перенаправляться на страницу аутентификации, но не смогут ее пройти, т. к. портал удален.

3.1.9 Режим отладки

Режим отладки следует включать перед самостоятельной диагностикой или по рекомендации технической поддержки. Чтобы включить режим отладки, выполните команду `angie debug` *в CLI*. Для отключения режима отладки выполните команду `no angie debug`.

Примечание

Использование режима отладки может снизить производительность, а также увеличить расход места на диске.

3.1.9.1 Отладочный лог

Чтобы включить отладочный лог, задайте в конфигурации уровень `debug` с помощью директивы adc__error_log:

```
error_log /path/to/log debug;
```

Если выключить режим отладки, но оставить уровень `debug` в директиве adc__error_log, Angie ADC будет добавлять записи в лог на уровне `info`.

Если переопределить adc__error_log в конфигурации, но не указать в ней уровень `debug`, отладочный лог будет отключен. Здесь переопределение лога на уровне adc__server отключает отладочный лог для отдельного сервера:

```
error_log /path/to/log debug;

http {
   server {
     error_log /path/to/log;
    # ...
```

Во избежание этого уберите строку, переопределяющую adc__error_log, либо задайте в ней уровень `debug`:

```
error_log /path/to/log debug;

http {
   server {
     error_log /path/to/log debug;
   #  ...
```

3.1.9.2 Расположение директивы

Расположение директивы adc__error_log влияет на полноту собираемой отладочной информации.

Директива, указанная на более низком уровне конфигурации (например, внутри блока `server` или `location`), заменяет настройки логирования, заданные на более высоком уровне (например, на основном уровне конфигурации или внутри блока `http`).

Отключение отладочного лога для конкретного сервера

Если глобально отладочный лог включен, но для отдельного сервера adc__error_log указан без уровня `debug`, то для этого сервера отладочная информация собираться не будет.

```
error_log /var/log/angie-lb/error.log debug; # Глобальный отладочный лог

http {

    server {

        listen 80;
        server_name example.com;

        error_log /var/log/angie-lb/example.com.error.log;
        # Отладочный лог для example.com отключен, в файле - уровень info

        # ...
    }

    server {

        listen 80;
        server_name another.com;

        # Для этого сервера будет использоваться глобальный отладочный лог
        # ...
    }
}
```

Сохранение отладочного лога для сервера

Чтобы сохранить сбор отладочной информации для конкретного сервера, но направить ее в другой файл, необходимо также указать уровень `debug`:

```
error_log /var/log/angie-lb/error.log debug; # Глобальный отладочный лог

http {

    server {
```

```
        listen 80;
        server_name example.com;

        error_log /var/log/angie-lb/example.com.error.log debug;
        # Отладочный лог для example.com включен, но пишется в отдельный файл

        # ...
    }
}
```

Таким образом, чтобы включить отладочный лог глобально, но переопределить файл лога для отдельных блоков, также укажите уровень `debug` в этих переопределениях. Иначе, если в директиве adc__error_log не указан уровень логирования, по умолчанию будет использоваться уровень `error` и отладочная информация для этих блоков будет потеряна.

3.1.9.3 Лог для отдельных адресов

Можно включить отладочный лог только для указанных клиентских адресов:

```
error_log /path/to/log;

events {
  debug_connection 192.168.1.1;
  debug_connection 192.168.10.0/24;
}
```

3.2 Глобальная балансировка

В этом разделе:

- *Настройка GSLB*
- *Типы глобальной балансировки*
- *Включение и выключение глобальной балансировки*
- *Использование EDNS Client Subnet*
- *Настройка IP-адресов ADNS*
- *Определение доступности дата-центров*
- *Добавление доменов и записей*
- *Балансировка по географическому положению*

Глобальная балансировка, также GSLB (Global Server Load Balancing) — это сервис, который позволяет распределять запросы клиентов между несколькими дата-центрами на основе их доступности и производительности.

Для работы глобальной балансировки собирается кластер Angie ADC, настраивается конфигурация GSLB и делегирование зон на GSLB-серверы Angie ADC. Локальный DNS-сервер будет отправлять клиентские запросы для этих зон на один из GSLB-серверов. Сервер GSLB решает, какой дата-центр лучше обслужит запрос, выбирает бэкенд и передает его IP-адрес DNS-серверу. DNS-сервер отправляет этот IP-адрес клиенту, после чего клиент направляет свой запрос на новый сервер по полученному адресу. Конфигурация GSLB распространяется на все узлы кластера.

Поддерживаются динамические записи типа A, AAAA и CNAME и статические записи типа A, AAAA, CNAME, MX, TXT.

Для динамических записей поддерживаются следующие типы балансировки:

- `round-robin`;

- `weighted round-robin`;
- `failover`;
- `ip-hash`;
- `geo-affinity`;
- `least connection`.

Поддерживается `Persistence` — закрепление клиента за выбранным бэкендом на определенный период времени. Доступность бэкендов контролируется мониторами доступности.

Можно просмотреть статистику работы GSLB: *Статистика глобальной балансировки*.

Возможности GSLB в Angie ADC:

- Гибкая настройка балансировки: поддержка статических и динамических записей, поддержка нескольких записей для одного домена.
- Масштабируемость: простота добавления новых доменов и записей через веб-интерфейс.
- Отказоустойчивость: непрерывная доступность приложений даже при сбоях в одном из дата-центров, возможность настройки TTL.
- Кластеризация: упрощение администрирования нескольких GSLB-модулей в разных дата-центрах.

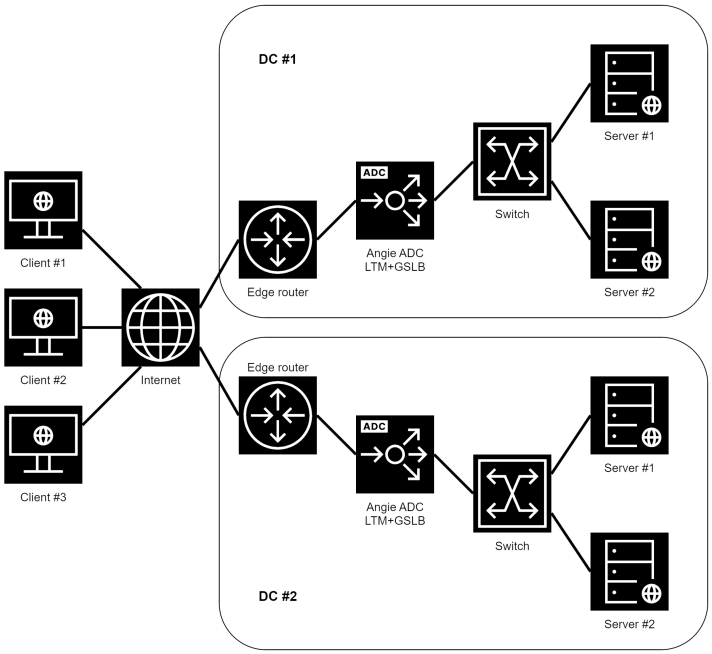


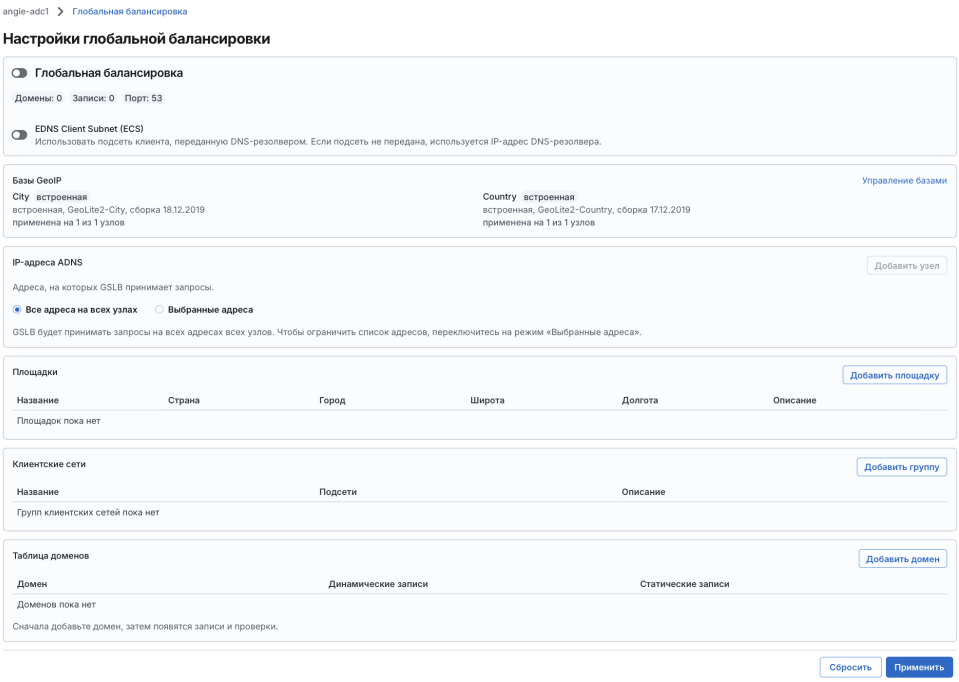
Рис. 1: Рис. 1: Пример развертывания кластера из двух Angie ADC с GSLB в двух дата-центрах

3.2.1 Настройка GSLB

Настройка GSLB включает в себя настройку конфигурации глобальной балансировки (`Управление трафиком` → `Глобальная балансировка`) и настройку сервиса GSLB.

Настройка GSLB состоит из следующих шагов:

1. Настройка мониторов доступности. Созданные мониторы необходимо привязать к сервисам GSLB в настройках динамической записи для обеспечения отказоустойчивости.



Для каждого дата-центра нужно настроить два типа мониторов доступности:

- *Монитор, определяющий доступность самого дата-центра* (проверяет доступность адреса, который GSLB отдает клиентам, т. е. отвечает на вопрос, принимает ли дата-центр клиентский трафик).
- *Мониторы, определяющие доступность приложений в дата-центре* (проверяют доступность серверов приложений, т. е. отвечают на вопрос, есть ли кому обрабатывать запросы в дата-центре).

2. Настройка конфигурации GSLB в веб-интерфейсе (на любом из узлов кластера):
   - Включение использования *EDNS Client Subnet*, если необходимо.
   - Настройка *IP-адресов ADNS*, если необходимо (позволяет ограничить адреса, на которых узлы кластера принимают DNS-запросы).
   - Настройка *площадок* и *групп клиентских подсетей* (для балансировки по географическому положению).
   - Добавление *доменов и DNS-записей*.
   - Применение всей конфигурации.
   - *Включение* функции глобальной балансировки.

   Синхронизация конфигурации GSLB на другие узлы кластера происходит автоматически.

3. Настройка делегирования заданных доменов на GSLB-узлы Angie ADC на первичном DNS-сервере.

   Пример для `www.example.com` — делегирование зоны `example.com` на GSLB-узлы Angie ADC в родительской зоне `com`:

```
www.example.com.       IN NS adc-dc1.example.com.
www.example.com.       IN NS adc-dc2.example.com.

; Glue-записи - IP-адреса GSLB-узлов Angie ADC
adc-dc1.example.com.  IN A  <IP-адрес dc1>
adc-dc2.example.com.  IN A  <IP-адрес dc2>
```

3.2.2 Типы глобальной балансировки

Тип балансировки задается в параметрах динамической записи. В Angie ADC поддерживаются следующие типы глобальной балансировки:

- *round-robin*;
- *weighted round-robin*;
- *failover*;
- *ip-hash*;
- *geo-affinity*;
- *least connection*.

Также поддерживается *Persistence* — закрепление клиента за выбранным дата-центром на определенный период времени. Доступность дата-центров контролируется мониторами доступности. Мониторы рекомендуется настроить заранее. При отсутствии доступных дата-центров, совместимых с типом записи, GSLB возвращает пустой DNS-ответ.

3.2.2.1 Балансировка round-robin

В режиме `round-robin` запросы последовательно распределяются между доступными бэкендами (дата-центрами) динамической записи: каждый следующий запрос направляется на следующий бэкенд. Бэкенды используются равномерно, приоритет и вес не учитываются.

3.2.2.2 Балансировка weighted round-robin

В режиме `weighted round-robin` для каждого запроса доступный бэкенд (дата-центр) выбирается случайно с вероятностью, пропорциональной его весу: чем больше значение параметра `Вес` у бэкенда, тем чаще на него направляются запросы. Этот тип балансировки рекомендуется, если дата-центры имеют разную производительность. Вес является обязательным параметром для этого типа балансировки.

3.2.2.3 Балансировка failover

В режиме `failover` запросы направляются на доступный бэкенд (дата-центр) с наивысшим приоритетом. Чем меньше значение, тем выше приоритет бэкенда, которому это значение назначено. Если бэкенд с наивысшим приоритетом недоступен, запросы направляются на следующий по приоритету доступный бэкенд. Этот тип балансировки подходит, если вы хотите использовать один дата-центр как основной, пока он доступен, и возвращаться на него при его восстановлении. Приоритет является обязательным параметром для этого типа балансировки.

3.2.2.4 Балансировка ip-hash

В режиме `ip-hash` для клиента выбирается один из доступных бэкендов (дата-центров) и все запросы этого клиента направляются на этот бэкенд, пока он доступен. Если бэкенд перестал быть доступен, то клиенту будет назначен другой бэкенд. Приоритет и вес не учитываются.

Клиент идентифицируется по адресу из *EDNS Client Subnet (ECS)*, а при его отсутствии — по IP-адресу DNS-резолвера. Без ECS все клиенты, обращающиеся через один кэширующий резолвер, определяются как один клиент (по адресу резолвера) и направляются на один и тот же бэкенд.

Примечание

Бэкенд вычисляется по текущему набору доступных бэкендов, поэтому при изменении текущего набора (выход дата-центра из строя или его восстановление) большинство клиентов будет перераспределено. Если требуется жесткое закрепление клиента за бэкендом, используйте *Persistence*.

3.2.2.5 Балансировка geo-affinity

В режиме `geo-affinity` запросы направляются на доступный бэкенд (дата-центр), ближайший к клиенту по географическому положению. Приоритет является обязательным параметром для этого типа балансировки. Вес не учитывается.

Для каждого бэкенда в записи указывается *площадка*, определяющая его географическое положение (обязательный параметр), и, при необходимости, *группа клиентских подсетей* (не более одной). Одна группа может быть назначена нескольким бэкендам одной или разных записей. Расположение клиента определяется по адресу из *EDNS Client Subnet (ECS)*, а при его отсутствии — по IP-адресу DNS-резолвера.

Бэкенд выбирается по следующему алгоритму:

1. Определяется *группа клиентских подсетей*, которой принадлежит подсеть клиента, и отбираются доступные бэкенды записи, которым назначена эта группа.
2. Если бэкендов с подходящей группой нет или группы не заданы, то по *базам GeoIP* определяются город и страна для клиента: сначала ищется совпадение по городу, а при его отсутствии — по стране.
3. Среди отобранных бэкендов выбирается ближайший к клиенту по координатам. Если выбрать по координатам нельзя, то бэкенд будет выбран по приоритету (чем меньше значение, тем выше приоритет бэкенда, которому это значение назначено).
4. Если подходящих бэкендов не нашлось, выполняется глобальный выбор среди всех доступных бэкендов записи, сначала по расстоянию, а затем по приоритету. При равном расстоянии выбирается бэкенд с меньшим числовым значением приоритета. При равном расстоянии и приоритете возвращаются все соответствующие бэкенды.

3.2.2.6 Балансировка least connection

В режиме `least connection` запрос направляется на доступный бэкенд (дата-центр) с наименьшей текущей нагрузкой — числом соединений или запросов на балансировщике нагрузки (LTM) этого бэкенда. В ответе возвращается один адрес. Приоритет и вес не учитываются. Режим доступен только для динамических записей A и AAAA.

Нагрузка бэкендов GSLB определяется с помощью датчиков, считающих количество соединений на балансировщиках нагрузки (LTM) этих бэкендов:

- На узле кластера, где работает балансировщик бэкенда, настраивается *датчик* с проверкой `Соединения LTM`. Датчик периодически запрашивает число соединений или запросов у API балансировщика нагрузки на своем узле.
- Датчик подключается к *монитору* типа `Метрика`. Обычно в мониторе один датчик — датчик того балансировщика, на котором работает VIP этого бэкенда. Несколько датчиков может понадобиться, если нагрузку одного бэкенда несут несколько узлов, например в паре высокой доступности. Если датчиков несколько, их значения сводятся в одно число по правилу агрегации.
- Для каждого бэкенда GSLB в динамической записи в поле `Монитор метрики` выбирается монитор, отслеживающий число соединений LTM.

Каждый GSLB-сервер сравнивает нагрузку LTM всех дата-центров.

Бэкенд выбирается по следующему алгоритму:

1. Отбираются доступные бэкенды с адресом, подходящим типу запроса.
2. Среди них остаются бэкенды, для которых есть актуальное значение монитора метрики. Значение актуально, пока не истекло время `Устаревание (stale_after)` датчиков монитора.
3. Выбирается бэкенд с наименьшим значением в мониторе. Если наименьшее значение у нескольких бэкендов, они выбираются по очереди.

4. Если актуального значения нет ни у одного доступного бэкенда, бэкенд выбирается по `round-robin`. Когда значения снова начинают поступать, запись автоматически возвращается к режиму `least connection`.

Значение монитора обновляется не чаще, чем выполняются замеры датчиков. Чтобы до следующего замера все новые клиенты не направлялись на один бэкенд, GSLB-сервер прибавляет к значению бэкенда число ответов, которые он сам выдал на этот бэкенд после последнего замера. Ответы других GSLB-серверов при этом не учитываются, поэтому оценка нагрузки между замерами приблизительная.

Пример: на бэкенде A — 12 соединений, на B — 4, на C — 9. Пока все бэкенды доступны и их значения актуальны, в ответе возвращается B. Если B станет недоступен, будет выбран C.

При включенном *Persistence* клиенту возвращается закрепленный за ним доступный бэкенд без сравнения нагрузки. Балансировка `least connection` применяется, когда бэкенд выбирается заново: при первом запросе клиента, при недоступности закрепленного бэкенда или после истечения привязки.

Примечание

Сравнивать можно только значения одной величины. Если мониторы метрики бэкендов одной записи используют датчики с разными объектами (например, `Весь LTM` у одного бэкенда и `Upstream` у другого), запись отвечает по `round-robin`. В этом случае в параметрах записи отображается предупреждение.

Рекомендации по настройке:

- Задайте для записи `TTL` не больше значения `Интервал проверки` датчиков: DNS-резолверы кэшируют ответ на время `TTL`, и все их клиенты в течение этого времени получают один и тот же бэкенд.
- Используйте `Интервал проверки` датчиков не менее `5s`.
- Синхронизируйте время на узлах кластера (NTP). Если часы узлов расходятся больше чем на `Устаревание (stale_after)` датчиков, значения датчиков другого узла сразу считаются устаревшими и не участвуют в выборе.
- Учитывайте, что при перезагрузке конфигурации балансировщика нагрузки статистика групп upstream и зон `status_zone` обнуляется. Пока не закроются соединения, открытые до перезагрузки, датчики с объектами `Upstream` и `Зона (status_zone)` показывают меньше соединений, чем есть на самом деле.

3.2.2.7 Закрепление бэкенда за клиентом (Persistence)

При настройке динамической записи вы можете закрепить клиента за выбранным бэкендом (дата-центром) на определенный период времени, включив переключатель `Persistence`. Повторные DNS-запросы клиента к одной записи будут возвращать один и тот же бэкенд, независимо от того, в какой дата-центр пришел запрос, что уменьшает число переключений между дата-центрами.

Клиент определяется по адресу из *EDNS Client Subnet (ECS)*, а при его отсутствии — по IP-адресу DNS-резолвера.

При выключении `Persistence` сохраненные привязки сбрасываются.

Закрепление работает следующим образом:

1. При первом запросе клиента бэкенд выбирается действующим типом балансировки и закрепляется за клиентом.
2. При каждом следующем DNS-запросе проверяется доступность закрепленного бэкенда. Если бэкенд доступен, система возвращает его и продлевает привязку на время, указанное в `Persistence timeout`.

3. Если закрепленный бэкенд недоступен, система выбирает другой доступный бэкенд и обновляет привязку. Восстановление предыдущего бэкенда не возвращает на него клиента.
4. Если привязка истекла по времени `Persistence timeout`, следующий запрос снова проходит через действующий тип балансировки, после чего сессия будет привязана к новому выбранному бэкенду.

> **Примечание**
>
> В отличие от балансировки *ip-hash*, которая заново распределяет клиентов между доступными бэкендами при изменении их состава, `Persistence` сохраняет индивидуальную привязку клиента на указанное время, если закрепленный бэкенд доступен.

3.2.3 Включение и выключение глобальной балансировки

Вы можете включить или выключить сервис глобальной балансировки с любого узла кластера в разделе `Управление трафиком` → `Глобальная балансировка`. При выключении глобальной балансировки GSLB перестает обрабатывать DNS-запросы. При этом настроенные параметры конфигурации GSLB сохраняются на всех узлах.

Чтобы включить или выключить глобальную балансировку:

1. Откройте веб-интерфейс Angie ADC и перейдите в раздел `Управление трафиком` → `Глобальная балансировка`.

   Откроется окно настройки глобальной балансировки.
2. Включите или выключите переключатель `Глобальная балансировка` в блоке глобальных параметров в верхней части экрана.
3. Нажмите `Применить` в нижней части экрана, чтобы применить изменение в конфигурации.

Изменение распространяется на все узлы кластера.

3.2.4 Использование EDNS Client Subnet

Функция `EDNS Client Subnet (ECS)` позволяет определять клиента по подсети, переданной DNS-резолвером. Если переключатель `EDNS Client Subnet (ECS)` включен и запрос содержит опцию ECS, то для определения клиента будет использована переданная DNS-резолвером подсеть клиента. Если ECS отсутствует или переключатель выключен, то для определения клиента используется IP-адрес DNS-резолвера.

В режиме балансировки `geo-affinity` ECS позволяет определять географическое расположение клиента. В режиме балансировки `ip-hash` и при использовании `Persistence` по ECS идентифицируется клиент и выбирается бэкенд, на который направляются все запросы этого клиента.

Чтобы включить определение клиента по подсети:

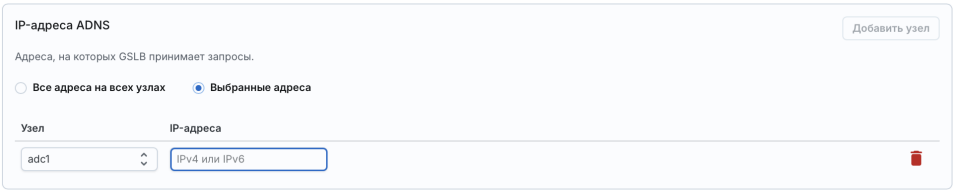
1. Откройте веб-интерфейс Angie ADC и перейдите в раздел `Управление трафиком` → `Глобальная балансировка`.

   Откроется окно настройки глобальной балансировки.
2. Включите переключатель `EDNS Client Subnet (ECS)` в блоке глобальных параметров в верхней части экрана.
3. Нажмите `Применить` в нижней части экрана, чтобы применить изменение в конфигурации.

3.2.5 Настройка IP-адресов ADNS

По умолчанию компонент GSLB принимает DNS-запросы на всех адресах всех узлов кластера Angie ADC. Список адресов можно ограничить, задав для каждого узла список локальных прослушиваемых IP-адресов.

Если узел принимает DNS-запросы из разных сетей в разных *доменах маршрутизации*, для него задается несколько строк, по одной на каждый домен маршрутизации. Запрос из одной сети к адресу в другом домене маршрутизации не проходит.



Чтобы задать список прослушиваемых IP-адресов:

1. Откройте веб-интерфейс Angie ADC и перейдите в раздел `Управление трафиком` → `Глобальная балансировка`.

   Откроется окно настройки глобальной балансировки.

2. В блоке `IP-адреса ADNS` выберите режим `Выбранные адреса`.
3. Нажмите `Добавить узел`.
4. Укажите имя узла и хотя бы один IP-адрес (IPv4 или IPv6).
5. В раскрывающемся списке `Домен маршрутизации` выберите домен маршрутизации узла, в котором находятся эти адреса, или оставьте `По умолчанию`, чтобы использовать общую сеть.

   Для одного узла можно добавить несколько строк с разными доменами маршрутизации; пара узла и домена маршрутизации в таблице должна быть уникальной.

   Примечание

   Проверяется только формат адреса. Не предусмотрена проверка наличия адреса на узле.

6. Повторите операцию для каждого узла, список адресов которого вы хотите ограничить.

   Примечание

   Если в таблице есть хотя бы одна строка, узел отвечает на DNS-запросы только на адресах из строк. Узел без строк в таблице на DNS-запросы не отвечает.

7. Нажмите `Применить` в нижней части экрана, чтобы применить изменение в конфигурации.

Статус применения конфигурации будет отображаться в верхней части экрана.

Чтобы изменить список прослушиваемых IP-адресов узла, в блоке `IP-адреса ADNS` выберите нужный узел и отредактируйте его. Добавить адрес можно кнопкой `+`, удалить — кнопкой `×` рядом с адресом. Затем нажмите `Применить` в нижней части экрана, чтобы применить изменение в конфигурации.

Чтобы удалить узел из таблицы, в блоке `IP-адреса ADNS` нажмите значок удаления напротив этого узла и нажмите `Применить` в нижней части экрана, чтобы применить изменение в конфигурации.

Важно

При переключении на режим `Все адреса на всех узлах` и применении конфигурации список ранее настроенных IP-адресов для каждого узла будет сброшен.

3.2.6 Определение доступности дата-центров

Для определения доступности дата-центра, т. е. принимает ли дата-центр клиентский трафик, необходимо настроить монитор этого дата-центра. Монитор будет проверять доступность адреса, который GSLB отдает клиентам. В монитор доступности дата-центра должны входить датчики со всех балансируемых дата-центров, проверяющие доступность адреса и порта, на которые приходят клиенты. Для этого подходят проверки `HTTP(S)` и `TCP`. Проверка `ICMP` не проверяет порт, а проверка `Angie` опрашивает API статуса Angie и не показывает, доступен ли адрес клиентам.

Подробнее о настройке мониторов см. *Настройка датчиков и мониторов*.

3.2.6.1 Рекомендации

- Для каждого дата-центра необходимо добавить монитор с датчиками со всех дата-центров, включая датчик самого дата-центра. Локальный датчик проверяет VIP изнутри узла, удаленные датчики из других дата-центров обнаруживают потерю внешнего канала связи. Датчики с удаленных узлов должны идти к VIP тем же путем, что и клиенты, не через внутреннюю бэкенд-сеть.
- Для датчика доступности используйте проверку `HTTP(S)` или `TCP` на адрес и порт, которые получает клиент. В качестве адреса может использоваться VIP узла Angie ADC. Если используется HTTPS-проверка, то в поле `SNI` укажите доменное имя, на которое выписан сертификат, иначе проверка сертификата не пройдет. Ожидаемый код ответа — `200`. Если бэкенд доступен только через домен маршрутизации, выберите этот домен в поле `Домен маршрутизации` датчика.
- Для корректного переключения клиентского трафика с недоступного дата-центра на доступный необходимо настроить перекрестные мониторы доступности для всех балансируемых дата-центров.

3.2.6.2 Состояния монитора

У монитора доступности могут быть следующие состояния:

- Если дата-центр работает, монитор находится в состоянии `исправен`.
- Если часть датчиков не работает или не присылает данные, но хотя бы один работает, монитор показывает `есть проблемы`. Дата-центр при этом остается в DNS-ответах.
- Если ни один датчик не подтверждает, что дата-центр работает, и хотя бы один фиксирует отказ, монитор переходит в состояние `неисправен`. Дата-центр исключается из DNS-ответов, а трафик переводится в другой дата-центр.
- Если ни от одного датчика нет данных, монитор переходит в состояние `нет данных`. В этом состоянии GSLB не меняет решение по дата-центру: если дата-центр был в DNS-ответах, он в них остается.

3.2.6.3 Пример

Для имени `www.example.com` используются два дата-центра, ЦОД-1 в Москве и ЦОД-2 в Новосибирске. В обоих дата-центрах установлены Angie ADC (узлы `dc-moscow` и `dc-novosibirsk`). Для обоих дата-центров нужно настроить мониторы, проверяющие их доступность.

Настройка:

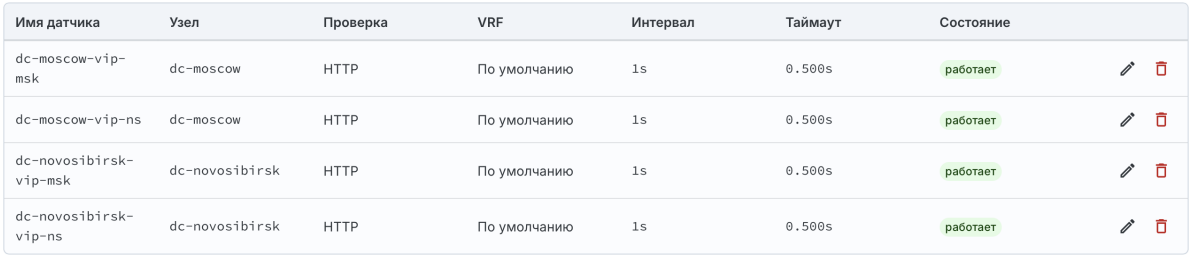
1. На любом узле Angie ADC перейдите в раздел `Система` → `Доступность` → вкладка `Датчики` и создайте четыре датчика: два для VIP `dc-moscow` и два для VIP `dc-novosibirsk`.

> **Совет**
>
> При создании датчика, проверяющего адрес, в поле `Узлы` можно выбрать сразу все узлы. Для каждого выбранного узла будет создан отдельный датчик, проверяющий этот адрес.

Параметры датчиков:

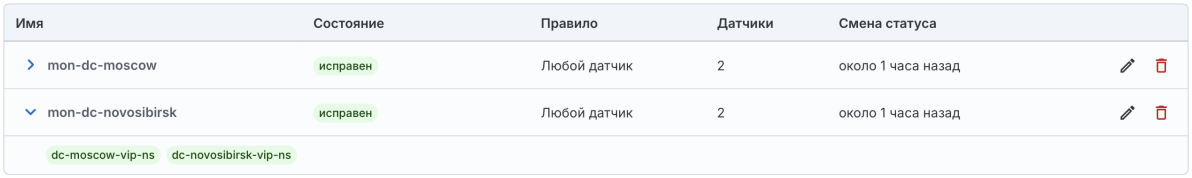
Имя проверяемого ресурса	Узлы	Проверка	Датчики
`vip-msk`	`dc-moscow`, `dc-novosibirsk`	HTTP на VIP `dc-moscow`	`dc-moscow-vip-msk` (локальный) `dc-novosibirsk-vip-msk` (удаленный)
`vip-ns`	`dc-moscow`, `dc-novosibirsk`	HTTP на VIP `dc-novosibirsk`	`dc-novosibirsk-vip-ns` (локальный) `dc-moscow-vip-ns` (удаленный)

Созданные датчики:



Имя датчика	Узел	Проверка	VRF	Интервал	Таймаут	Состояние
dc-moscow-vip-msk	dc-moscow	HTTP	По умолчанию	1s	0.500s	работает
dc-moscow-vip-ns	dc-moscow	HTTP	По умолчанию	1s	0.500s	работает
dc-novosibirsk-vip-msk	dc-novosibirsk	HTTP	По умолчанию	1s	0.500s	работает
dc-novosibirsk-vip-ns	dc-novosibirsk	HTTP	По умолчанию	1s	0.500s	работает

2. Создайте мониторы доступности дата-центров. В монитор доступности каждого дата-центра должны входить локальный и удаленный датчики.



Имя	Состояние	Правило	Датчики	Смена статуса
mon-dc-moscow	исправен	Любой датчик	2	около 1 часа назад
mon-dc-novosibirsk	исправен	Любой датчик	2	около 1 часа назад
dc-moscow-vip-ns dc-novosibirsk-vip-ns				

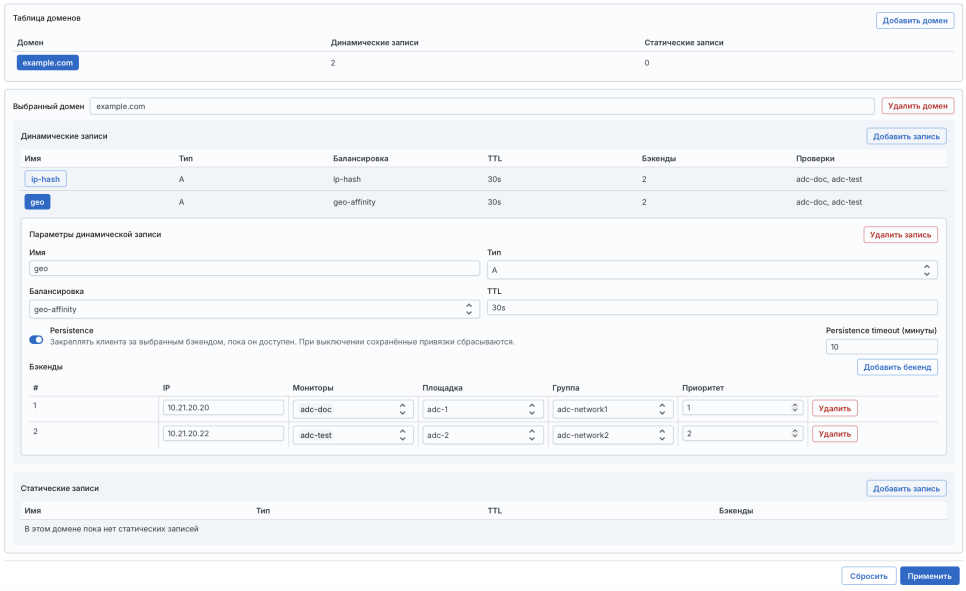
Здесь:

- В мониторе `mon-dc-moscow` датчики `dc-novosibirsk-vip-msk` и `dc-moscow-vip-msk` проверяют доступность дата-центра в Москве.
- В мониторе `mon-dc-novosibirsk` датчики `dc-novosibirsk-vip-ns` и `dc-moscow-vip-ns` проверяют доступность дата-центра в Новосибирске.
- По правилу `Любой датчик` монитор считается исправным, а дата-центр доступным, если его `VIP` отвечает хотя бы с одного узла. Если узел дата-центра выключен или потерял связь с остальными узлами, удаленный датчик переходит в состояние `не работает`. Локальный датчик при этом через время `Устаревание` переходит в `нет данных`. После этого монитор становится `неисправен`.

3. Перейдите в раздел `Управление трафиком` → `Глобальная балансировка` и настройте конфигурацию GSLB. Для домена `example.com` добавьте динамическую запись типа `A` с именем `www`, укажите режим балансировки и задайте два бэкенда, по одному на дата-центр. Для каждого бэкенда в колонке `Мониторы` выберите монитор соответствующего дата-центра.
4. Завершите настройку динамической записи, добавив *мониторы приложений*.

Мониторы объединяются по логике **И**: дата-центр остается в DNS-ответах, только если по последним полученным данным исправны все мониторы (и монитор дата-центра, и мониторы приложений).

3.2.7 Добавление доменов и записей



Чтобы добавить домен и настроить для него глобальную балансировку, выполните следующие действия:

1. Откройте веб-интерфейс Angie ADC и перейдите в раздел `Управление трафиком` → `Глобальная балансировка`.

   Откроется окно настройки глобальной балансировки.

2. В блоке `Таблица доменов` нажмите `Добавить домен` и укажите имя домена, например `example.com`. Имя домена должно быть корректным DNS-именем без завершающей точки.

3. Настройте записи для добавленного домена. Выберите тип записи (статическая или динамическая) и укажите необходимые параметры.

> **Совет**
>
> - Чтобы настроить балансировку для домена, а не только для записей внутри него, создайте динамическую запись типа `A` с именем `@` и укажите необходимые параметры балансировки.
> - Чтобы задать общее правило балансировки для разных поддоменов, создайте динамическую запись типа `A` с именем `*` и укажите необходимые параметры балансировки.

Параметры динамической записи типа A и AAAA

`Имя`	Имя записи. Должно быть уникальным в рамках одного домена.
`Тип`	Тип записи. Возможные значения: • `A` — сопоставляет доменное имя с IPv4-адресом. • `AAAA` — сопоставляет доменное имя с IPv6-адресом.
`Балансировка`	Тип балансировки. Возможные значения: • `round-robin` — запросы распределяются по бэкендам последовательно. • `weighted round-robin` — для каждого запроса бэкенд выбирается случайно с вероятностью, пропорциональной его весу (на бэкенды с большим весом запросы будут попадать чаще). • `failover` — запрос направляется на доступный бэкенд с наивысшим приоритетом. Чем меньше значение, тем выше приоритет бэкенда, которому это значение назначено. • `geo-affinity` — запрос направляется на доступный бэкенд, ближайший к клиенту по географическому положению (подробнее см. *Балансировка geo-affinity*). • `ip-hash` — все запросы одного клиента направляются на один и тот же доступный бэкенд (подробнее см. *Балансировка ip-hash*). • `least connection` — запрос направляется на доступный бэкенд с наименьшим числом соединений или запросов на его балансировщике нагрузки (LTM) (подробнее см. *Балансировка least connection*).
`TTL`	Значение TTL (Time to Live) с указанием единицы времени: `ms` (миллисекунды), `s` (секунды), `m` (минуты) или `h` (часы). Определяет, как долго DNS-запись может храниться в кэше. Все последующие запросы в течение времени TTL будут идти строго на выбранный адрес. По умолчанию установлено значение `30s`.
`Persistence`	Закрепляет клиента за выбранным бэкендом, пока он доступен: повторные DNS-запросы клиента возвращают один и тот же бэкенд (подробнее см. *Закрепление бэкенда за клиентом (Persistence)*). По умолчанию переключатель выключен. **Примечание** При выключении `Persistence` сохраненные привязки сбрасываются.
`Persistence timeout`	Время привязки в минутах. Возможные значения: от `2` до `1440` минут. По умолчанию `10` минут. Поле доступно при включенном `Persistence` и настраивается независимо от `TTL` записи.
`Бэкенды`	Таблица бэкендов GSLB. Необходимо задать минимум один бэкенд. Набор параметров бэкенда зависит от выбранного типа балансировки: **Параметры бэкенда для round-robin** • `IP`: IP-адрес бэкенда (например, IP-адрес узла кластера Angie ADC). Поддерживаются IPv4- и IPv6-адреса. • `Мониторы`: один или несколько мониторов доступности, привязанных к бэкенду. Выбираются из списка *настроенных мониторов* типа `Здоровье`. Если задано несколько мониторов, бэкенд считается доступным, когда исправны все заданные мониторы. **Параметры бэкенда для weighted round-robin** • `IP`: IP-адрес бэкенда (например, IP-адрес узла кластера Angie ADC). Поддерживаются IPv4- и IPv6-адреса. • `Мониторы`: один или несколько мониторов доступности, привязанных к бэкенду. Выбираются из списка *настроенных мониторов* типа `Здоровье`. Если задано несколько мониторов, бэкенд считается доступным, когда исправны все заданные мониторы. • `Вес`: вес бэкенда. На бэкенды с большим весом запросы будут попадать чаще. Обязательный параметр.

Параметры динамической записи типа CNAME

`Имя`	Имя записи.
`Тип`	Тип записи `CNAME` — задает псевдоним для другого доменного имени.
`Балансировка`	Тип балансировки. Возможные значения: • `round-robin` — система проверяет доступность бэкендов и распределяет запросы по бэкендам последовательно. • `weighted round-robin` — система проверяет доступность бэкендов и для каждого запроса выбирает бэкенд случайно с вероятностью, пропорциональной его весу (на бэкенды с большим весом запросы будут попадать чаще). • `failover` — система проверяет доступность бэкендов и выбирает лучший по приоритету. Чем меньше значение, тем выше приоритет бэкенда, которому это значение назначено. • `geo-affinity` — запрос направляется на доступный бэкенд, ближайший к клиенту по географическому положению (подробнее см. *Балансировка geo-affinity*). • `ip-hash` — все запросы одного клиента направляются на один и тот же доступный бэкенд (подробнее см. *Балансировка ip-hash*).
`TTL`	Значение TTL (Time to Live) с указанием единицы времени: `ms` (миллисекунды), `s` (секунды), `m` (минуты) или `h` (часы). Определяет, как долго DNS-запись может храниться в кэше. Все последующие запросы в течение времени TTL будут идти строго на выбранный домен. По умолчанию установлено значение `30s`.
`Persistence`	Закрепляет клиента за выбранным бэкендом, пока он доступен: повторные DNS-запросы клиента возвращают один и тот же бэкенд (подробнее см. *Закрепление бэкенда за клиентом (Persistence)*). По умолчанию переключатель выключен. **Примечание** При выключении `Persistence` сохраненные привязки сбрасываются.
`Persistence timeout`	Время привязки в минутах. Возможные значения: от `2` до `1440` минут. По умолчанию `10` минут. Поле доступно при включенном `Persistence` и настраивается независимо от `TTL` записи.
`Бэкенды`	Таблица бэкендов. Необходимо задать минимум один бэкенд. Набор параметров бэкенда зависит от выбранного типа балансировки: **Параметры бэкенда для round-robin** • `Host`: доменное имя, на которое будет указывать CNAME-запись. • `Мониторы`: один или несколько мониторов доступности, привязанных к бэкенду. Выбираются из списка *настроенных мониторов* типа `Здоровье`. Если задано несколько мониторов, бэкенд считается доступным, когда исправны все заданные мониторы. **Параметры бэкенда для weighted round-robin** • `Host`: доменное имя, на которое будет указывать CNAME-запись. • `Мониторы`: один или несколько мониторов доступности, привязанных к бэкенду. Выбираются из списка *настроенных мониторов* типа `Здоровье`. Если задано несколько мониторов, бэкенд считается доступным, когда исправны все заданные мониторы. • `Вес`: вес бэкенда. На бэкенды с большим весом запросы будут попадать чаще. Обязательный параметр.

Параметры статической записи типа A и AAAA

`Имя`	Имя записи.
`Тип`	Тип записи. Возможные значения: • `A` — сопоставляет доменное имя с IPv4-адресом. • `AAAA` — сопоставляет доменное имя с IPv6-адресом.
`TTL`	Значение TTL (Time to Live) с указанием единицы времени: `ms` (миллисекунды), `s` (секунды), `m` (минуты) или `h` (часы). Определяет, как долго DNS-запись может храниться в кэше. По умолчанию установлено значение `300s`.
`Бэкенды`	Таблица бэкендов. Для каждого бэкенда задаются его параметры: • `IP`: IP-адрес бэкенда (например, IP-адрес узла кластера Angie ADC). Поддерживаются IPv4- и IPv6-адреса.

Параметры статической записи типа CNAME

`Имя`	Имя записи.
`Тип`	Тип записи `CNAME` — задает псевдоним для другого доменного имени. Необходимо указать ровно один хост.
`TTL`	Значение TTL (Time to Live) с указанием единицы времени: `ms` (миллисекунды), `s` (секунды), `m` (минуты) или `h` (часы). Определяет, как долго DNS-запись может храниться в кэше. По умолчанию установлено значение `300s`.
`Бэкенды`	Целевой домен Необходимо указать ровно один домен: • `Host`: доменное имя, на которое будет указывать CNAME-запись.

Параметры статической записи типа MX

`Имя`	Имя записи.
`Тип`	Тип записи `MX` — указывает почтовый сервер для домена. Необходимо указать хотя бы один почтовый сервер.
`TTL`	Значение TTL (Time to Live) с указанием единицы времени: `ms` (миллисекунды), `s` (секунды), `m` (минуты) или `h` (часы). Определяет, как долго DNS-запись может храниться в кэше. По умолчанию установлено значение `300s`.
`Бэкенды`	Почтовые серверы. • `Host`: доменное имя почтового сервера. • `Приоритет`: приоритет сервера. Чем меньше значение, тем выше приоритет сервера, которому это значение назначено. Необязательный параметр.

Параметры статической записи типа TXT

`Имя`	Имя записи.
`Тип`	Тип записи `TXT` — содержит произвольный текст.
`TTL`	Значение TTL (Time to Live) с указанием единицы времени: `ms` (миллисекунды), `s` (секунды), `m` (минуты) или `h` (часы). Определяет, как долго DNS-запись может храниться в кэше. По умолчанию установлено значение `300s`.
`Бэкенды`	Значения статической записи типа TXT. • `Текст`: TXT-запись должна содержать непустой текст длиной не более 4096 символов.

4. Нажмите `Применить` в нижней части экрана, чтобы применить конфигурацию.

Статус применения конфигурации будет отображаться в верхней части экрана.

Чтобы отредактировать домен или запись, нажмите на название этого домена или записи и измените нужные параметры. Затем нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

Чтобы удалить домен или запись, нажмите значок удаления напротив этого домена или записи. Затем нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

3.2.8 Балансировка по географическому положению

В режиме балансировки *geo-affinity* GSLB направляет запросы клиента на ближайший к нему доступный бэкенд (дата-центр). Расположение бэкенда задается *площадкой*. Клиентов из определенных подсетей можно закрепить за бэкендом с помощью *группы клиентских подсетей*.

В этом разделе:

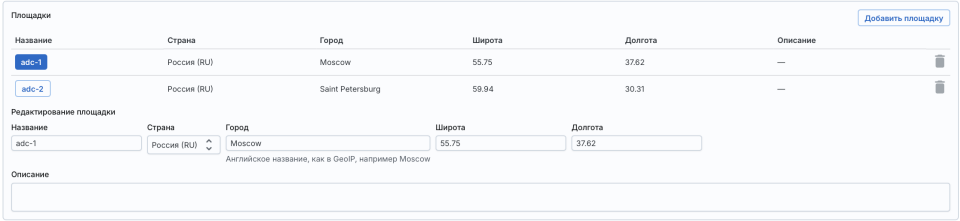
- *Настройка географических площадок*
- *Настройка групп клиентских подсетей*
- *Настройка баз GeoIP*
- *Настройка балансировки по географическому положению*

3.2.8.1 Настройка географических площадок

Площадка назначается бэкенду при выборе типа балансировки `geo-affinity` и позволяет задать географическое расположение бэкенда: страну, город и координаты. Одну площадку можно назначить нескольким бэкендам.

Примечание

Для большей точности рекомендуется всегда указывать координаты, так как автоматическое определение координат по городу не выполняется.



Чтобы добавить площадку:

1. Откройте веб-интерфейс Angie ADC и перейдите в раздел `Управление трафиком` → `Глобальная балансировка`.

   Откроется окно настройки глобальной балансировки.

2. В блоке `Площадки` нажмите `Добавить площадку`.

3. Задайте параметры площадки:

`Название`	Название площадки, например `Москва`. Название должно быть уникальным в рамках GSLB-кластера. Обязательный параметр.
`Страна`	Страна размещения площадки, выбирается из списка. Параметр обязателен, если задан параметр `Город`.
`Город`	Город размещения площадки. Указывается на английском в соответствии с названием в базе GeoIP, например `Moscow`. Необязательный параметр.
`Широта`	Географическая широта площадки (в десятичных градусах). Число в диапазоне от `-90` до `90`, рекомендуется указывать хотя бы два знака после точки. Параметр обязателен, если задан параметр `Долгота`.
`Долгота`	Географическая долгота площадки (в десятичных градусах). Число в диапазоне от `-180` до `180`, рекомендуется указывать хотя бы два знака после точки. Параметр обязателен, если задан параметр `Широта`.
`Описание`	Произвольное описание площадки. Необязательный параметр.

4. Нажмите `Применить` в нижней части экрана, чтобы сохранить площадку в конфигурации.

Чтобы отредактировать площадку, нажмите на ее название и измените нужные параметры, а затем нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

Чтобы удалить площадку, нажмите значок удаления напротив этой площадки и нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

> **Примечание**
>
> Площадку, назначенную бэкенду, нельзя удалить. Перед удалением площадки удалите ее из параметров всех бэкендов.

3.2.8.2 Настройка групп клиентских подсетей

Группа клиентских подсетей позволяет назначать правило балансировки на группу адресов, например на офис или отдел. При балансировке `geo-affinity` запросы из подсетей, входящих в группу, будут рассматриваться как относящиеся к одному расположению и распределяться на подходящий бэкенд. Одну группу можно назначить нескольким бэкендам.



Чтобы добавить группу:

1. Откройте веб-интерфейс Angie ADC и перейдите в раздел `Управление трафиком` → `Глобальная балансировка`.

   Откроется окно настройки глобальной балансировки.

2. В блоке `Клиентские сети` нажмите `Добавить группу`.

3. Задайте параметры группы:

`Название`	Имя группы. Должно быть уникальным в рамках GSLB-кластера. Обязательный параметр.
`Подсети`	Список подсетей в формате CIDR (IPv4 или IPv6). Необходимо указать хотя бы одну подсеть. Обязательный параметр. **Примечание** Адрес сети приводится к каноническому виду: например, `10.0.0.15/24` сохраняется как `10.0.0.0/24`. Подсети не могут совпадать или пересекаться ни внутри группы, ни с подсетями других групп.
`Описание`	Произвольное описание группы. Необязательный параметр.

4. Нажмите `Применить` в нижней части экрана, чтобы сохранить группу в конфигурации.

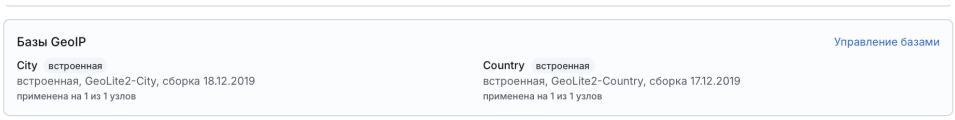
Чтобы отредактировать группу клиентских подсетей, нажмите на ее название и измените нужные параметры. Добавить подсеть можно кнопкой `+`, удалить — кнопкой `×` рядом с подсетью. Затем нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

Чтобы удалить группу, нажмите значок удаления напротив этой группы и нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

Примечание

Группу, назначенную бэкенду, нельзя удалить. Перед удалением группы удалите ее из параметров всех бэкендов.

3.2.8.3 Настройка баз GeoIP



Если клиент не относится ни к одной группе клиентских подсетей, GSLB определяет его город, страну и координаты по базам GeoIP. Используемые базы отображаются в блоке `Базы GeoIP`.

Angie ADC поставляется со встроенными базами двух типов:

- `City` — основная база, которая позволяет определить страну, город и координаты клиента;
- `Country` — вспомогательная база, которая позволяет определить только страну клиента и используется, если City-база по каким-то причинам недоступна.

Совет

Для более точного определения местоположения клиентов рекомендуется загрузить актуальную пользовательскую базу `City` и обновлять ее самостоятельно, так как базы GeoIP не обновляются автоматически.

Базы синхронизируются на всех узлах кластера.

Чтобы загрузить пользовательскую базу `City`:

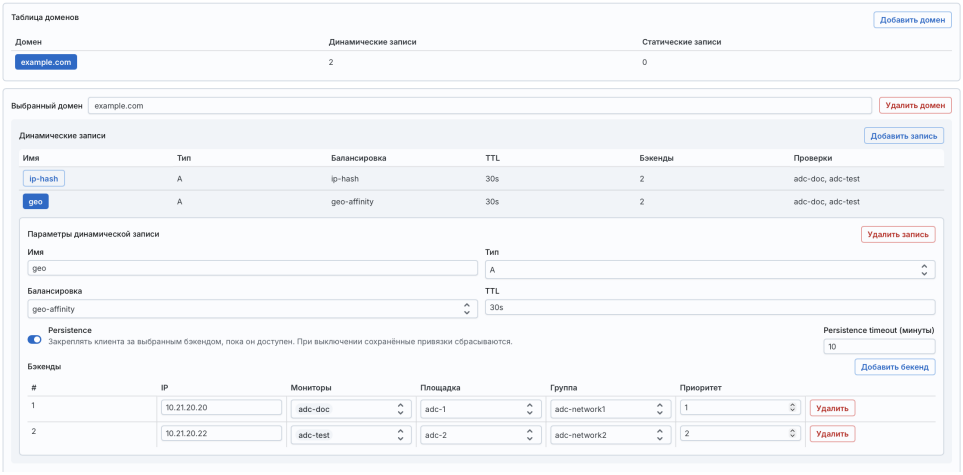
1. В блоке `Базы GeoIP` перейдите по ссылке `Управление базами`. Также можно перейти в раздел `Система` → `Базы GeoIP`.
2. Откроется страница настройки `Базы GeoIP`.
3. В блоке `City` нажмите `Загрузить` и укажите файл базы.

> **Примечание**
>
> Файл должен иметь формат MaxMind DB (`.mmdb`). Размер файла не должен превышать 512 МБ.

После загрузки база будет применена на узле сразу. Синхронизация базы на другие узлы кластера может занять некоторое время, в течение которого узлы могут определять местоположение клиентов по разным базам.

Подробнее см. *Базы GeoIP*.

3.2.8.4 Настройка балансировки по географическому положению



1. В разделе `Управление трафиком` → `Глобальная балансировка` включите переключатель `Глобальная балансировка`.
2. Включите переключатель `EDNS Client Subnet (ECS)`, чтобы GSLB определял расположение клиента по его подсети.
3. В блоке `Базы GeoIP` проверьте дату сборки действующих баз и при необходимости *загрузите актуальные базы*.
4. В блоке `Площадки` добавьте географические площадки, которые будут определять расположение ваших дата-центров.
5. В блоке `Клиентские сети` добавьте группы с корпоративными подсетями, если необходимо.
6. В блоке `Таблица доменов` добавьте домены, которые нужно балансировать. Для этого нажмите `Добавить домен` и укажите имя домена. Имя домена должно быть корректным DNS-именем без завершающей точки.
7. Для каждого домена добавьте динамические записи с типом балансировки `geo-affinity` и необходимыми бэкендами. Для каждого бэкенда укажите площадку и приоритет (обязательно) и группу клиентских подсетей, если есть. Также необходимо указать *мониторы доступности дата-центра* и *мониторы доступности приложений в дата-центре*.

8. Нажмите `Применить` в нижней части экрана, чтобы сохранить конфигурацию.
9. Настройте *делегирование доменов* на GSLB-узлы Angie ADC.

Запросы клиентов будут направляться в ближайший доступный дата-центр по географическому положению. Подробнее об алгоритме выбора бэкенда при балансировке `geo-affinity` см. *Балансировка geo-affinity*.

3.3 Типовые задачи и примеры

В этом разделе собраны примеры настройки Angie ADC под разные задачи.

3.3.1 Сеть и адресация

- *Настройка IPv6*
- *Настройка пула SNAT*
- *Настройка Transparent Proxy для TCP- и UDP-трафика*
- *Изоляция внешнего трафика и проксирование во внутреннюю сеть*

3.3.2 TLS и сертификаты

- *Настройка ACME*
- *Балансировка трафика на основе набора шифров*

3.3.3 Балансировка и отказоустойчивость

- *Глобальная балансировка с проверкой доступности приложений*
- adc_keepalive-oneconnect

3.3.4 Безопасность и контроль доступа

- *Ограничение доступа к ресурсам по IP-адресам*
- *Ограничение числа соединений, частоты запросов и скорости передачи*

3.3.5 Доставка контента

- *Загрузка и раздача статических файлов*

3.3.6 Администрирование и наблюдаемость

- *Делегирование сервиса оператору*
- *Настройка пользовательских метрик*

3.3.6.1 Сеть и адресация

Примеры сетевой настройки Angie ADC на уровне L3–L4: адресация, трансляция адресов и прозрачное проксирование трафика.

- *Настройка IPv6*
- *Настройка пула SNAT*
- *Настройка Transparent Proxy для TCP- и UDP-трафика*
- *Изоляция внешнего трафика и проксирование во внутреннюю сеть*

Настройка IPv6

IPv6 в Angie ADC настраивается на трех уровнях:

- Настройка доступа к веб-интерфейсу Angie ADC (management plane).
- Настройка сетевых протоколов маршрутизации (control plane).
- Настройки для передачи и обработки клиентского трафика (data plane).

Доступ к веб-интерфейсу Angie ADC

Веб-интерфейс Angie ADC одновременно поддерживает IPv4 и IPv6. Для доступа к веб-интерфейсу с IPv6-адресом `2001:db8::10` введите в браузере:

- `http://[2001:db8::10]:8080`
- `https://[2001:db8::10]:8443` (если требуется безопасное подключение).

Если есть DNS-запись для адреса `2001:db8::10`, можно обращаться к веб-интерфейсу по имени.

Настройка сетевых протоколов маршрутизации

IPv6-адреса интерфейсов задаются вручную в *сетевых настройках* узла (получение IPv6-адреса по DHCP не поддерживается). Адрес IPv6-сервиса можно задать на *интерфейсе lo* с префиксом `/128`.

Динамическая маршрутизация Angie ADC (команды *routing* и *vrrp*) работает только с IPv4:

- BGP — только адресное семейство IPv4 unicast, соседи задаются IPv4-адресами;
- OSPF — только OSPFv2, OSPFv3 не поддерживается;
- VRRP — виртуальный адрес группы только IPv4.

Поэтому IPv6-сервисы публикуются со статической маршрутизацией: на маршрутизаторе задается статический маршрут к IPv6-адресу сервиса через IPv6-адрес интерфейса Angie ADC, а маршруты самого узла — в *сетевых настройках*.

Передача и обработка клиентского трафика

Для поддержки IPv6:

- Бэкенд-серверы должны быть настроены на прием подключений по протоколу IPv6.
- В конфигурации балансировщика нагрузки необходимо включить прием трафика по IPv6:

  ```
  server {
      listen 80;
      listen [::]:80;
      location / {
  ```

  После этого балансировщик сможет принимать подключения по IPv6.

- Также необходимо добавить AAAA-записи в DNS, чтобы клиенты могли находить балансировщик по IPv6-адресу.
- Для маршрутизации трафика к бэкенд-серверам в секции `upstream` должны быть указаны IPv6-адреса.

  В примере ниже один сервер задан адресом IPv4, а второй — IPv6:

  ```
  http {
      upstream myapp1 {
          server 192.168.0.128:80;
          server [2001:db8::4]:80;
  ```

```
    }
}
```

Поддержка смешанных подключений IPv4 и IPv6 в Angie ADC

Angie ADC поддерживает гибкую маршрутизацию трафика между клиентами и бэкенд-серверами с разными конфигурациями.

Бэкенд-серверы могут быть трех типов:

- только IPv4;
- только IPv6;
- dual-stack (одновременно поддерживаются оба протокола).

Пример:

К некоторому ресурсу подключаются IPv4-клиенты (отмечены зеленым цветом) и IPv6-клиенты (отмечены красным цветом).

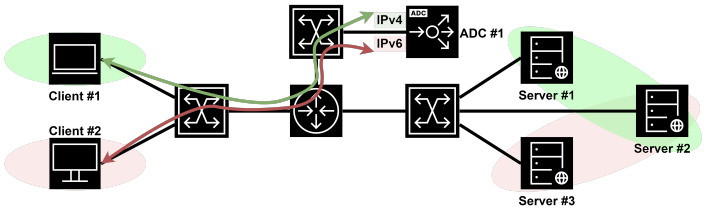


Рис. 1

Только IPv4

IPv4-сессии установлены между Angie ADC и бэкенд-серверами с поддержкой IPv4:

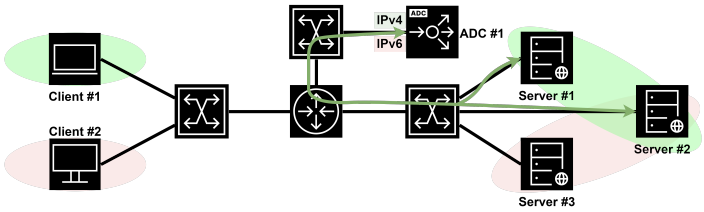


Рис. 2

Только IPv6

IPv6-сессии установлены между Angie ADC и бэкенд-серверами с поддержкой IPv6:

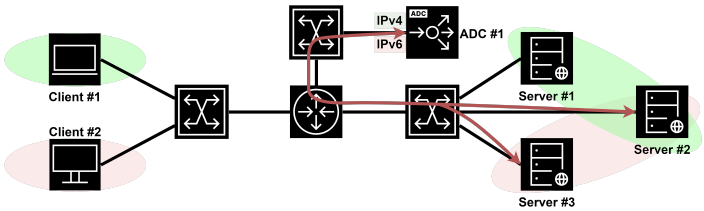


Рис. 3

Смешанные подключения

Angie ADC может проксировать входящие IPv4-подключения в любые сессии (как IPv4, так и IPv6) в сторону бэкенд-серверов. Аналогично и для IPv6-подключений.

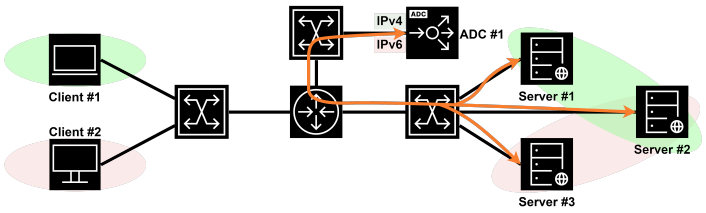


Рис. 4

Таким образом, Angie ADC позволяет гибко проксировать трафик между различными протоколами.

Преимущества такой схемы:

- Практически мгновенная публикация в сети IPv6-сервиса без поддержки IPv6 на бэкенд-серверах.
- Постепенный переход бэкенд-инфраструктуры на IPv6 без потери доступности сервисов снаружи по IPv4, т. е. возможна миграция с IPv4 на IPv6 с минимальными изменениями инфраструктуры.

Брандмауэр для IPv6

Правила брандмауэра для IPv4 и IPv6 задаются отдельно. Порты, которые использует Angie ADC, перечислены в adc_network-ports.

Чтобы открыть порт для IPv6, в контексте *firewall* выполните команду *open* с параметром `ip6` и сохраните правила командой *save*:

```
(firewall)$$ open ip6 tcp 9999 enp0s2
(firewall)$$ save
```

Настройка пула SNAT (SNAT Pool)

Введение

Пул SNAT (SNAT Pool, Source Network Address Translation Pool) — это набор IP-адресов, которые Angie ADC использует для подмены исходных IP-адресов клиентов при передаче трафика на серверы. SNAT-пулы применяются в высоконагруженных средах с большим количеством одновременно открытых сессий. Они позволяют обойти ограничение на количество одновременных подключений (около 65000 на один IP-адрес). Ограничение связано с количеством доступных клиентских сокетов (TCP- и UDP-портов), используемых для установки соединений. SNAT-пулы могут использоваться как для L4-, так и для L7-балансировки.

Примечание

Также возможен подход, основанный на горизонтальном масштабировании за счет установки нескольких Angie ADC и распределения трафика между ними. Этот подход позволяет решить проблему не только с ограничением количества сессий, но и снять ограничение на производительность системы, например, когда при больших объемах трафика необходимо обрабатывать данные на скоростях более 10 Гбит/с.

Ручная настройка SNAT-пулов

Настройка вручную создаваемых SNAT-пулов происходит в три этапа:

1. Выбор пула адресов и их настройка.
2. Настройка маршрутизации.
3. Настройка правил балансировки.

Пример простой схемы с одним Angie ADC представлен на рисунке ниже:

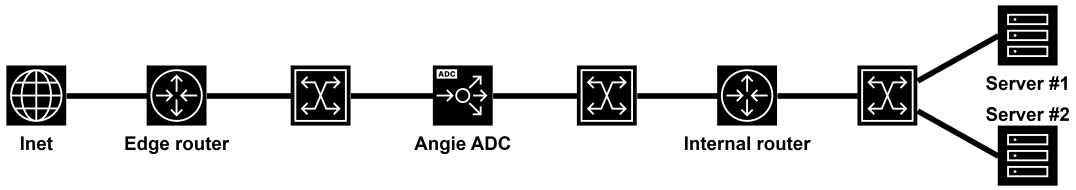


Рис. 1

1. Выбор пула адресов и их настройка

Размер пула адресов напрямую зависит от количества сессий, которые требуется одновременно поддерживать. Чем больше сессий должно работать одновременно, тем больше IP-адресов должно входить в пул.

Выбор адресов условно свободный, можно использовать адреса из разных подсетей. Мы не рекомендуем использовать чужие валидные адреса, чтобы избежать случайных пересечений с адресами клиентов. Также лучше выбирать адреса не из произвольного диапазона, а выделить конкретную подсеть, которая будет полностью использоваться в пуле. Это упростит дальнейшую настройку маршрутизации.

В примере ниже мы будем использовать подсеть `192.168.12.20/30`, включающую в себя четыре адреса. Так как все четыре адреса будут использоваться в качестве адресов отправителя пакетов на участке сети между Angie ADC и апстримами, то необходимо все эти четыре адреса назначить на сетевой интерфейс системы, например на *интерфейс lo*.

Пример конфигурации представлен ниже. Адреса назначаются с маской `/32`. Это нужно, чтобы система обрабатывала возвращающийся от серверов трафик и устанавливала полноценные соединения.

```
$$ configuration
## set system interface lo ip address 192.168.12.20/32
## set system interface lo ip address 192.168.12.21/32
## set system interface lo ip address 192.168.12.22/32
## set system interface lo ip address 192.168.12.23/32
```

Примечание

В этом примере между апстримами и Angie ADC размещен маршрутизатор. Ситуация, когда апстримы и один из интерфейсов Angie ADC размещены в одной подсети, будет рассмотрена отдельно (см. *Заключение* ниже).

2. Настройка маршрутизации

В этом примере мы будем использовать протокол BGP для динамической маршрутизации. Настройка других протоколов динамической маршрутизации выполняется аналогично.

Анонсируем в BGP все четыре адреса пула (четыре префикса с маской `/32`). Список префиксов `snat` отбирает их одной записью для всей подсети пула. BGP на узле должен быть уже запущен командой `routing bgp asn` и иметь соседей (см. *Настройка динамической маршрутизации*):

```
$$ configuration
## routing prefix-list snat seq 5 permit 192.168.12.20/30 le 32
## routing route-map snat permit 10 match-prefix-list snat
## routing bgp redistribute connected route-map snat
```

Настройку BGP-соседей опустим для краткости (подробнее о настройке BGP см. *BGP-маршрутизация*).

Примечание

На представленной выше схеме BGP-соседом должен стать маршрутизатор Internal router, так как трафик от серверов будет возвращаться через него.

Убедитесь, что BGP-сосед получил четыре префикса `/32` из подсети `192.168.12.20/30`, например командой `show ip bgp` на маршрутизаторе Internal router.

3. Настройка правил балансировки

Для распределения клиентов по адресам из пула можно использовать различные модули, например Geo, Geo IP, Map, Split Clients. Рассмотрим несколько типовых сценариев с описанием используемых модулей.

Сценарий A: использование модуля Split Clients

Стандартная ситуация, когда на Angie ADC попадают подключения пользователей из интернета напрямую. Предполагается, что пользователи распределяются равномерно по всему пространству адресов. В этом случае для настройки можно использовать модуль Split Clients (применяется в контексте `http`). `split_clients` работает как при L7-, так и при L4-балансировке.

Пример конфигурации:

```
split_clients "${remote_addr}AAA" $variant {
    25% 192.168.12.20;
    25% 192.168.12.21;
    25% 192.168.12.22;
    25% 192.168.12.23;
}
```

Примечание

К адресу клиента добавлен текст `AAA`. Это нужно для изменения значения, выдаваемого хэш-функцией. Если потребуется поменять распределение клиентов по адресам из пула, можно поменять добавляемый текст.

Сценарий B: использование модуля Map

Возможна ситуация, когда перед Angie ADC с точки зрения трафика, идущего от клиентов, расположен другой балансировщик:

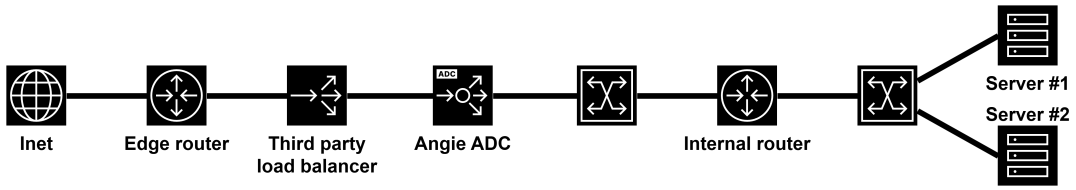


Рис. 2

Если этот балансировщик использует SNAT-пул, то переменная `remote_addr` может не обеспечить достаточного разнообразия. Это может привести к коллизиям — перекосу в распределении клиентов по адресам из пула SNAT. Решить указанную проблему можно, например, используя модуль Map, с помощью которого можно в явном виде задать соответствие «старого» и «нового» адресов отправителя. Метод `map` работает как при L7-, так и при L4-балансировке.

Пример конфигурации (восемь адресов из предыдущего пула привязываются к четырем адресам пула SNAT):

```
map $remote_addr $variant {
    "10.10.10.0" "192.168.12.20";
    "10.10.10.1" "192.168.12.20";
    "10.10.10.2" "192.168.12.21";
    "10.10.10.3" "192.168.12.21";
    "10.10.10.4" "192.168.12.22";
    "10.10.10.5" "192.168.12.22";
    "10.10.10.6" "192.168.12.23";
    "10.10.10.7" "192.168.12.23";
}
```

Сценарий C: модуль Split Clients и хэш переменной $request_id

Для балансировки HTTP-трафика можно использовать подход, при котором не важно, используется ли какой-либо NAT/PAT или прокси между реальным клиентом и Angie ADC. Для распределения клиентов будет использоваться модуль Split Clients и хэш от переменной `$request_id`. Значение переменной генерируется автоматически и, по сути, является случайным числом. Этот метод имеет ограниченную область применения — L7-балансировка для протокола HTTP.

Пример конфигурации:

```
split_clients "${request_id}" $variant {
    25% 192.168.12.20;
    25% 192.168.12.21;
    25% 192.168.12.22;
    25% 192.168.12.23;
 }
```

Примечание

При использовании этого метода разные сессии одного и того же клиента могут привязываться к различным адресам из пула. Это не должно быть большой проблемой, так как современные веб-системы используют заголовок `X-Forwarded-For` для определения адреса клиента и не смотрят на адрес отправителя в IP-пакете.

Теперь с помощью директивы proxy_bind укажем, где и как использовать указанное распределение клиентов. Директиву можно задать в контекстах `http`, `server` или `location`.

Пример:

```
location / {
proxy_pass http://backend ;
proxy_bind ${variant};
}
```

Заключение

Предложенные выше способы ручного создания SNAT-пула позволят уверенно перешагнуть ограничение в 65000 одновременных сессий как для L4-, так и для L7-балансировки. Однако следует все же понимать, что ограничение количества одновременно поддерживаемых сессий зависит не только от количества сокетов, но и от объемов использования целого ряда других системных ресурсов.

Чтобы адаптировать используемый подход к ситуации, когда один из интерфейсов Angie ADC расположен в одной подсети с апстрим-серверами, потребуется следующее:

- не использовать динамическую маршрутизацию;
- настроить адреса из пула на физическом интерфейсе, а не на loopback-интерфейсе (адреса должны быть из той же IP-подсети, в которой расположены серверы);
- для обеспечения отказоустойчивости можно использовать несколько Angie ADC, а для каждого IP-адреса из пула создать отдельную *группу VRRP* (со своим VRID) на интерфейсе в подсети серверов, вместо того чтобы назначать адреса непосредственно на физический интерфейс.

Настройка Transparent Proxy для TCP- и UDP-трафика

Angie ADC работает как обратный прокси для TCP- и UDP-трафика. Апстрим-серверы видят, что весь трафик приходит с IP-адреса самого прокси Angie ADC:

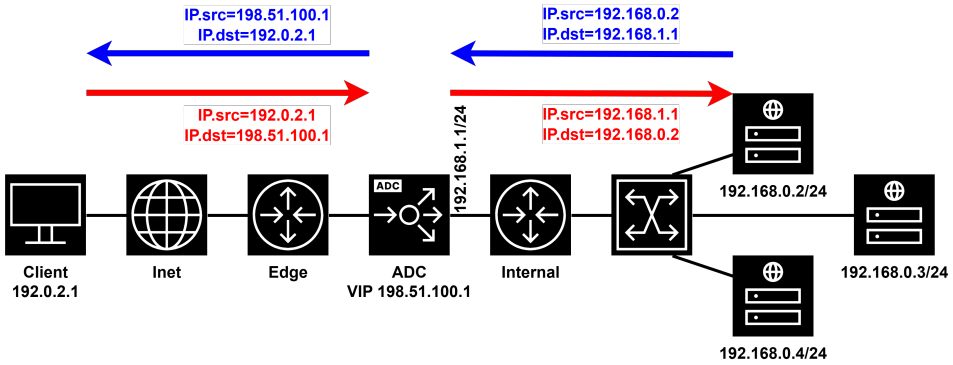


Рис. 1: красным цветом обозначен поток трафика от клиента к сервису, синим — обратный трафик.

Для определения и передачи настоящего IP-адреса клиента апстрим-серверу доступны следующие два метода:

- *IP Transparency* — апстрим-серверы видят соединение как исходящее от реального клиента (для TCP- и UDP-трафика).
- *Direct Server Return (DSR)* — дополнительно позволяет отправлять ответы от апстрим-серверов напрямую клиентам, минуя промежуточный балансировщик (только для UDP-трафика). Метод может быть реализован через NAT.

IP Transparency

При использовании IP Transparency апстрим-серверы будут видеть настоящий IP-адрес клиента, с которого приходят пакеты. IP Transparency может использоваться как с TCP-, так и с UDP-протоколами.

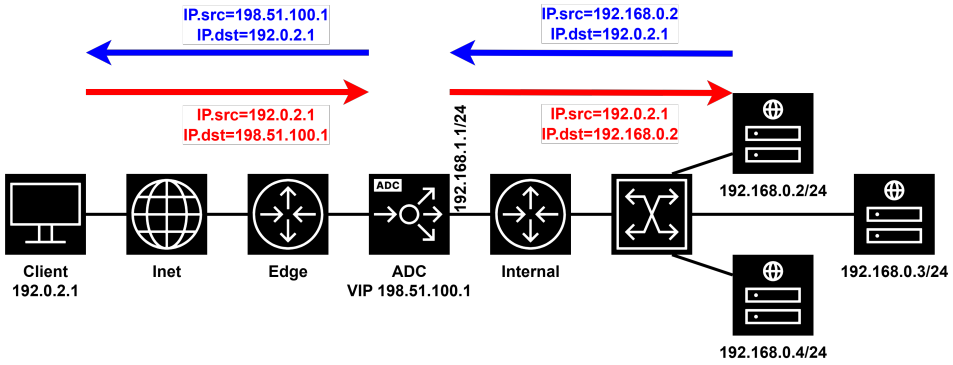


Рис. 2: пример сети, в которой на системе балансировки Angie ADC включена опция IP Transparency.

Предусловия

Должно выполняться одно из следующих условий:

- Балансировщик и апстрим-серверы находятся в одной подсети, балансировщик является маршрутизатором по умолчанию (default gateway) для апстрим-серверов.
- Балансировщик находится на пути передачи трафика между клиентом и апстрим-серверами (трафик проходит через балансировщик в обоих направлениях).

Пример настройки балансировщика

```
# in the 'http' context
upstream http_upstreams {
     server 192.168.0.2;
     server 192.168.0.3;
     server 192.168.0.4;
}

server {
    listen 80;

    location / {
        proxy_bind $remote_addr transparent;
        proxy_pass http://http_upstreams;
    }
}
```

В этом примере:

- Настроен простой виртуальный HTTP-сервер, распределяющий трафик между группой апстрим-серверов.
- Исходный адрес для трафика, направляемого на апстрим-серверы, подменяется с помощью параметра `transparent` в директиве adc__proxy_bind. Чаще всего в качестве исходного адреса указывается адрес удаленного клиента.

Настройка маршрутизации

При использовании IP Transparency трафик должен проходить через Angie ADC и обрабатываться им. Для этого необходимо настроить корректную маршрутизацию.

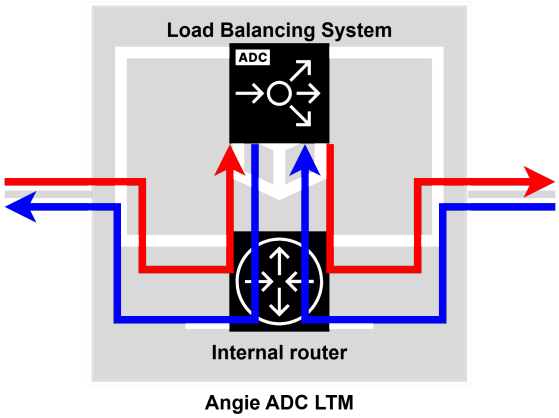


Рис. 3: движение трафика через Angie ADC с настроенным IP Transparency.

Маршрутизация настраивается на основе политик PBR (Policy-Based Routing) в веб-интерфейсе Angie ADC на странице `Система` → `Сетевые настройки` (см. *Настройка маршрутизации*): весь трафик от апстрим-серверов направляется в отдельную таблицу маршрутизации, в которой есть только локальный маршрут. Так ответы апстрим-серверов, адресованные IP-адресам клиентов, принимаются узлом Angie ADC и передаются обратно через прокси.

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, через который проходит трафик к апстрим-серверам.
3. Добавьте локальный маршрут для всего трафика в отдельной таблице:
    1. В блоке `Маршруты` нажмите `Добавить маршрут`.
    2. В поле `Сеть назначения` укажите `0.0.0.0/0`.
    3. В поле `Тип` выберите `Локальный`.
    4. В поле `Интерфейс` оставьте значение `Без интерфейса`.
    5. В поле `Таблица` укажите номер таблицы маршрутизации, например `100`.
4. Добавьте правила, по которым весь трафик с апстрим-серверов обрабатывается с помощью таблицы маршрутизации `100`. Для каждого апстрим-сервера:
    1. В блоке `Правила маршрутизации` нажмите `Добавить правило`.
    2. В поле `Сеть источника` укажите адрес апстрим-сервера, например `192.168.0.2/32`.
    3. В поле `Таблица` укажите `100`.

    В нашем примере нужны три правила: для `192.168.0.2/32`, `192.168.0.3/32` и `192.168.0.4/32`. Вместо добавления отдельных серверов можно добавить одно правило для подсети, если это необходимо (например, `10.21.20.0/24`).
5. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.
6. Повторите настройку на каждом узле кластера, через который проходит этот трафик.

Чтобы проверить результат, подключитесь к *интерфейсу командной строки* на порту 2222 и убедитесь, что трафик с апстрим-серверов обрабатывается в таблице `100` и что в этой таблице есть только один маршрут — весь трафик уходит в локальный интерфейс `lo`:

```
$ ip rule
0:      from all lookup local
32764:  from 192.168.0.2 lookup 100
32765:  from 192.168.0.3 lookup 100
32766:  from 192.168.0.4 lookup 100
32767:  from all lookup main
32768:  from all lookup default
```

```
$ ip route show table 100
local default dev lo scope host
```

Приоритеты правил в выводе могут отличаться.

Direct Server Return (DSR)

> **Примечание**
>
> Применение DSR возможно только для UDP-трафика.

При использовании Direct Server Return (DSR) апстрим-серверы будут видеть настоящий IP-адрес клиента, с которого приходят пакеты, и будут отправлять ответ непосредственно удаленному клиенту (т. е. пакеты с ответом полностью обходят балансировщик нагрузки). DSR может дать небольшой прирост производительности:

- Позволяет не удерживать открытыми UDP-сокеты в ожидании пакета ответа (повышает масштабируемость).
- Пакеты с ответами могут полностью обходить L7-обработку (снижает задержку).

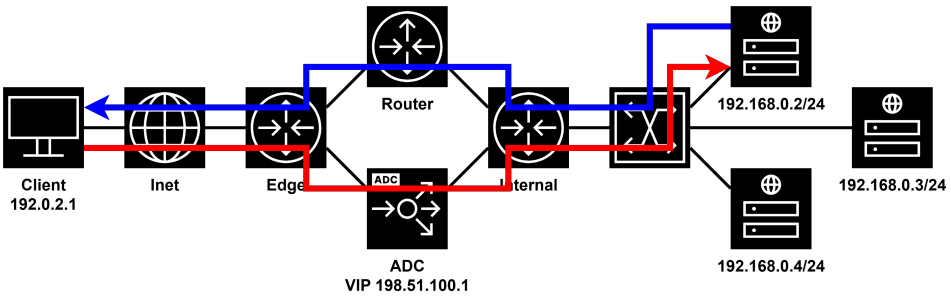


Рис. 4: движение трафика через Angie ADC с DSR.

Ограничения при использовании DSR:

- Балансировщик нагрузки не видит пакетов с ответами, поэтому не может определить, отвечает ли апстрим-сервер или вышел из строя.
- Балансировщик не может анализировать запрос глубже первого пакета, чтобы выбрать апстрим-сервер, поэтому его возможности по принятию решений о балансировке (например, маршрутизация на основе содержимого) ограничены.
- Балансировщик не может участвовать в процессах согласования или обработке состояний, таких как SSL/TLS.
- Такие функции, как кэширование и логирование, недоступны при использовании DSR.

Кроме того, при использовании DSR необходимо:

- переписывать исходный адрес ответа, чтобы он соответствовал публичному адресу балансировщика нагрузки;
- настроить активные проверки для апстрим-серверов.

Пример настройки балансировщика

```
# in the 'stream' context
server {
    listen 53 udp;
```

```
    proxy_bind $remote_addr:$remote_port transparent;
    proxy_responses 0;
    #proxy_timeout 1s;
}

upstream dns_upstreams {
    server 192.168.0.2:53;
    server 192.168.0.3:53;
    server 192.168.0.4:53;
}
```

В этом примере:

- Создан кластер из трех DNS-серверов с балансировкой нагрузки. Каждый из DNS-серверов должен возвращать разные IP-адреса при запросах `www.example.com`.
- Настроена простая конфигурация обратного прокси, которая распределяет нагрузку между этими DNS-серверами.
- Параметр `transparent` в директиве `proxy_bind` позволяет апстрим-серверу видеть исходный IP-адрес и порт (переменные `$remote_addr` и `$remote_port`).
- Балансировщик не ожидает ответ от апстрим-серверов (директива `proxy_responses=0`). Ответ будет отправлен клиенту напрямую.

Переписывание IP-адреса и порта при ответе

Апстрим-сервер генерирует ответные пакеты, в которых в качестве исходного адреса используется его локальный IP-адрес. Этот исходный адрес необходимо переписать на IP-адрес и порт балансировщика нагрузки, к которому изначально подключался клиент. Есть два способа для переписывания исходящих пакетов:

- Router NAT — переписывание на промежуточном маршрутизаторе.
- Origin NAT — переписывание при отправке пакетов с каждого апстрим-DNS-сервера.

Router NAT

Вы можете изменять (переписывать) исходящие пакеты на промежуточном маршрутизаторе, который является маршрутом по умолчанию для апстрим-серверов.

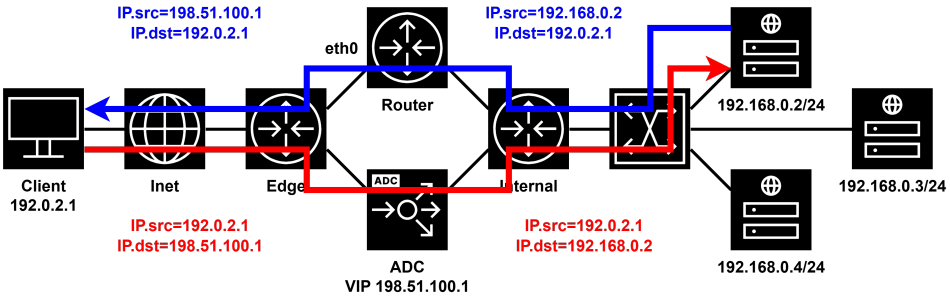


Рис. 5: движение трафика с Router NAT

Для этого настройте на маршрутизаторе stateless NAT-переписывание:

Например:

```
# tc qdisc add dev eth0 root handle 10: htb
# tc filter add dev eth0 parent 10: protocol ip prio 10 u32 match ip src 192.168.0.2␣
↪match ip sport 53 action nat egress 192.168.0.2 198.51.100.1
# tc filter add dev eth0 parent 10: protocol ip prio 10 u32 match ip src 192.168.0.3␣
↪match ip sport 53 action nat egress 192.168.0.3 198.51.100.1
```

```
# tc filter add dev eth0 parent 10: protocol ip prio 10 u32 match ip src 192.168.0.4␣
↪match ip sport 53 action nat egress 192.168.0.4 198.51.100.1
```

Убедитесь, что вы указали корректный исходящий интерфейс (например, `eth0`) и правильные IP-адреса для каждого апстрим-сервера. В зависимости от конфигурации можно сократить количество команд `tc filter`, объединив их с помощью CIDR-масок для параметров `src` и `egress old`.

Чтобы вывести текущую конфигурацию `tc filter`, выполните:

```
# tc filter show dev eth0
```

Origin NAT

Вариант с переписыванием исходящих пакетов при их отправке с каждого апстрим-DNS-сервера применим, если у вас есть возможность настраивать сеть на апстрим-серверах, особенно если они напрямую подключены к интернету.

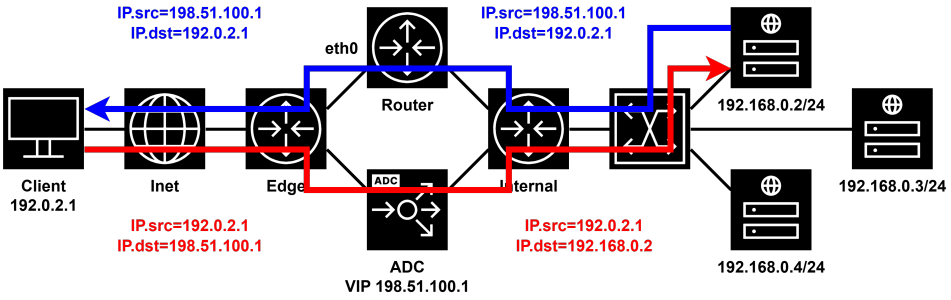


Рис. 6: движение трафика с Origin NAT

Необходимо настроить stateless NAT-переписывание на каждом апстрим-сервере.

Пример:

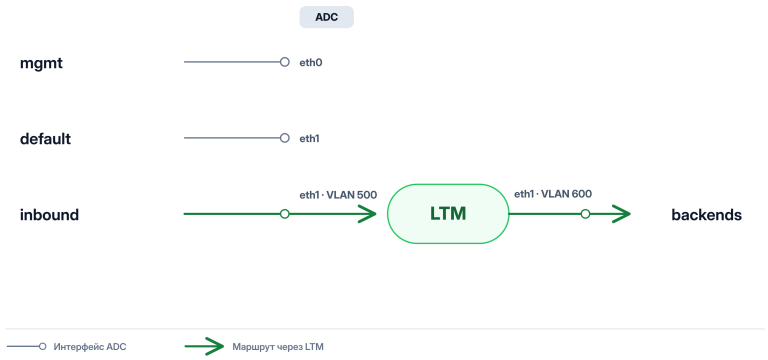
```
# tc qdisc add dev eth0 root handle 10: htb
# tc filter add dev eth0 parent 10: protocol ip prio 10 u32 match ip src 192.168.0.2␣
↪match ip sport 53 action nat egress 192.168.0.2 198.51.100.1
```

Такую конфигурацию необходимо применить на каждом апстрим-сервере, убедившись, что выбран корректный интерфейс и корректные IP-адреса.

Изоляция внешнего трафика и проксирование во внутреннюю сеть

Изоляцию внешнего трафика и его проксирование во внутреннюю сеть можно настроить с помощью *доменов маршрутизации*. Внешний клиентский трафик принимается в отдельном домене маршрутизации, а бэкенды размещаются в другом домене, созданном специально для них. Клиенты попадают к бэкендам только через балансировщик Angie ADC: балансировщик принимает соединение во внешнем домене маршрутизации и проксирует запрос во внутренний домен.

Пример



Зеленым цветом обозначен путь клиентского трафика через балансировщик Angie ADC.

В примере используются следующие домены маршрутизации:

- `mgmt` — предустановленный домен для управления узлом, в примере он не меняется;
- `default` — общая сеть узла (в веб-интерфейсе — значение `По умолчанию`);
- `inbound` — домен для внешнего клиентского трафика;
- `backends` — домен для внутреннего трафика и бэкендов.

Трафик между доменами маршрутизации не передается, поэтому клиент из `inbound` не может обратиться к бэкендам напрямую. Домен `backends` также недоступен напрямую из общей сети узла, если для него не настроены *утечки маршрутов*.

Оба домена маршрутизации (`inbound` и `backends`) подключены к узлу через VLAN-интерфейсы (VLAN 500 для `inbound` и VLAN 600 для `backends`) на одном физическом интерфейсе. Виртуальный сервер принимает клиентские соединения на IP-адресе, назначенном для `vl500`.

Настройка

1. Перейдите в раздел `Система` → `Сетевые настройки` и выберите узел, для которого будет проводиться настройка.
2. В блоке `Домены маршрутизации` нажмите `Добавить домен маршрутизации` и добавьте домены маршрутизации `inbound` и `backends` (см. *Добавление домена маршрутизации*).
3. В блоке `Интерфейсы` нажмите `Добавить интерфейс` и добавьте *VLAN-интерфейсы* для созданных доменов маршрутизации. Для обоих интерфейсов укажите один и тот же родительский физический интерфейс:
   - `vl500` — VLAN ID внешней сети, домен маршрутизации `inbound` и IPv4-адрес, на котором виртуальный сервер будет принимать клиентские соединения;
   - `vl600` — VLAN ID сети бэкендов, домен маршрутизации `backends` и IPv4-адрес в сети бэкендов.
4. В блоке `Маршруты` нажмите `Добавить маршрут` и добавьте маршрут по умолчанию для каждого домена маршрутизации:

Сеть назначения	Тип	Шлюз	Интерфейс
`0.0.0.0/0`	`Обычный`	IP-адрес шлюза	`vl500`
`0.0.0.0/0`	`Обычный`	IP-адрес шлюза	`vl600`

Поле `Таблица` оставьте пустым: маршруты относятся к доменам маршрутизации своих интерфейсов, поэтому два маршрута по умолчанию не конфликтуют.

5. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.
6. Повторите настройку на каждом узле кластера, который принимает этот трафик.
7. В *конфигурации балансировщика* привяжите виртуальный сервер к домену `inbound`, а соединения с бэкендами — к домену `backends`.

```
# in the 'http' context
upstream app_servers {
    server backend1;
    server backend2;
}

server {
    listen VIP:80 interface=inbound;

    location / {
        proxy_interface backends;
        proxy_pass http://app_servers;
    }
}
```

   В этом примере:

   - `VIP` — IP-адрес, назначенный интерфейсу `vl500`.
   - Параметр `interface=inbound` директивы listen привязывает слушающий сокет к домену маршрутизации `inbound`: виртуальный сервер принимает соединения только из этого домена маршрутизации.
   - Директива adc__proxy_interface направляет соединения с бэкендами через домен маршрутизации `backends`: адреса бэкендов ищутся в таблице маршрутизации этого домена.
8. Проверьте результат:
   - запрос клиента из внешней сети к `VIP` возвращает ответ бэкенда, например `curl http://VIP/`;
   - адреса бэкендов из внешней сети недоступны.

3.3.6.2 TLS и сертификаты

Примеры настройки TLS в Angie ADC: выпуск и обновление сертификатов и балансировка на основе параметров TLS-соединения.

- *Настройка ACME*
- *Балансировка трафика на основе набора шифров*

Настройка ACME

Модуль ACME в Angie ADC обеспечивает автоматическое получение сертификатов с использованием протокола ACME. Протокол ACME предусматривает несколько способов проверки доменов (также используется термин *верификация*); модуль реализует *HTTP-проверку*, *DNS-проверку*, *ALPN-проверку*, а также *проверку с помощью хуков* через самостоятельно реализуемый внешний сервис.

Шаги настройки

Общие шаги для включения запроса сертификатов в конфигурации:

- **Настройте ACME-клиент** в блоке `http` с помощью директивы adc__acme_client, задающей уникальное имя клиента и другие параметры; можно настроить несколько клиентов ACME.

- **Укажите домены, для которых запрашиваются сертификаты**: для доменных имен, перечисленных во всех директивах adc__server_name всех блоков `server` с директивами adc__acme, указывающими на один и тот же ACME-клиент, будет выдан единый сертификат.

  IP-адреса (IPv4 или IPv6), указанные в adc__server_name, также являются допустимыми идентификаторами сертификата, за исключением DNS-проверки.

  Обратите внимание: публичные центры сертификации могут выдавать сертификаты для IP-адресов только в рамках определенных профилей сертификатов; например, Let's Encrypt в настоящее время требует профиль, допускающий IP-идентификаторы (см. документацию по профилям). Чтобы запросить такой профиль, задайте параметр `profile=` директивы adc__acme_client.

- **Настройте обработку запросов и вызовов ACME**: это нужно для проверки владения доменом. Способ настройки зависит от способа проверки доменных имен:

Способ	Требования к пользователю	Мультидомены	Домены со звездочкой
HTTP-проверка	Открыть порт 80 (или указанный в adc__acme_http_port) для входящих соединений на сервере Angie.	✓	
DNS-проверка	Открыть порт 53 (или указанный в adc__acme_dns_port) для входящих соединений на сервере Angie. Настроить NS-запись для поддомена `_acme-challenge.`, направив ее на свой сервер Angie.	✓	✓
ALPN-проверка	Открыть порт 443 для входящих соединений; ACME-сервер подключается только к этому порту.	✓	
Проверка хуками	Реализовать внешний сервис (скрипт или приложение), который по команде Angie сможет внести изменения в DNS-зону или разместить специальный ответ на веб-сервере.	✓	✓

  Задайте тип проверки параметром `challenge=` директивы adc__acme_client: `http` (по умолчанию), `dns` или `alpn`. Для проверки хуками укажите `challenge=http` или `challenge=dns` (для доменов со звездочкой нужен `dns`) и добавьте именованный `location` с директивой adc__acme_hook.

- **Настройте SSL с использованием полученного сертификата и ключа**: Модуль делает сертификаты и ключи доступными в виде встроенных переменных, которые можно использовать в конфигурации для заполнения adc__ssl_certificate и adc__ssl_certificate_key.

Совет

Процесс получения и обновления сертификатов зависит от работы многих служб и может занимать какое-то время. Запаситесь терпением, а в случае возникновения проблем или сомнений обратитесь к *отладочному логу*.

Подробности реализации

По умолчанию ключи и сертификаты клиентов хранятся в кодировке PEM в `/var/lib/angie/acme`. Это местоположение можно переопределить на `/var/transfer/acme` с помощью директивы `acme_client_path`:

```
$ ls /var/transfer/acme/example/

  account.key  certificate.pem  private.key
```

Предупреждение

При хранении сертификатов в `/var/transfer` их возможно перезаписать.

Примечание

Эти файлы сохраняются на диске между перезапусками. При запуске клиент повторно использует сохраненный сертификат, если тот еще действителен, вместо запроса нового, что устраняет задержку на выпуск и лишние обращения к серверу CA, на которые могут действовать ограничения частоты запросов.

Примечание

Перезагрузка конфигурации заново сверяет каждый клиент ACME с сертификатами, сохраненными на диске. Клиент, сертификат которого в данный момент недействителен (в том числе если его предыдущий запрос завершился ошибкой), запрашивается заново немедленно, независимо от retry_after_error. Задержка перед повторной попыткой (как и значение `retry_after_error=off`) действует, только пока Angie работает, и не сохраняется после перезагрузки. Поэтому повторные перезагрузки при постоянно неудачных запросах могут приводить к частым обращениям к серверу CA, на которые действуют упомянутые выше ограничения частоты запросов.

Клиенту ACME требуется учетная запись на сервере CA. Для ее создания и управления ею клиент использует закрытый ключ (`account.key`); если ключа у него еще нет, ключ создается при запуске. Затем клиент использует его для регистрации учетной записи на сервере.

Примечание

Если у вас уже есть ключ учетной записи, поместите его в подкаталог клиента перед запуском для повторного использования учетной записи. Файл ключа также можно указать с помощью параметра `account_key` в adc__acme_client.

Некоторые CA требуют привязать учетную запись ACME к уже существующей внешней учетной записи с помощью External Account Binding (EAB), прежде чем выпускать сертификаты. Для этого задайте параметр `eab` директивы adc__acme_client, указав идентификатор ключа и MAC-ключ, предоставленные CA; точный синтаксис приведен в описании директивы.

Клиент ACME также использует отдельный ключ (`private.key`) для запросов на подпись сертификата (CSR); если нужно, этот ключ сертификата также создается автоматически при запуске.

При запуске клиент запрашивает сертификат, если его еще нет, подписывая и отправляя CSR для всех доменов, которыми он управляет, серверу CA. Сервер проверяет владение доменом путем HTTP- или DNS-проверки и выдает сертификат, который клиент сохраняет локально (`certificate.pem`).

Как сказано выше, сертификат будет единым для всех доменных имен, для которых используется один и тот же ACME-клиент, то есть потенциально может быть мультидоменным. Список всех имен, для которых выдан сертификат, см. в разделе *Subject Alternative Name* (SAN) полученного сертификата. Проверить его можно в командной строке, например:

```
$ openssl x509 -in certificate.pem -noout -text | grep -A5 "Subject Alternative Name"
```

Когда приближается завершение срока действия сертификата или изменяется список доменов, клиент подписывает и отправляет еще один CSR на сервер CA. Сервер снова проверяет владение и выдает новый сертификат, который клиент устанавливает локально, заменяя предыдущий.

В конфигурации полученный сертификат и соответствующий ключ доступны через префиксные переменные adc__v_acme_cert_name и adc__v_acme_cert_key_name. Их значения — содержимое соответствующих файлов, которое следует использовать с директивами adc__ssl_certificate и adc__ssl_certificate_key, например:

```
server {

    listen 443 ssl;

    server_name example.com www.example.com;
    acme example;

    ssl_certificate $acme_cert_example;
    ssl_certificate_key $acme_cert_key_example;
}
```

Примечание

Клиент ACME определяет адрес сервера CA по его имени через adc__resolver того же контекста, который по умолчанию обращается к DNS-серверам из `/etc/resolv.conf`; задавайте директиву явно, только если нужны другие серверы или параметры. На узле без поддержки IPv6 resolver может все равно отправлять AAAA-запросы (IPv6) для сервера CA и не суметь подключиться; отключите их параметром `ipv6=off`, например `resolver conf ipv6=off;`.

Сбор доменов и использование сертификата

Директива adc__acme служит только для сбора доменных имен для запросов сертификатов. Она не определяет, где можно использовать сертификат: любой блок `server` может ссылаться на полученный сертификат через переменную $acme_cert_<имя>, независимо от того, содержит ли блок директиву `acme`.

Например, если у вас есть блок `server` с маской, который уже охватывает все поддомены, дополнительные блоки `server` для конкретных поддоменов не нуждаются в директиве `acme`:

```
http {

    acme_client example https://acme-v02.api.letsencrypt.org/directory
        challenge=dns;

    # В этом блоке перечислены домены для запроса сертификата
    server {

        listen 443 ssl;

        server_name example.com *.example.com;
        acme example;
```

```
        ssl_certificate $acme_cert_example;
        ssl_certificate_key $acme_cert_key_example;
    }

    # Этот блок использует тот же сертификат, но не добавляет
    # свой server_name в запрос на сертификат
    server {

        listen 443 ssl;

        server_name app.example.com;

        ssl_certificate $acme_cert_example;
        ssl_certificate_key $acme_cert_key_example;
    }
}
```

Явный список доменов

Чтобы точно контролировать набор доменных имен в сертификате, не полагаясь на автоматический сбор из всех блоков `server`, создайте отдельный блок `server`, содержащий только директивы adc__server_name и adc__acme. Чтобы этот блок не обрабатывал реальный трафик, привяжите его к Unix-сокету:

```
# Отдельный блок, определяющий список доменов сертификата
server {

    listen unix:/tmp/acme_example.sock;

    server_name example.com www.example.com;
    acme example;
}
```

Другие блоки `server` могут затем использовать сертификат через переменную $acme_cert_<имя>, не влияя на то, какие домены запрашиваются.

Один сертификат для связанных доменов

Если пользователи переходят между связанными доменами, например `example.com` и `www.example.com`, мы рекомендуем охватить их одним сертификатом. Тогда браузер может отправлять запросы ко второму домену через соединение, открытое для первого, если оба имени разрешаются в один и тот же адрес (объединение соединений). Объединение работает по HTTP/2, который включается директивой adc__http2, и избавляет браузер от нового соединения и TLS-рукопожатия.

Здесь директивы adc__acme обоих блоков `server` указывают на один клиент, поэтому его сертификат охватывает оба имени; первый блок только перенаправляет `www.example.com` на `example.com`:

```
http {

    acme_client example https://acme-v02.api.letsencrypt.org/directory;
    http2 on;

    # Перенаправляет www.example.com на example.com
    server {

        listen 443 ssl;

        server_name www.example.com;
```

```
        acme example;

        ssl_certificate $acme_cert_example;
        ssl_certificate_key $acme_cert_key_example;

        return 301 https://example.com$request_uri;
    }

    # Обслуживает сайт
    server {

        listen 443 ssl;

        server_name example.com;
        acme example;

        ssl_certificate $acme_cert_example;
        ssl_certificate_key $acme_cert_key_example;
    }
}
```

Отдельные сертификаты для разных доменов

Каждый adc__acme_client управляет одним сертификатом. Чтобы получить несколько независимых сертификатов (например, для несвязанных доменов, которым не следует использовать общий сертификат), настройте отдельный adc__acme_client для каждого из них в блоке `http` и укажите в директиве adc__acme каждого блока `server` соответствующий клиент по имени:

```
http {

    # Два независимых клиента, каждый управляет своим сертификатом
    acme_client shop https://acme-v02.api.letsencrypt.org/directory
        challenge=http;

    acme_client blog https://acme-v02.api.letsencrypt.org/directory
        challenge=http;

    server {

        listen 443 ssl;

        server_name shop.example.com www.shop.example.com;
        acme shop;

        ssl_certificate $acme_cert_shop;
        ssl_certificate_key $acme_cert_key_shop;
    }

    server {

        listen 443 ssl;

        server_name blog.example.com;
        acme blog;

        ssl_certificate $acme_cert_blog;
        ssl_certificate_key $acme_cert_key_blog;
```

```
    }
}
```

> **Совет**
>
> Если клиентов много, мы рекомендуем держать каждую директиву `acme_client` в том же подключаемом файле (или шаблоне), что и использующие ее блоки `server`: тогда клиент и его домены редактируются вместе. Называйте клиент по основному домену, заменяя точки и дефисы символами подчеркивания (`shop_example_com`; правила для имен см. в описании adc__acme_client), по обслуживаемому сервису или по имени файла.

HTTP-проверка

Проверка выполняется автоматически. Когда Angie заказывает сертификат, ACME-сервер запрашивает по HTTP файл-токен по адресу `/.well-known/acme-challenge/<TOKEN>`. Angie отвечает на такие запросы сам, поэтому отдавать этот путь вручную не требуется. Получив файл, ACME-сервер сверяет токен с выданным значением и, если они совпадают, засчитывает проверку домена.

Пример конфигурации

Здесь ACME-клиент с именем `example` управляет сертификатами для `example.com` и `www.example.com` (учтите, что wildcard-сертификаты не поддерживаются при HTTP-проверке):

```
http {

    acme_client example https://acme-v02.api.letsencrypt.org/directory;

    server {

        listen 80; # Не обязательно: если порт HTTP-проверки
                   # никто не слушает, модуль откроет его сам
                   # (см. директиву 'acme_http_port')

        listen 443 ssl;

        server_name example.com www.example.com;
        acme example;

        ssl_certificate $acme_cert_example;
        ssl_certificate_key $acme_cert_key_example;
    }
}
```

Как уже отмечалось, порт 80 должен быть открыт для приема вызовов ACME по HTTP. Если ни один сервер не слушает порт HTTP-проверки, модуль создает отдельный слушающий сокет на порту 80 (или указанном в adc__acme_http_port). Отдельный блок adc__server не требуется.

DNS-проверка

Проверка выполняется автоматически, но требует настройки DNS с вашей стороны. Когда Angie заказывает сертификат, ACME-сервер отправляет DNS-запрос TXT-записи в поддомене `_acme-challenge.` проверяемого домена. Angie отвечает на такие запросы сам: он выступает авторитетным сервером имен для этого поддомена и возвращает TXT-запись с тем значением, которого ждет ACME-сервер. ACME-сервер сверяет полученную запись с выданным значением и, если они совпадают, засчитывает проверку домена.

Чтобы запрос дошел до Angie, DNS вашего домена должен делегировать поддомен `_acme-challenge.` серверу Angie; нужные записи приведены ниже. По умолчанию Angie отвечает с очень небольшим TTL, а некоторые DNS-провайдеры отфильтровывают ответы с таким низким TTL — если проверка не завершается, увеличьте его директивой adc__acme_dns_ttl.

DNS-проверка подтверждает контроль над доменным именем, поэтому не может проверять идентификаторы в виде IP-адресов: для клиента с `challenge=dns` Angie игнорирует IP-адрес в adc__server_name и выводит предупреждение при запуске. Блок `server`, в котором указан IP-адрес, должен по-прежнему содержать хотя бы одно доменное имя, которое клиент может проверить.

Примечание

Сервер Angie должен быть доступен из интернета на UDP-порту 53 (или указанном в adc__acme_dns_port). Если сервер находится за межсетевым экраном, убедитесь, что этот порт открыт для входящих соединений.

Например, чтобы подтвердить домен `example.com`, используя сервер Angie с IP-адресом `203.0.113.10`, DNS-конфигурация вашего домена должна включать следующие записи:

```
_acme-challenge.example.com. 60    IN      NS       ns.example.com.
            ns.example.com. 60    IN       A       203.0.113.10
```

Эта конфигурация делегирует разрешение DNS для `_acme-challenge.example.com` на `ns.example.com`, обеспечивая доступность `ns.example.com` путем сопоставления с IP-адресом (`203.0.113.10`).

Предупреждение

Распространение изменений NS-записей может занимать от нескольких минут до 48 часов в зависимости от TTL и DNS-провайдера. Рекомендуется проверить корректность настройки перед запросом сертификата.

Для проверки корректности настройки DNS можно использовать следующие команды:

```
$ dig NS _acme-challenge.example.com +short  # Проверка NS-записи для поддомена _acme-
↪challenge

  ns.example.com.

$ dig A ns.example.com +short  # Проверка A-записи для сервера имен

  203.0.113.10

$ nc -zv 203.0.113.10 53  # Проверка доступности DNS-сервера на порту 53
```

Этот способ позволяет запрашивать wildcard-сертификаты, например сертификат, включающий запись `*.example.com` в разделе *Subject Alternative Name* (SAN). Чтобы в явной форме запросить сертификат для поддомена, например `www.example.com`, следует отдельно подтвердить этот поддомен описанным выше способом.

Предупреждение

Применимость данного сценария во многом зависит от возможностей, предоставляемых вашим DNS-провайдером; некоторые провайдеры не позволяют выполнять такие настройки.

Пример конфигурации

В целом, конфигурация схожа с примером из предыдущего раздела. Нет необходимости в настройках, специфичных для HTTP; вместо этого достаточно установить `challenge=dns` для директивы adc__acme_client.

Здесь ACME-клиент с именем `example` управляет сертификатами для `example.com` и `*.example.com`:

```
http {

    acme_client example https://acme-v02.api.letsencrypt.org/directory
        challenge=dns;

    server {

        server_name example.com *.example.com;
        acme example;

        ssl_certificate $acme_cert_example;
        ssl_certificate_key $acme_cert_key_example;
    }
}
```

ALPN-проверка

Проверка работает автоматически. ACME-сервер устанавливает TLS-соединение и запрашивает через ALPN протокол `acme-tls/1`. Модуль отдает временный сертификат для валидационного запроса.

Чтобы использовать этот способ, задайте `challenge=alpn` в директиве adc__acme_client и убедитесь, что TLS-слушатель доступен на порту 443: ACME-сервер подключается только к этому порту. Если сервер слушает другой порт, на него нужно перенаправить внешний порт 443.

Пример конфигурации

Конфигурация аналогична предыдущим разделам; достаточно задать `challenge=alpn` для директивы adc__acme_client и убедиться, что TLS-сервер доступен на порту 443.

Здесь ACME-клиент с именем `example` управляет сертификатом для `example.com` и `www.example.com`:

```
http {

    acme_client example https://acme-v02.api.letsencrypt.org/directory
        challenge=alpn;

    server {

        listen 443 ssl;

        server_name example.com www.example.com;
        acme example;

        ssl_certificate $acme_cert_example;
        ssl_certificate_key $acme_cert_key_example;
    }
}
```

Проверка с помощью хуков

В отличие от предыдущих способов, эта проверка требует дополнительных усилий. Здесь ACME-сервер производит обычную HTTP-проверку или DNS-проверку, но обращается не к самому серверу Angie, а к внешнему сервису, которым сервер Angie управляет с помощью вызовов-хуков (adc__acme_hook). В свою очередь, этот сервис настраивает отдельный DNS- или HTTP-сервер, куда и направляются запросы ACME-сервера.

Получив ожидаемый ответ от настроенного таким образом DNS- или HTTP-сервера, ACME-сервер подтверждает, что домен принадлежит клиенту.

Когда для выпуска или обновления сертификата требуется проверка домена, Angie формирует внутренний запрос к именованному `location`, содержащему директиву adc__acme_hook. Способ обработки этого запроса полностью зависит от других директив, заданных в том же `location`.

Общая схема такова:

1. Создайте именованный `location` с директивой adc__acme_hook.
2. Настройте обработчик запроса в том же `location` с помощью модуля, подходящего для вашей конфигурации: adc__fastcgi_pass для FastCGI, adc__proxy_pass для HTTP.
3. Передайте обработчику переменные ACME с помощью поддерживаемого им механизма, например, `fastcgi_param` для FastCGI.

Обработчик должен возвращать код состояния `2xx`, который можно передать через заголовок `Status`. Любой другой код от хука `add` прерывает попытку обновления сертификата; от хука `remove` тот же код только записывается в журнал как предупреждение, и обновление продолжается. Вывод обработчика игнорируется.

Минимальная конфигурация

Независимо от используемого обработчика, `location` для хука имеет следующую структуру:

```
location @acme_hook_location {

    acme_hook example;

    # Директива обработчика (fastcgi_pass, proxy_pass, ...)
    # Передайте переменные ACME с помощью механизма обработчика:
    #   ACME_HOOK       - $acme_hook_name ("add" или "remove")
    #   ACME_CHALLENGE  - $acme_hook_challenge ("dns" или "http")
    #   ACME_DOMAIN     - $acme_hook_domain
    #   ACME_TOKEN      - $acme_hook_token
    #   ACME_KEYAUTH    - $acme_hook_keyauth
}
```

При DNS-проверке обработчик должен использовать `ACME_HOOK` для определения действия: если значение `add`, создать TXT-запись для `_acme-challenge.`*`ACME_DOMAIN`* со значением из `ACME_KEYAUTH`; если значение `remove`, удалить эту запись.

Пример с FastCGI

Здесь настраивается ACME-клиент `example` для подтверждения домена при помощи DNS-вызова, на что указывает параметр `challenge=dns` директивы adc__acme_client.

Блок `server` применяется ко всем поддоменам `example.com` (например, `*.example.com`) и использует ACME-клиент `example` для управления сертификатами, что указано в директиве adc__acme.

Именованный блок `location` обрабатывает вызовы хуков. Директива adc__acme_hook связывает его с ACME-клиентом `example`. Запросы хуков отправляются на локальный FastCGI-сервер на порту 9000 с помощью adc__fastcgi_pass. Директивы `fastcgi_param` передают переменные ACME во внешний сервис.

```
acme_client example https://acme-v02.api.letsencrypt.org/directory
    challenge=dns;

server {

    listen 80;

    server_name *.example.com;

    acme example;

    ssl_certificate $acme_cert_example;
    ssl_certificate_key $acme_cert_key_example;

    location @acme_hook_location {

        acme_hook example;

        fastcgi_pass localhost:9000;

        fastcgi_param ACME_CLIENT $acme_hook_client;
        fastcgi_param ACME_HOOK $acme_hook_name;
        fastcgi_param ACME_CHALLENGE $acme_hook_challenge;
        fastcgi_param ACME_DOMAIN $acme_hook_domain;
        fastcgi_param ACME_TOKEN $acme_hook_token;
        fastcgi_param ACME_KEYAUTH $acme_hook_keyauth;

        include fastcgi.conf;
    }
}
```

Пример соответствующего внешнего FastCGI-сервиса на Perl:

```
#!/usr/bin/perl

use strict; use warnings;

use FCGI;

my $socket = FCGI::OpenSocket(":9000", 5);
my $request = FCGI::Request(\*STDIN, \*STDOUT, \*STDERR, \%ENV, $socket);

while ($request->Accept() >= 0) {
    print "\r\n";

    my $client =    $ENV{ACME_CLIENT};
    my $hook =      $ENV{ACME_HOOK};
    my $challenge = $ENV{ACME_CHALLENGE};
    my $domain =    $ENV{ACME_DOMAIN};
    my $token =     $ENV{ACME_TOKEN};
    my $keyauth =   $ENV{ACME_KEYAUTH};

    if ($hook eq 'add') {

        DNS_set_TXT_record("_acme-challenge.$domain.", $keyauth);

    } elsif ($hook eq 'remove') {
```

```
        DNS_clear_TXT_record("_acme-challenge.$domain.");
    }
};

FCGI::CloseSocket($socket);
```

Здесь `DNS_set_TXT_record()` и `DNS_clear_TXT_record()` — функции, предположительно добавляющие и удаляющие TXT-записи в конфигурации некого внешнего DNS-сервера, к которому и обратится ACME-сервер. В этих записях должны содержаться переданные сервером Angie данные, что позволит внешнему DNS-серверу успешно пройти проверку, аналогичную описанной в разделе *DNS-проверка*. Подробности реализации таких функций выходят за рамки этого руководства; так, например, передавать параметры можно и через URI запроса:

```
# ...

location @acme_hook_location {

    acme_hook example uri=/acme_hook/$acme_hook_name?domain=$acme_hook_domain&key=
↪$acme_hook_keyauth;

    fastcgi_pass localhost:9000;

    fastcgi_param REQUEST_URI $request_uri;
    fastcgi_param ACME_CLIENT $acme_hook_client;
    fastcgi_param ACME_CHALLENGE $acme_hook_challenge;
    fastcgi_param ACME_TOKEN $acme_hook_token;

    include fastcgi.conf;
}
```

Пример с PHP-FPM

Еще один пример, с использованием PHP-FPM:

```
location @acme_hook_location {

    acme_hook example;
    root /var/www/dns;
    fastcgi_pass unix:/run/php-fpm/php-dns.sock;
    fastcgi_index hook.php;
    fastcgi_param SCRIPT_FILENAME /var/www/dns/hook.php;
    include fastcgi_params;

    fastcgi_param ACME_CLIENT $acme_hook_client;
    fastcgi_param ACME_HOOK $acme_hook_name;
    fastcgi_param ACME_CHALLENGE $acme_hook_challenge;
    fastcgi_param ACME_DOMAIN $acme_hook_domain;
    fastcgi_param ACME_TOKEN $acme_hook_token;
    fastcgi_param ACME_KEYAUTH $acme_hook_keyauth;
}
```

```
[dns]
listen = /run/php-fpm/php-dns.sock
listen.mode = 0666
user = angie
group = angie
chdir = /var/www/dns
```

```
# ...
```

Переданные параметры доступны в PHP через `$_SERVER['...']`.

ACME в потоковом модуле

Потоковый модуль ACME позволяет автоматизировать выпуск и использование сертификатов для TCP-трафика. Для его корректной работы необходимо сначала настроить HTTP-аналог: ACME-клиент должен быть объявлен в контексте `http`, а сам блок `stream` должен располагаться *после* блока `http` в конфигурации.

Пример конфигурации

По умолчанию для получения сертификатов используется режим HTTP-проверки. Как описано в разделе *HTTP-проверка*, ACME-сервер должен иметь доступ к порту 80; если на нем не слушает ни один HTTP-сервер, Angie открывает этот порт сам, поэтому сервер на порту 80 в этом примере необязателен:

```
# HTTP-часть
http {

    # ACME-клиент для потоковой части
    acme_client example https://acme-v02.api.letsencrypt.org/directory;

    # Необязателен: без него Angie сам открывает порт 80
    server {

        listen 80;
        return 444;
    }
}

# Потоковая часть
stream {

    server {

        listen 12345 ssl;
        proxy_pass backend_upstream;

        ssl_certificate $acme_cert_example;
        ssl_certificate_key $acme_cert_key_example;

        server_name example.com www.example.com;
        acme example; # ссылка на ACME-клиент, определенный в HTTP-части
    }

    upstream backend_upstream {

        server 127.0.0.1:54321;
    }
}
```

Также можно использовать DNS-проверку, настроив `challenge=dns` в директиве adc__acme_client; тогда порт 80 не используется.

Можно использовать и ALPN-проверку. При `challenge=alpn` проверочный запрос обрабатывает сам сервер stream, если он терминирует TLS с сертификатом и ключом из переменных клиента,

как в примере выше. ACME-сервер подключается только к порту 443, поэтому сервер stream должен принимать соединения на нем (`listen 443 ssl` вместо `12345`), а порт 80 не используется.

Балансировка трафика на основе набора шифров

В этой статье рассматривается балансировка трафика на основе набора шифров. На один VIP-адрес балансировщика нагрузки поступает два типа трафика:

- TLS-трафик с шифрованием ГОСТ;
- TLS-трафик без ГОСТ.

Для стандартного TLS выполняется Offload и балансировка на Angie ADC. Трафик ГОСТ направляется на отдельный бэкенд-сервер без расшифровки.

Настройка

Конфигурация основного бэкенд-сервера:

```
http {
    default_type text/plain;

    server {
        listen 80;
        server_name localhost;

        location / {
            return 200 "Hello, this is default backend\n";
        }
    }
}
```

Конфигурация бэкенд-сервера для ГОСТ-трафика:

```
http {
    default_type text/plain;

    server {
        listen 443 ssl;
        server_name localhost;
        ssl_certificate /etc/angie-lb/crt/server.crt;
        ssl_certificate_key /etc/angie-lb/crt/server.key;
        ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
        ssl_ciphers IANA-GOST2012-GOST8912-GOST8912:GOST2012-MAGMA-MAGMAOMAC:GOST2012-
↪KUZNYECHIK-KUZNYECHIKOMAC;
        ssl_prefer_server_ciphers on;

        location / {
            return 200 "Hello, this is GOST-based server\n";
        }
    }
}
```

Случай 1

Трафик балансируется на ГОСТ-бэкенд, если ГОСТ присутствует в списке шифров (может присутствовать наряду с другими шифрами).

Конфигурация:

```
http {

    upstream backend {
        server IP.OF.MAIN.BACKEND:80;
    }

    server {
        listen       127.0.0.1:8443 ssl;
        ssl_certificate /etc/angie-lb/crt/cp.crt;
        ssl_certificate_key /etc/angie-lb/crt/cp.key;
        server_name  localhost;
        status_zone  default;
        location / {
            proxy_pass http://backend;
        }
    }

}

stream {

    map $ssl_preread_ciphers $handler {
        "~TLS_GOST" 127.0.0.1:9443;
        default     127.0.0.1:8443;
    }

    server {
        listen       443;
        ssl_preread  on;
        pass $handler;
    }

    server {
        listen       127.0.0.1:9443;
        proxy_pass   IP.OF.GOST.BACKEND:443;
    }
}
```

Случай 2

Трафик балансируется на ГОСТ-бэкенд, если заданы только ГОСТ-шифры. Если помимо ГОСТ-шифров есть другие шифры, трафик отправляется на основной бэкенд.

Конфигурация:

```
http {

    upstream backend {
        server IP.OF.MAIN.BACKEND:80;
    }

    server {
        listen       127.0.0.1:8443 ssl;
        ssl_certificate /etc/angie-lb/crt/cp.crt;
        ssl_certificate_key /etc/angie-lb/crt/cp.key;
        server_name  localhost;
        status_zone  default;
        location / {
```

```
            proxy_pass http://backend;
        }
    }

}

stream {

    map $ssl_preread_ciphers $backend {
        "~^(TLS_GOST[^:]*)(:TLS_GOST[^:]*)*(:TLS_EMPTY_RENEGOTIATION_INFO_SCSV)?$" ␣
↪127.0.0.1:9443;
        default 127.0.0.1:8443;
    }

    server {
        listen       443;
        ssl_preread  on;
        pass $backend;
    }

    server {
        listen       127.0.0.1:9443;
        proxy_pass   IP.OF.GOST.BACKEND:443;
    }
}
```

Проверка

Случай 1

Трафик без ГОСТ отправляется на основной бэкенд:

```
# curl --ciphers '!IANA-GOST2012-GOST8912-GOST8912:!GOST2012-MAGMA-MAGMAOMAC:!
↪GOST2012-KUZNYECHIK-KUZNYECHIKOMAC:HIGH' --tlsv1.2 --tls-max 1.2 https://example.com
Hello, this is default backend
```

Трафик с ГОСТ отправляется на ГОСТ-бэкенд:

```
# curl --ciphers 'ALL' --tlsv1.2 --tls-max 1.2 https://example.com
Hello, this is GOST-based server
```

Случай 2

Трафик без ГОСТ отправляется на основной бэкенд:

```
# curl --ciphers '!IANA-GOST2012-GOST8912-GOST8912:!GOST2012-MAGMA-MAGMAOMAC:!
↪GOST2012-KUZNYECHIK-KUZNYECHIKOMAC:HIGH' --tlsv1.2 --tls-max 1.2 https://example.com
Hello, this is default backend
```

Трафик с ГОСТ отправляется на основной бэкенд:

```
# curl --ciphers 'ALL' --tlsv1.2 --tls-max 1.2 https://example.com
Hello, this is default backend
```

Трафик, где только ГОСТ, отправляется на ГОСТ-бэкенд:

```
# curl --ciphers 'IANA-GOST2012-GOST8912-GOST8912:GOST2012-MAGMA-MAGMAOMAC:GOST2012-
↪KUZNYECHIK-KUZNYECHIKOMAC' --tlsv1.2 --tls-max 1.2 https://example.com
Hello, this is GOST-based server
```

3.3.6.3 Балансировка и отказоустойчивость

Примеры балансировки нагрузки и обеспечения отказоустойчивости в Angie ADC: глобальная балансировка и управление соединениями с серверами группы.

- *Глобальная балансировка с проверкой доступности приложений*
- adc_keepalive-oneconnect

Глобальная балансировка с проверкой доступности приложений

Рассмотрим схему, где:

- Для домена `www.example.com` используются два дата-центра (бэкенда), ЦОД-1 и ЦОД-2.
- В дата-центре ЦОД-1 есть два бэкенда (приложения), app1 и app2, и база данных db1.
- В дата-центре ЦОД-2 есть два бэкенда (приложения), app3 и app4, и две базы данных, db2 и db3.
- В каждом дата-центре установлен Angie ADC, dc1 и dc2, соответственно.
- Трафик распределяется между дата-центрами по методу балансировки `round-robin`. При этом учитывается доступность дата-центров. Дата-центр считается доступным, если одновременно доступны хотя бы один бэкенд (приложение) и все имеющиеся базы данных этого дата-центра.

Дата-центр	Бэкенд	База данных	Узел Angie ADC
ЦОД-1	app1, app2	db1	dc1
ЦОД-2	app3, app4	db2, db3	dc2

Настройка

1. На любом узле кластера Angie ADC перейдите в раздел `Система` → `Доступность` → вкладка `Датчики` и создайте семь датчиков (см. *Настройка датчиков и мониторов*).

Датчик (имя датчика автоматически формируется из имени проверяемого ресурса и имени узла)	Узел кластера	Проверка	Ресурс
dc1-app1	dc1	HTTP	app1
dc1-app2	dc1	HTTP	app2
dc1-db1	dc1	TCP	db1
dc2-app3	dc2	HTTP	app3
dc2-app4	dc2	HTTP	app4
dc2-db2	dc2	TCP	db2
dc2-db3	dc2	TCP	db3

2. Перейдите на вкладку `Мониторы` и создайте четыре монитора.

Монитор	Датчики	Правило
`mon-dc1-app`	`dc1-app1`, `dc1-app2`	`Любой датчик`
`mon-dc1-db`	`dc1-db1`	`Любой датчик`
`mon-dc2-app`	`dc2-app3`, `dc2-app4`	`Любой датчик`
`mon-dc2-db`	`dc2-db2`, `dc2-db3`	`Все датчики`

Здесь:

- Мониторы приложения используют правило `Любой датчик`, т. е. дата-центр продолжает обслуживать трафик, пока отвечает хотя бы один бэкенд.
- Мониторы БД используют правило `Все датчики`, т. е. дата-центр продолжает обслуживать трафик, если отвечают все его БД.

3. Перейдите в раздел `Управление трафиком` → `Глобальная балансировка` и настройте конфигурацию GSLB. Для домена `example.com` добавьте динамическую запись типа `A` с именем `www`, балансировкой `round-robin` и двумя бэкендами — по одному на дата-центр (см. *Добавление доменов и записей*).

Дата-центр	Бэкенд (IP-адрес узла кластера Angie ADC)	Мониторы
ЦОД-1	`VIP dc1`	`mon-dc1-app`, `mon-dc1-db`
ЦОД-2	`VIP dc2`	`mon-dc2-app`, `mon-dc2-db`

Оба монитора на бэкенде объединяются по логике **И**: дата-центр доступен, только когда исправны и монитор приложения, и монитор БД. Запросы по методу `round-robin` распределяются по дата-центрам последовательно с учетом их доступности.

> **Важно**
>
> Если для балансировки используется более сложный режим, чем `round-robin`, то также необходимо завести мониторы, определяющие доступность дата-центров. Подробнее см. *Определение доступности дата-центров*.

4. Настройте делегирование зоны `example.com` на GSLB-узлы Angie ADC в родительской зоне `com`:

```
example.com.       IN NS dc1.example.com.
example.com.       IN NS dc2.example.com.

; Glue-записи - IP-адреса GSLB-узлов Angie ADC
dc1.example.com.  IN A  <IP-адрес dc1>
dc2.example.com.  IN A  <IP-адрес dc2>
```

Keepalive как аналог OneConnect profile от F5

Для повторного использования уже открытых TCP-соединений с серверами бэкенда используйте механизм keepalive.

Особенности:

- Если в upstream-группе определено несколько серверов, то keepalive-соединения устанавливаются с каждым из них в соответствии с выбранным методом балансировки.
- Мастер-процесс запускает несколько рабочих процессов в зависимости от настройки директивы worker_processes и у каждого рабочего процесса будет собственный пул keepalive-соединений:

– Если все запросы обрабатывает один рабочий процесс, то они могут проксироваться в одно и то же установленное соединение.

– Если запросы распределяются между несколькими рабочими процессами, то для каждого процесса формируются свои keepalive-соединения с бэкендом.

Настройка

1. Задайте директиву keepalive в блоке `upstream`.

   Пример:

```
upstream http_backend {
    server 192.168.0.1;
    server 192.168.0.2;

    keepalive 32;
}
```

2. Для HTTP установите директиву proxy_http_version в значение `1.1`, а поле заголовка `Connection` в adc__proxy_set_header очистите:

   Пример:

```
server {
    # ...

    location / {
        proxy_pass http://http_backend;
        proxy_http_version 1.1;
        proxy_set_header Connection "";
        # ...
    }
}
```

3. Если требуется разделять потоки по IP-адресам, используйте привязку по sticky learn в группе upstream в сочетании с директивой geo.

   Пример:

```
geo $idmask {
    ranges;
    default                   ZZ;
    10.21.0.0-10.21.0.255     tau;
    10.21.4.0-10.21.4.255     chi;
    10.21.8.0-10.21.8.255     alpha;
    10.21.20.0-10.21.20.255   nu;
}

upstream http_backend {
    server 10.21.8.6:80;
    server 10.21.8.13:80;

    sticky learn
        create=$idmask
        lookup=$idmask
        zone=client_sessions:1m
        timeout=60s;

    keepalive 32;
}
```

```
server {
    listen       10.21.8.8:80;
    server_name  localhost;

    location / {
        proxy_http_version 1.1;
        proxy_set_header Connection "";

        proxy_pass http://http_backend;
    }
}
```

В этом случае в пределах одного рабочего процесса поведение Angie ADC будет очень похоже на механизм OneConnect в F5 BIG-IP.

3.3.6.4 Безопасность и контроль доступа

Примеры ограничения доступа к ресурсам и защиты от избыточной нагрузки в Angie ADC.

- *Ограничение доступа к ресурсам по IP-адресам*
- *Ограничение числа соединений, частоты запросов и скорости передачи*

Ограничение доступа к ресурсам по IP-адресам

Angie ADC позволяет ограничивать доступ к ресурсам по IP-адресам с помощью директив `allow` и `deny`. Для HTTP-трафика директивы allow и deny задаются в блоках `http`, `server`, `location` и `limit_except`. Для TCP-трафика используются директивы allow и deny в блоках `stream` и `server`. Можно ограничивать доступ ко всему серверу или к отдельным путям. В качестве адресов можно указывать отдельные IPv4- или IPv6-адреса, сети CIDR, все UNIX-сокеты или все адреса клиентов.

> **Примечание**
>
> Правила проверяются последовательно, сверху вниз, до первого совпадения: как только адрес клиента совпал с правилом `allow` или `deny`, проверка прекращается.

Списки доступа можно сочетать с ограничением числа соединений и скорости передачи, см. *Ограничение числа соединений, частоты запросов и скорости передачи*.

Примеры

Белый список

```
server {
    allow 192.168.1.0/24;
    allow 10.1.1.0/16;
    allow 2001:0db8::/32;
    deny  all;
}
```

Здесь разрешается доступ только с указанных адресов, все остальные блокируются. Правила перечисляются от разрешающих к завершающему `deny all`.

Черный список

```
server {
    deny  192.168.1.1;
    deny  5.6.7.0/24;
    allow all;
}
```

Здесь блокируется доступ с указанных адресов, всем остальным доступ разрешается. Правила перечисляются от запрещающих к завершающему `allow all`.

TCP (stream)

```
stream {
    server {
        listen 12345;

        deny  192.168.1.1;
        allow 192.168.1.0/24;
        allow 2001:0db8::/32;
        deny  all;

        proxy_pass backend;
    }
}
```

Здесь разрешается доступ из указанных сетей, кроме одного конкретного адреса. Все остальные адреса тоже блокируются.

Ограничение доступа к отдельному пути

Чтобы применить список доступа не ко всему серверу, а к конкретному URI, поместите директивы в соответствующий блок location. Например, доступ к разделу `/admin/` разрешается только из внутренней сети:

```
server {
    location /admin/ {
        allow 192.168.1.0/24;
        deny  all;
    }

    location / {
        proxy_pass http://backend;
    }
}
```

Работа с большими списками

Если правил (адресов) много, можно вынести список правил в отдельный файл и подключить его через директиву `include`.

```
location / {
    include    /etc/angie-lb/http.d/blacklist.conf;
    allow      all;
}
```

Файл списка можно создать в веб-интерфейсе Angie ADC: в *редакторе конфигурации балансировщика* нажмите значок добавления напротив нужной папки, задайте имя файла (например,

`blacklist.conf`) и заполните его. Файл должен содержать только правила, например:

```
deny 192.168.1.1;
deny 5.6.7.0/24;
```

В качестве альтернативы можно использовать переменные из модуля Geo: модуль сопоставляет IP-адрес клиента со значением переменной, которое затем используется для принятия решения о доступе.

```
http {
    geo $blocked {
        default         0;
        192.168.1.1     1;
        5.6.7.0/24      1;
    }

    server {
        location / {
            if ($blocked) {
                return 403;
            }
        }
    }
}
```

Ограничение числа соединений, частоты запросов и скорости передачи

Angie ADC позволяет ограничивать доступ к проксируемым ресурсам, настраивая три параметра нагрузки:

- *число одновременных соединений*;
- *частоту обработки запросов*;
- *скорость передачи ответа клиенту*.

Ограничения используются для защиты upstream-серверов приложений от перегрузки слишком большим количеством одновременных запросов пользователей.

Ограничение числа соединений

Ограничение числа соединений настраивается с помощью двух основных директив:

- limit_conn_zone: задает зону разделяемой памяти. Через эту зону рабочие процессы совместно используют счетчики для значений ключа.
- limit_conn: задает максимально допустимое число соединений для одного значения ключа. Учитываются только те соединения, в которых обрабатывается запрос и полностью прочитан его заголовок.

Примеры

В следующем примере число соединений ограничивается для каждого IP-адреса, для запросов к `location /download/` разрешается не более одного соединения с одного адреса:

```
http {
    limit_conn_zone $binary_remote_addr zone=addr:10m;

    server {
        location /download/ {
            limit_conn addr 1;
```

```
        }
    }
}
```

Здесь с помощью директивы limit_conn_zone задан ключ `$binary_remote_addr` (IP-адрес клиента) и параметры зоны разделяемой памяти `zone=addr:10m`. С помощью директивы limit_conn ограничение применено в контексте `location /download/`: указано имя зоны разделяемой памяти `addr` и допустимое число соединений на один ключ `1`.

Ограничить число соединений для конкретного сервера можно также с помощью переменной `$server_name`:

```
http {
    limit_conn_zone $server_name zone=servers:10m;

    server {
        limit_conn servers 1000;
    }
}
```

Директив limit_conn может быть несколько. Например, следующая конфигурация одновременно ограничивает число соединений с одного IP-адреса и общее число соединений с виртуальным сервером:

```
limit_conn_zone $binary_remote_addr zone=perip:10m;
limit_conn_zone $server_name zone=perserver:10m;

server {
    limit_conn perip 10;
    limit_conn perserver 100;
}
```

При превышении ограничения сервер возвращает клиенту код 503; его можно переопределить директивой limit_conn_status.

Примечание

В HTTP/2 и HTTP/3 каждый параллельный запрос считается отдельным соединением.

Пробный запуск

Прежде чем включать ограничение в рабочем режиме, поведение можно проверить с помощью директивы limit_conn_dry_run. В режиме пробного запуска число соединений фактически не ограничивается, но число избыточных соединений учитывается в зоне разделяемой памяти, что позволяет оценить корректность ограничений без влияния на клиентов. Каждое соединение, которое превысило бы заданное ограничение, будет записано в лог с пометкой «dry run».

Примечание

Ограничение числа соединений доступно и для TCP/UDP-трафика: директивы limit_conn и limit_conn_zone задаются в блоках `stream` и `server`.

Ограничение частоты запросов

Ограничение частоты запросов позволяет замедлять атаки с подбором паролей методом перебора и помогает защититься от DDoS-атак, ограничивая частоту входящих запросов до значения, типичного для реальных пользователей.

Ограничение частоты запросов работает по алгоритму «дырявого ведра» (leaky bucket): запросы поступают в ведро с разной скоростью, а покидают его с фиксированной. Для ограничения частоты запросов нужно настроить глобальные параметры «дырявого ведра»:

- ключ — параметр, по которому один клиент отличается от другого, обычно переменная;
- зону разделяемой памяти — имя и размер зоны, в которой хранятся состояния этих ключей («дырявое ведро»);
- скорость — предельная частота запросов, заданная в запросах в секунду (`r/s`) или в запросах в минуту (`r/m`) («вытекание из дырявого ведра»). Запросы в минуту используются, чтобы задать частоту меньше одного запроса в секунду.

Ограничение частоты запросов настраивается с помощью двух основных директив:

- limit_req_zone: задает параметры ограничения — ключ, зону разделяемой памяти и среднюю скорость;
- limit_req применяет ограничение в контекстах `server`, `location` или `http`.

Примеры

В следующем примере обработка запросов к `/search/` ограничивается в среднем одним запросом в секунду с одного IP-адреса:

```
http {
    limit_req_zone $binary_remote_addr zone=one:10m rate=1r/s;

    server {
        location /search/ {
            limit_req zone=one;
        }
    }
}
```

Примечание

Размер зоны разделяемой памяти выбирайте из расчета примерно 16 000 IP-адресов на 1 мегабайт; подробнее см. limit_req_zone.

Всплески запросов

Запросы могут поступать неравномерно, поэтому строгое ограничение может привести к отклонению кратковременных всплесков. Параметр `burst` задает число запросов, которые могут превысить заданную скорость: избыточные запросы помещаются в очередь и обрабатываются с указанной скоростью, а запросы сверх размера очереди отклоняются с кодом 503.

```
limit_req zone=one burst=5;
```

Такая конфигурация допускает в среднем не более одного запроса в секунду со всплесками до пяти запросов.

Если задерживать избыточные запросы в пределах всплеска не требуется и их нужно обрабатывать без задержки, добавьте параметр `nodelay`:

```
limit_req zone=one burst=5 nodelay;
```

Параметр `delay` задает число запросов в пределах всплеска, которые обрабатываются без задержки; последующие избыточные запросы задерживаются до достижения заданной скорости:

```
limit_req zone=one burst=5 delay=3;
```

Пробный запуск

Прежде чем включать ограничение в рабочем режиме, поведение можно проверить с помощью директивы limit_req_dry_run. В режиме пробного запуска скорость обработки запросов фактически не ограничивается, но число избыточных запросов учитывается в зоне разделяемой памяти, что позволяет оценить корректность ограничений без влияния на клиентов:

```
limit_req zone=one burst=5 nodelay;
limit_req_dry_run on;
```

Каждый запрос, который превысил бы заданное ограничение частоты, будет записан в лог с пометкой «dry run».

Ограничение скорости передачи

Директива limit_rate ограничивает скорость передачи ответа клиенту. Скорость задается в байтах в секунду, значение `0` отключает ограничение. Ограничение действует на отдельный запрос, поэтому при двух одновременных соединениях суммарная скорость для клиента будет вдвое выше заданной.

Директива limit_rate_after задает начальный объем данных, который передается без ограничения; ограничение начинает действовать только после его превышения. Это удобно, например, при отдаче медиафайлов, когда начало ролика нужно передать быстро, а дальнейшую загрузку — ограничить.

Примечание

Директивы `limit_rate` и `limit_rate_after` применимы только к HTTP-трафику. Для ограничения полосы пропускания в TCP/UDP (`stream`) используйте директивы proxy_download_rate и proxy_upload_rate.

Примеры

```
location /download/ {
    limit_rate_after 500k;
    limit_rate       50k;
}
```

Ограничение скорости часто сочетают с ограничением числа соединений, чтобы контролировать суммарное потребление полосы пропускания одним клиентом:

```
http {
    limit_conn_zone $binary_remote_addr zone=addr:10m;

    server {
        location /download/ {
            limit_conn       addr 1;
            limit_rate_after 1m;
            limit_rate       50k;
        }
    }
}
```

Динамическое ограничение скорости

В значении limit_rate можно использовать переменные, это позволяет менять ограничение в зависимости от условий. В следующем примере скорость передачи выбирается с помощью директивы `map` в зависимости от версии протокола TLS (встроенная переменная $ssl_protocol): чем новее протокол, тем выше допустимая скорость:

```
map $ssl_protocol $response_rate {
    "TLSv1.1"  10k;
    "TLSv1.2"  100k;
    "TLSv1.3"  1000k;
}

server {
    listen 443 ssl;

    ssl_certificate     example.com.crt;
    ssl_certificate_key example.com.key;

    location / {
        limit_rate $response_rate;
    }
}
```

3.3.6.5 Доставка контента

Примеры отдачи статического контента средствами Angie ADC.

- *Загрузка и раздача статических файлов*

Загрузка и раздача статических файлов

Angie ADC поддерживает загрузку и раздачу статических файлов (изображений, статических HTML-страниц и пр.). Загрузка осуществляется по протоколу SCP (Secure Copy Protocol), после чего файл будет доступен по HTTP.

Чтобы добавить статический файл, выполните следующие действия:

1. На машине-источнике запустите загрузку файла (например страницу-заглушку `maintenance.html`):

   ```
   scp -P 2222 maintenance.html admin@<имя_хоста>:/maintenance.html
   ```

2. В веб-интерфейсе Angie ADC перейдите к редактированию конфигурации балансировщика нагрузки (`Управление трафиком` → `Балансировщик нагрузки`) и в блоке `http` настройте доступ к каталогу с этим файлом:

   ```
   http {
       server {
           listen 80;
           root /var/transfer;
       }
   }
   ```

3. Если для расширения файла не определен MIME-тип или требуется указать его явно, добавьте соответствующую строку в блок `types` (например `application/pkix-crl crl;` для CRL).

4. Сохраните изменения, нажав кнопку `Сохранить`.

   Файл `maintenance.html` будет доступен по адресу `http://<имя_хоста>/maintenance.html`.

Чтобы проверить, что файл корректно отдается клиентам, выполните запрос `curl`. Например, для хоста `adc.angie.local`:

```
$ curl adc.angie.local/maintenance.html -v
```

Если получен код `200 OK` и указан правильный Content-Type, то файл был успешно загружен и доступен.

Раздача файлов из разных локальных каталогов

В зависимости от типа файлы могут раздаваться из разных каталогов, например HTML-страницы из `/static/www`, а изображения из `/static/images`. Для настройки используется директива location.

Чтобы настроить раздачу файлов из разных локальных каталогов, выполните следующие действия:

1. Создайте локальный каталог со всеми необходимыми подкаталогами.

   Например:

   ```
   mkdir -p static/www static/images
   ```

2. Перенесите в этот каталог статические файлы. Например, поместите файл `index.html` в `/static/www`, а изображение `image1.png` в `/static/images`.

3. Скопируйте весь каталог в файловое хранилище Angie ADC по SCP:

   ```
   scp -P 2222 -r static admin@<имя_хоста>:/
   ```

4. В веб-интерфейсе Angie ADC перейдите к редактированию конфигурации балансировщика нагрузки (`Управление трафиком` → `Балансировщик нагрузки`) и в блоке `http` настройте доступ к каталогам со статическими файлами:

   ```
   server {
       location / {
           root /static/www;
       }

       location /images/ {
           root /static;
       }
   }
   ```

5. Сохраните изменения, нажав кнопку `Сохранить`.

Теперь запросы, URI которых начинаются на `/images/`, будут обрабатываться в `/static/images`. Другие запросы будут обрабатываться в `/static/www`. Если файл не найден, отобразится ошибка 404.

Например, на запрос `http://<имя_хоста>/images/image1.png` будет отдан файл `/static/images/image1.png`, а на запрос `http://<имя_хоста>/files/index.html` будет отдан файл `/static/www/files/index.html`.

3.3.6.6 Администрирование и наблюдаемость

Примеры эксплуатации Angie ADC: делегирование управления сервисами и сбор пользовательских метрик.

- *Делегирование сервиса оператору*
- *Настройка пользовательских метрик*

Делегирование сервиса оператору

Angie ADC поддерживает передачу управления выбранными сервисами оператору. Для этого администратор создает отдельные файлы конфигурации, в которых будет настраиваться балансировка сервиса, и выдает права на доступ к этим файлам оператору. Администратор также подключает эти файлы в основной конфигурационный файл `angie.conf` с помощью директивы `include`. Оператор, занимающийся обслуживанием сервиса, редактирует конфигурацию балансировщика нагрузки в выделенных для него файлах. При этом он не видит другие файлы конфигурации, т. к. не имеет к ним доступа. При сохранении любого файла, включенного по `include`, вся конфигурация балансировщика валидируется и применяется. Также можно настроить доступ оператора к данным мониторинга сервиса.

Важно

Включаемые файлы должны содержать синтаксически верные директивы и блоки, иначе итоговая конфигурация не пройдет валидацию и не будет применена.

Настройка со стороны администратора

Ниже приведен пример делегирования оператору управления сервисом `example.com`.

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки`.
2. Создайте файлы `example_upstream.conf` и `example_server.conf` в папке `http.d`.
3. В конфигурации `angie.conf` создайте блок, управляющий сервисом `example.com`, например:

```
http {

    upstream example_upstream {
        zone example_zone 1m;
        include "http.d/example_upstream.conf";
    }

    server {
        listen       VIP:80;
        server_name  example.com;
        status_zone  example_zone;

        location / {
            proxy_pass "http://example_upstream";
            include "http.d/example_server.conf";
        }
    }

}
```

Здесь:

- Создана группа серверов `example_upstream` для балансировки нагрузки.
- Выделена зона разделяемой памяти `example_zone`. В ней хранится текущее состояние серверов, счетчики запросов и сессии.
- С помощью директивы adc__include подключен внешний файл `example_upstream.conf`, в котором оператор сможет указать IP-адреса или домены бэкенд-серверов.
- Описаны правила обработки запросов.

- Метрики для вывода статистики (adc__status_zone) будут собираться в уже заданную зону разделяемой памяти `example_zone`.
- Все входящие запросы будут перенаправляться на бэкенд-серверы, описанные в файле `example_upstream.conf`.
- С помощью директивы adc__include подключен файл `example_server.conf` с дополнительными настройками для проксирования, которые также может настраивать оператор.

4. Выдайте оператору *права* на редактирование файлов `http.d/example_upstream.conf` и `http.d/example_server.conf`.

> **Совет**
>
> Рекомендуется также передать оператору внутренние инструкции и стандарты компании по наполнению этих конфигурационных файлов.

5. Выдайте оператору *права доступа* к зоне разделяемой памяти `example_zone` для просмотра статистики сервиса на странице мониторинга.

Теперь в разделе `Управление трафиком` → `Балансировщик нагрузки` оператору доступны файлы `http.d/example_upstream.conf` и `http.d/example_server.conf`.

Изменения, внесенные оператором в файл, автоматически валидируются системой и применяются после нажатия кнопки `Сохранить` без прерывания трафика. Если конфигурация не проходит валидацию, то она не применяется.

Пример работы оператора

1. В веб-интерфейсе Angie ADC перейдите в раздел `Управление трафиком` → `Балансировщик нагрузки`.

   Откроется экран с файлами, доступ к которым у вас есть. Вы можете просматривать и редактировать эти файлы.

> **Важно**
>
> Отредактированные файлы должны содержать синтаксически верные директивы и блоки, иначе итоговая конфигурация балансировщика не пройдет валидацию и не будет применена.

2. В файле `example_upstream.conf` укажите адреса бэкендов и алгоритм балансировки. Например:

```
least_conn;
server 192.0.2.10:8080;
server 192.0.2.11:8080;
```

3. Нажмите `Сохранить`. Изменения в конфигурации будут применены сразу.
4. Если необходимо, в файле `example_server.conf` добавьте дополнительные настройки для проксирования, например заголовок запроса:

```
proxy_set_header X-Custom-Header "value";
```

5. Нажмите `Сохранить`. Изменения в конфигурации будут применены сразу.

Настройка пользовательских метрик

Angie может собирать пользовательские числовые метрики в разделяемой памяти и выводить их через API статистики по адресу `/status/http/metric_zones/`. Это обеспечивает модуль HTTP Metric.

> **Примечание**
>
> Это руководство описывает метрики для HTTP-трафика. Для TCP- и UDP-трафика см. модуль Stream Metric, который выводит свои зоны по адресу `/status/stream/metric_zones/`.

Шаги настройки

1. Создайте зону метрик в блоке `http`:
   - adc__metric_zone создает зону с одной метрикой.
   - adc__metric_complex_zone создает зону с несколькими именованными метриками.
2. Обновляйте метрики при обработке запросов директивой adc__metric. Используйте пару `key=value` (оба — комплексные значения), и выберите этап обновления параметром `on=` (`request`, `response` или `end`).
3. Откройте API через `location`:

```
location /status/ {
    api /status/http/metric_zones/;
}
```

Пример

Подсчет запросов по хостам и вывод метрик через API:

```
http {
    metric_zone requests:128k count;

    server {
        listen 80;

        location / {
            metric requests $host=1;
        }

        location /status/ {
            api /status/http/metric_zones/;
        }
    }
}
```

Примечания

- При `expire=on` и переполнении памяти истекают самые давно неиспользуемые записи. При `expire=off` новые обновления отбрасываются, а счетчик `discarded` увеличивается.
- Если задан `discard_key`, метрики истекших записей агрегируются под этим ключом в API.
- Длина ключей и значений ограничена 255 байт; длинные ключи усекутся в API.
- Пустое значение трактуется как `0`, а непустая строка без числа в начале — как `1`.

ГЛАВА 4

Отказоустойчивость и маршрутизация

Здесь описывается обеспечение отказоустойчивости с помощью пары высокой доступности, а также настройка динамической и статической маршрутизации.

В этом разделе:

- *Пара высокой доступности*
- *IP-маршрутизация*

4.1 Пара высокой доступности

В этом разделе:

- *Обзор работы*
- *Создание пары высокой доступности*
- *Настройка высокой доступности в паре*
- *Управление парой*
- *Привязка клиентских сессий*

Высокая доступность (High Availability) — это режим, при котором два устройства Angie ADC объединяются в пару высокой доступности, обеспечивающую синхронизацию конфигурации основного узла на резервный и сохранение работоспособности системы при сбое одного из узлов пары.

Пример типовой схемы работы пары высокой доступности:

Примечание

Рекомендуется резервировать все компоненты инфраструктуры. Отказ сопутствующей инфраструктуры (например выход из строя вышестоящего маршрутизатора или сбой серверов) выходит за рамки решения высокой доступности Angie ADC.

Пример отказоустойчивой инфраструктуры:

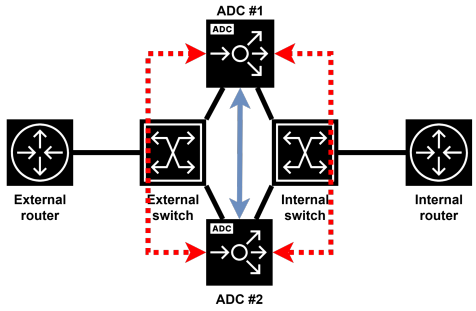


Рис. 1: Рис. 1

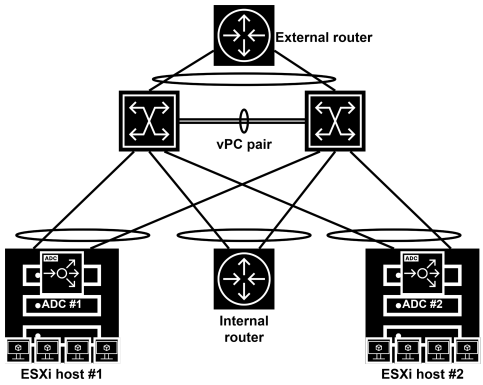


Рис. 2: Рис. 2

4.1.1 Обзор работы

Вы можете объединить два устройства Angie ADC в пару высокой доступности в режиме Active / Standby.

4.1.1.1 Режим Active / Standby

При создании пары одно устройство назначается основным, а второе — резервным. Конфигурации узлов синхронизированы. Основной узел принимает соединения и управляет серверами. Резервный узел находится в режиме ожидания. При выходе из строя основного узла происходит *смена ролей*: резервный узел становится основным, а основной после восстановления переходит в режим ожидания.

Высокая доступность достигается за счет двунаправленных проверок доступности узлов. Узлы отслеживают состояние друг друга, отправляя запросы (UDP-сообщения) на все интерфейсы соседнего узла, участвующие в паре. По умолчанию запросы отправляются раз в 250 мс. Если с момента получения последнего успешного ответа от основного узла прошло больше времени, чем указано в таймауте ожидания, интерфейс будет считаться недоступным. По умолчанию таймаут равен 3 секундам. Если проверка доступности всех интерфейсов основного узла пары завершается неудачно, происходит смена ролей. Параметры опроса можно *настраивать*.

Поддерживается *привязка клиентских сессий* (sticky sessions), позволяющая сохранять клиентские сессии при смене основного узла, принимающего соединения.

Информация о состоянии пары, ролях узлов и событиях в работе пары отображается в веб-интерфейсе Angie ADC. Подробнее см. *Просмотр информации о паре*.

4.1.1.2 Развертывание

Развертывание пары высокой доступности включает следующие шаги:

1. *Предварительные действия*.
2. *Создание пары высокой доступности в режиме Active / Standby*.
3. *Настройка высокой доступности в паре*.

4.1.1.3 Обновление конфигурации и синхронизация

Конфигурации узлов автоматически синхронизируются при создании пары.

> **Примечание**
>
> После изменения конфигурации основного узла необходимо вручную запустить синхронизацию узлов пары.

При синхронизации основной узел передает свою конфигурацию на резервный узел. На резервном узле перезаписываются следующие файлы и папки:

- конфигурация балансировщика нагрузки;
- сертификаты и ключи балансировщика нагрузки;
- конфигурация маршрутизации (VRRP, BGP, OSPF);
- конфигурация GSLB;
- все файлы в папках `/etc/angie/crt` и `/etc/angie-lb/crt`;
- все файлы в папке `/var/transfer`.

Остальные файлы резервного узла, если они находятся вне указанных папок (например файл лицензии), удалены не будут.

Подробнее см. *Обновление конфигурации и синхронизация*.

4.1.2 Создание пары высокой доступности

Вы можете создать пару высокой доступности в веб-интерфейсе Angie ADC.

4.1.2.1 Требования

Для создания пары высокой доступности должны выполняться следующие условия:

- Оба устройства Angie ADC должны иметь одинаковую версию ПО и лицензию.
- Время на узлах пары должно быть синхронизировано, например, по *NTP*.

4.1.2.2 Предварительные действия

1. Разверните два устройства Angie ADC из будущей пары.

   При этом должны выполняться следующие условия:

   - В пару можно поставить устройства Angie ADC, у которых хотя бы одна общая подсеть.
   - Интерфейсы самого устройства Angie ADC могут находиться в разных подсетях, но при формировании пар интерфейсов все IP-адреса попарно должны быть из одинаковых подсетей.
   - Каждый узел должен иметь собственный набор уникальных IP-адресов. Поддерживаются только IPv4-адреса. Необходимо прописать IP-адреса для всех физических интерфейсов, которые будут использоваться для обеспечения высокой доступности.

> **Предупреждение**
>
> В дальнейшем не рекомендуется изменять IP-адреса узлов, объединенных в пару высокой доступности, иначе пара потеряет работоспособность.

Мы рекомендуем иметь одинаковое количество интерфейсов на обоих устройствах Angie ADC, чтобы каждый интерфейс получил пару на другом устройстве Angie ADC. Интерфейсы без пары не будут участвовать в обеспечении высокой доступности.

2. Настройте авторизацию на резервном узле Angie ADC с использованием локальной учетной записи `admin` (эти учетные данные необходимы для создания пары).
3. Настройте минимальную конфигурацию узла, который будет иметь роль основного. При создании пары запустится синхронизация конфигураций (конфигурация основного узла будет перенесена на резервный узел). Настройку также можно выполнить позже, после создания пары, при этом необходимо будет вручную запустить синхронизацию конфигураций после настройки.

4.1.2.3 Создание пары высокой доступности в режиме Active / Standby

При создании пары высокой доступности роль основного узла (Active) автоматически назначается тому узлу, с которого создается пара, роль резервного (Standby) — добавляемому узлу.

Чтобы создать пару высокой доступности, выполните следующие действия:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Высокая доступность и кластеризация` → `Высокая доступность`.

   Откроется экран подключения резервного узла к текущему узлу.

2. На экране `Создание пары высокой доступности` заполните следующие поля:

   - `IP-адрес` — IP-адрес второго узла пары (IPv4) для удаленного администрирования и мониторинга этого узла. Это может быть выделенный интерфейс только для управления или один из интерфейсов, передающих продуктовый трафик. Этот адрес не распространяется и не синхронизируется.
   - `Логин` и `Пароль` — данные для авторизации на резервном узле.

   > **Примечание**
   >
   > Используйте логин локальной учетной записи `admin` (см. "Предварительные действия" выше).

3. Нажмите `Подключить`.

   Между двумя узлами будет создано соединение. Откроется окно настройки соответствия интерфейсов.

4. В окне `Настройка соответствия интерфейсов` в раскрывающихся списках основного и резервного узла выберите интерфейсы, которые вы хотите поставить в пару. Опрос доступности узлов будет проводиться в рамках каждой добавленной пары.

   Чтобы добавить еще одну пару, нажмите значок `Добавить` и повторите действия.

   В списках отображаются только интерфейсы в состоянии `up`. Интерфейсы loopback, в состоянии `down` и без IP-адреса не отображаются и недоступны для выбора.

   > **Примечание**

> Адреса двух сопоставляемых интерфейсов должны быть из одной подсети. Минимально достаточно одной пары интерфейсов, но мы рекомендуем задать пары для всех интерфейсов обоих узлов.

5. Нажмите `Сохранить`.

   Будет сформирована пара высокой доступности в режиме Active / Standby. Сразу после создания у пары будет отображаться статус `starting` (происходит синхронизация конфигураций). После успешной синхронизации статус поменяется на `on` (пара в рабочем состоянии).

6. После объединения двух устройств Angie ADC в пару необходимо *настроить механизмы высокой доступности* на узлах этой пары.

4.1.3 Настройка высокой доступности в паре

После объединения двух устройств Angie ADC в пару необходимо настроить механизмы высокой доступности на узлах этой пары.

Для этого необходимо выбрать механизм обеспечения высокой доступности. Поддерживаются следующие механизмы:

- VRRP;
- OSPF;
- BGP.

Можно одновременно использовать несколько механизмов на разных интерфейсах устройства.

Настройку основного узла можно проводить до или после создания пары высокой доступности. При создании пары уже имеющиеся конфигурации синхронизируются, а после создания пары можно запустить ручную синхронизацию конфигураций.

4.1.3.1 VRRP

В паре высокой доступности группы VRRP работают только на узле с ролью Active. На узле Standby все группы выключены, даже если они включены в конфигурации: повышение приоритета или команда `no vrrp ... shutdown` эту роль не отменяют. При смене ролей группы включаются на узле, который стал Active.

Различайте три состояния:

Состояние	Значение
Выключение группы (`shutdown`)	Администратор выключил конкретную группу на конкретном узле
Active / Standby	Роль узла в паре высокой доступности
Master / Backup	Текущий результат выборов VRRP в конкретной группе

Чтобы настроить VRRP в действующей паре:

1. Определите, какой узел имеет роль Active.
2. На узле Active подключитесь к *CLI*, перейдите в режим `configuration` и создайте группу командой *vrrp*:

```
$$ configuration
## vrrp <VRID> interface <имя_интерфейса> address <IP_адрес/префикс>
```

3. Проверьте *соответствие интерфейсов* узлов в настройках пары, особенно если имена интерфейсов на узлах различаются.

4. Запустите *синхронизацию пары*. Она переносит конфигурацию основного узла на резервный, в том числе группы VRRP.
5. Проверьте группы на обоих узлах командой *vrrp show* и работу VIP на узле Active.
6. Проверьте переключение ролей пары и доступ к сервису через VIP после него.

Выключение группы на узле Active не заменяет проверку переключения пары: пока второй узел остается Standby, он не принимает VIP. Схема с разными Master для двух VIP (*Active-Active*) к действующей паре не применяется.

Пример вывода команды `ip a`, выполненной на активном узле (интерфейс `vrrp4-ens33-1@ens33` находится в состоянии `UP`):

```
ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default␣
↪qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet 203.0.113.1/32 brd 203.0.113.1 scope global lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group␣
↪default qlen 1000
link/ether 00:0c:29:96:0c:dc brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 10.65.1.7/24 brd 10.65.1.255 scope global ens33
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe96:cdc/64 scope link
valid_lft forever preferred_lft forever
3: vrrp4-ens33-1@ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue␣
↪state UP group default qlen 1000
link/ether 00:00:5e:00:01:01 brd ff:ff:ff:ff:ff:ff
inet 10.65.1.5/24 metric 1000 scope global vrrp4-ens33-1
valid_lft forever preferred_lft forever
inet6 fe80::200:5eff:fe00:101/64 scope link
valid_lft forever preferred_lft forever
```

Пример вывода команды `ip a`, выполненной на резервном узле (интерфейс `vrrp4-ens33-1@ens33` находится в состоянии `DOWN`):

```
ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default␣
↪qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet 203.0.113.1/32 brd 203.0.113.1 scope global lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group␣
↪default qlen 1000
link/ether 00:0c:29:c1:36:b4 brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 10.65.1.8/24 brd 10.65.1.255 scope global ens33
```

```
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fec1:36b4/64 scope link
valid_lft forever preferred_lft forever
5: vrrp4-ens33-1@ens33: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue␣
↪state DOWN group default qlen 1000
link/ether 00:00:5e:00:01:01 brd ff:ff:ff:ff:ff:ff protodown on protodown_reason <7>
inet 10.65.1.5/24 metric 1000 scope global vrrp4-ens33-1
valid_lft forever preferred_lft forever
inet6 fe80::200:5eff:fe00:101/64 scope link
valid_lft forever preferred_lft forever
```

Далее вы можете настроить высокую доступность двумя способами:

- Назначение адреса сервиса на виртуальный VRRP-интерфейс.
- Назначение адреса сервиса на интерфейс `lo`.

Назначение адреса сервиса на виртуальный VRRP-интерфейс

При смене роли узла сервис будет перенесен на тот узел, который взял на себя роль Active. У группы VRRP один виртуальный адрес; для нескольких адресов сервисов нужно несколько групп. Для маршрутизатора адрес сервиса находится в подключенной сети, то есть доступен напрямую:

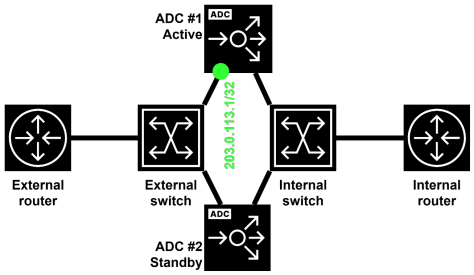


Рис. 3: Рис. 1

Если клиенты находятся в одной IP-сети с адресом сервиса, этот способ будет наиболее удобным:

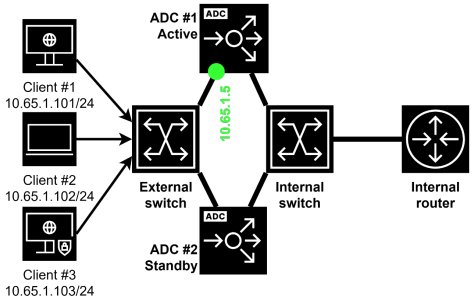


Рис. 4: Рис. 2

Назначение адреса сервиса на интерфейс lo

Адрес сервиса задается на *интерфейсе lo* обоих узлов: синхронизация пары не переносит интерфейсы и их адреса (см. *Динамическая маршрутизация в паре высокой доступности*), поэтому адрес задается на каждом узле. При настройке статического маршрута на маршрутизаторе необходимо указать VIP группы VRRP как адрес следующего перехода (next-hop) для префикса, содержащего адрес сервиса. На интерфейсе `lo` может быть задано несколько адресов одновременно. Мы рекомендуем использовать этот способ как более гибкий:

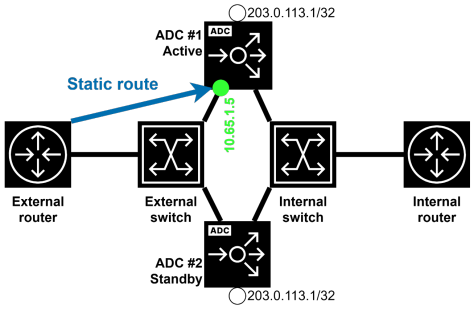


Рис. 5: Рис. 3

После расформирования пары

Бывший резервный узел сохраняет ограничения роли Standby: его группы VRRP остаются выключенными, а маршруты не анонсируются. Чтобы использовать узел самостоятельно, выполните на нем команду *no ha standby*:

```
$$ configuration
## no ha standby
```

Пока узел входит в пару, команда отклоняется. Команда снимает ограничения и для анонсов динамической маршрутизации, поэтому перед ее выполнением проверьте планируемую роль узла в сети. Затем убедитесь командой `show vrrp` в основном режиме CLI, что группы участвуют в выборах (состояние Master или Backup), и проверьте доступность адресов групп VRRP.

4.1.3.2 Динамическая маршрутизация в паре высокой доступности

В паре высокой доступности маршрутизацию настраивают на узле Active. *Синхронизация пары* копирует на узел Standby раздел маршрутизации целиком вместе с группами VRRP; имена интерфейсов групп VRRP, OSPF и `update-source interface` заменяются по *соответствию интерфейсов*. Адреса в `update-source <IPv4>` и `router-id` копируются как есть. Интерфейсы, их адреса (в том числе на `lo`) и статические маршруты синхронизация не переносит: они задаются на каждом узле.

Узел Standby устанавливает соседство, но ограничивает свои анонсы:

- в BGP на каждого соседа действует исходящий фильтр, запрещающий все префиксы;
- в OSPF узел объявляет максимальную метрику своих каналов (`max-metric router-lsa administrative`) и не перераспределяет подключенные сети; перераспределение статических маршрутов и маршрутов ядра (`redistribute static`, `redistribute kernel`) и `default-information` не ограничиваются.

После смены ролей ограничения снимаются с нового узла Active. Если пара расформирована, бывший резервный узел сохраняет эти ограничения до команды *no ha standby*.

Идентификатор маршрутизатора в паре

Если адрес сервиса задан на `lo` обоих узлов пары, их идентификаторы маршрутизатора совпадают:

- без `router-id` FRR выбирает идентификатор по наибольшему адресу на `lo`, то есть по общему адресу сервиса;
- заданный `router-id` синхронизация копирует с узла Active на узел Standby.

С одинаковыми идентификаторами узлы не устанавливают OSPF-соседство друг с другом. В BGP соседи тоже видят у обоих узлов один идентификатор.

Чтобы идентификаторы различались, не задавайте `router-id`, а добавьте на `lo` каждого узла свой адрес `/32`, численно больший всех адресов сервисов на `lo`. Адреса на `lo` не синхронизируются,

поэтому у каждого узла остается свой адрес, и FRR выбирает идентификатор по нему. Например, при адресе сервиса `203.0.113.1`:

```
## set system interface lo ip address 203.0.113.11/32
```

на первом узле и `203.0.113.12/32` на втором. Если адреса на `lo` анонсируются через `redistribute connected` без карты маршрутов, анонсируется и собственный адрес узла; чтобы анонсировать только адрес сервиса, используйте карту маршрутов со списком префиксов.

4.1.3.3 OSPF

Если в сети используются протоколы динамической маршрутизации, то вы можете добавить пару высокой доступности Angie ADC в OSPF-домен. При этом только основной узел пары будет анонсировать маршрут на адрес сервиса.

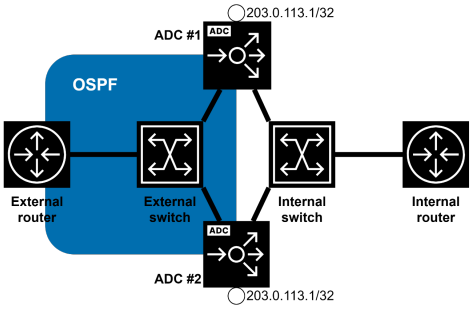


Рис. 6: Рис. 4

Пример

Сервис доступен по адресу `203.0.113.1`. Необходимо, чтобы основной узел пары анонсировал маршрут на префикс `203.0.113.1/32`.

Сначала задайте адрес `203.0.113.1/32` на *интерфейсе lo* обоих узлов пары, а также собственный адрес узла для идентификатора маршрутизатора (`203.0.113.11/32` на основном и `203.0.113.12/32` на резервном узле, см. *Идентификатор маршрутизатора в паре*):

```
$$ configuration
## set system interface lo ip address 203.0.113.1/32
## set system interface lo ip address 203.0.113.11/32
```

Интерфейсы основного узла:

```
ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default␣
↪qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet 203.0.113.1/32 scope global lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group␣
↪default qlen 1000
link/ether 00:0c:29:96:0c:dc brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 10.65.1.7/24 brd 10.65.1.255 scope global ens33
```

```
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe96:cdc/64 scope link
valid_lft forever preferred_lft forever
```

Интерфейсы резервного узла:

```
ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default␣
↪qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet 203.0.113.1/32 scope global lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group␣
↪default qlen 1000
link/ether 00:0c:29:c1:36:b4 brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 10.65.1.8/24 brd 10.65.1.255 scope global ens33
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fec1:36b4/64 scope link
valid_lft forever preferred_lft forever
```

Далее на узле Active включите OSPF на интерфейсе `ens33` и перераспределите в OSPF адрес сервиса через карту маршрутов:

```
$$ configuration
## routing prefix-list svc seq 5 permit 203.0.113.1/32
## routing route-map svc permit 10 match-prefix-list svc
## routing ospf 1
## routing ospf 1 interface ens33 area 0
## routing ospf 1 redistribute connected route-map svc
```

После внесения изменений *синхронизируйте конфигурации в паре*: синхронизация копирует настройки маршрутизации на узел Standby, где Angie ADC сам ограничивает анонсы (см. *Динамическая маршрутизация в паре высокой доступности*). Карта маршрутов `svc` пропускает в OSPF только адрес сервиса, без собственных адресов узлов на `lo`.

Проверка

Проверка на маршрутизаторе или L3-коммутаторе (список OSPF-соседей):

```
R1#sho ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:39    10.65.1.7       GigabitEthernet0/0
2.2.2.2           1   FULL/DR         00:00:38    10.65.1.8       GigabitEthernet0/0
```

Соседство по протоколу OSPF устанавливают оба узла пары одновременно:

```
R1#sho ip ro os
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set
203.0.113.0/32 is subnetted, 1 subnets
O E2     203.0.113.1 [110/20] via 10.65.1.7, 00:52:39, GigabitEthernet0/0
```

Маршрут анонсируется только одним узлом. В этом можно убедиться, если просмотреть список LSA5 в LSDB маршрутизатора:

```
R1#sho ip os database external
    OSPF Router with ID (10.65.1.140) (Process ID 1)

        Type-5 AS External Link States
Routing Bit Set on this LSA in topology Base with MTID 0
LS age: 1341
Options: (No TOS-capability, No DC, Upward)
LS Type: AS External Link
Link State ID: 203.0.113.1 (External Network Number )
Advertising Router: 1.1.1.1
LS Seq Number: 80000005
Checksum: 0x575B
Length: 36
Network Mask: /32
Metric Type: 2 (Larger than any link state path)
MTID: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 0
```

Теперь выключите основной узел и проверьте изменения:

```
R1#sho ip os ne

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:33    10.65.1.8       GigabitEthernet0/0
```

```
R1#sho ip os da ex
    OSPF Router with ID (10.65.1.140) (Process ID 1)

        Type-5 AS External Link States
Routing Bit Set on this LSA in topology Base with MTID 0
LS age: 114
Options: (No TOS-capability, No DC, Upward)
LS Type: AS External Link
Link State ID: 203.0.113.1 (External Network Number )
Advertising Router: 2.2.2.2
LS Seq Number: 80000001
Checksum: 0x139B
Length: 36
Network Mask: /32
Metric Type: 2 (Larger than any link state path)
MTID: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 0
```

```
R1#sho ip ro os
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set
203.0.113.0/32 is subnetted, 1 subnets
O E2     203.0.113.1 [110/20] via 10.65.1.8, 00:01:57, GigabitEthernet0/0
R1#
```

Остался только один OSPF-сосед, который стал основным узлом пары. Теперь он анонсирует маршрут до префикса `203.0.113.1/32`.

4.1.3.4 BGP

Маршрутизатор устанавливает BGP-сессии с обоими узлами пары. Обе BGP-сессии активны одновременно, но анонс префикса производится только с основного узла.

Пример типовой схемы:

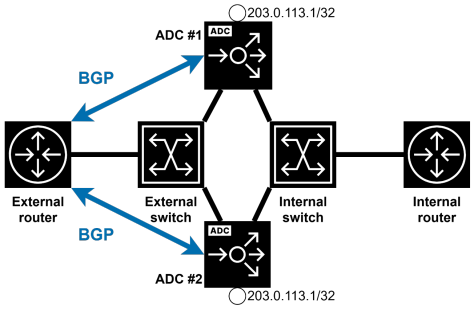


Рис. 7: Рис. 5

Пример

Сервис доступен по адресу `203.0.113.1`. Основной узел пары будет анонсировать маршрут на префикс `203.0.113.1/32`.

Сначала задайте адрес `203.0.113.1/32` на *интерфейсе lo* обоих узлов пары, а также собственный адрес узла для идентификатора маршрутизатора (`203.0.113.11/32` на основном и `203.0.113.12/32` на резервном узле, см. *Идентификатор маршрутизатора в паре*):

```
$$ configuration
## set system interface lo ip address 203.0.113.1/32
## set system interface lo ip address 203.0.113.11/32
```

Интерфейсы основного узла:

```
ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default␣
↪qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

```
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet 203.0.113.1/32 scope global lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group␣
↪default qlen 1000
link/ether 00:0c:29:96:0c:dc brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 10.65.1.7/24 brd 10.65.1.255 scope global ens33
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe96:cdc/64 scope link
valid_lft forever preferred_lft forever
```

Интерфейсы резервного узла:

```
ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default␣
↪qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet 203.0.113.1/32 scope global lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group␣
↪default qlen 1000
link/ether 00:0c:29:c1:36:b4 brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 10.65.1.8/24 brd 10.65.1.255 scope global ens33
valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fec1:36b4/64 scope link
valid_lft forever preferred_lft forever
```

На узле Active настройте BGP так, чтобы узел устанавливал соединение с маршрутизатором (`10.65.1.140`), и перераспределите в BGP адрес сервиса через карту маршрутов:

```
$$ configuration
## routing prefix-list svc seq 5 permit 203.0.113.1/32
## routing route-map svc permit 10 match-prefix-list svc
## routing bgp asn 65001
## routing bgp neighbor 10.65.1.140 remote-as 65001
## routing bgp redistribute connected route-map svc
```

Запустите *синхронизацию конфигураций* между узлами пары высокой доступности, чтобы настроить BGP на узле Standby.

Примечание

Не настраивайте маршрутизацию на узле Standby отдельно: следующая синхронизация заменит ее настройками узла Active.

Проверка

Пример конфигурации со стороны маршрутизатора:

```
router bgp 65001
bgp log-neighbor-changes
neighbor 10.65.1.7 remote-as 65001
neighbor 10.65.1.8 remote-as 65001
```

Убедитесь, что маршрутную информацию отправляет только основной узел (`10.65.1.7`):

```
R1#sho ip bg su
BGP router identifier 10.65.1.140, local AS number 65001
BGP table version is 17, main routing table version 17
2 network entries using 296 bytes of memory
2 path entries using 128 bytes of memory
1/1 BGP path/bestpath attribute entries using 136 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 560 total bytes of memory
BGP activity 4/2 prefixes, 13/11 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/
↪PfxRcd
10.65.1.7       4        65001    3283    3206       17    0    0 02:43:57        2
10.65.1.8       4        65001      28      29       17    0    0 00:01:17        0
R1#sho ip bgp
BGP table version is 17, local router ID is 10.65.1.140
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network          Next Hop            Metric LocPrf Weight Path
r>i 10.65.1.0/24     10.65.1.7                0    100      0 ?
*>i 203.0.113.1/32   10.65.1.7                0    100      0 ?
R1#sho ip ro bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set
203.0.113.0/32 is subnetted, 1 subnets
B        203.0.113.1 [200/0] via 10.65.1.7, 02:45:34
R1#
```

Теперь выключите основной узел и проверьте изменения:

```
R1#sho ip bg su
BGP router identifier 10.65.1.140, local AS number 65001
BGP table version is 21, main routing table version 21
2 network entries using 296 bytes of memory
2 path entries using 128 bytes of memory
1/1 BGP path/bestpath attribute entries using 136 bytes of memory
```

```
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 560 total bytes of memory
BGP activity 6/4 prefixes, 15/13 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/
↪PfxRcd
10.65.1.7       4        65001       0       0        1    0    0 00:07:13 Active
10.65.1.8       4        65001     228     222       21    0    0 00:11:04        2
```

Остался только один BGP-сосед (`10.65.1.8`), который стал основным узлом пары. Теперь он анонсирует маршрут до префикса `203.0.113.1/32`:

```
R1#sho ip bg
BGP table version is 21, local router ID is 10.65.1.140
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network          Next Hop            Metric LocPrf Weight Path
r>i 10.65.1.0/24     10.65.1.8                0    100      0 ?
*>i 203.0.113.1/32   10.65.1.8                0    100      0 ?
R1#sho ip ro bg
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set
203.0.113.0/32 is subnetted, 1 subnets
B        203.0.113.1 [200/0] via 10.65.1.8, 00:05:50
```

Анонсы ограничивает исходящий фильтр, который Angie ADC добавляет на узле Standby каждому BGP-соседу (см. *Динамическая маршрутизация в паре высокой доступности*). Фрагмент конфигурации FRR узла Standby:

```
access-list angie-ha-standby seq 5 deny any
!
router bgp 65001
 no bgp default ipv4-unicast
 neighbor 10.65.1.140 remote-as 65001
 !
 address-family ipv4 unicast
  redistribute connected route-map svc
  neighbor 10.65.1.140 activate
  neighbor 10.65.1.140 distribute-list angie-ha-standby out
 exit-address-family
exit
```

На узле Active фильтра нет. При смене ролей фильтр переходит на новый узел Standby.

4.1.4 Управление парой

В этой статье:

- *Просмотр информации о паре*
- *Обновление конфигурации и синхронизация*
- *Настройка протокола опроса доступности узлов*
- *Удаление пары*

См. также *Привязка клиентских сессий* (sticky sessions).

4.1.4.1 Просмотр информации о паре

1. Откройте веб-интерфейс Angie ADC на одном из узлов пары.
2. Перейдите в раздел `Высокая доступность и кластеризация` → `Высокая доступность`.

   Откроется экран просмотра свойств пары.

Отображаются следующие параметры:

`Состояние пары`	Состояние пары высокой доступности. Возможны следующие варианты: • `on` — статус отображается при нормальной работе пары. Высокая доступность обеспечивается. • `failed` — статус отображается после попытки запуска пары, если пару сформировать не удалось. Синхронизация и обмен данными между узлами в паре невозможны. Высокая доступность не обеспечивается. • `starting` — пара запускается. Статус отображается сразу после создания пары в процессе ее конфигурации и синхронизации. • `not_reachable` — статус отображается, когда узел не получает ответ от соседнего узла по всем интерфейсам, участвующим в паре, в течение заданного таймаута (например из-за сетевой проблемы или недоступности соседнего узла). Если резервный узел фиксирует недоступность основного узла, выполняется переключение ролей: резервный узел становится основным. При этом для соседнего узла будет отображаться его последняя известная роль. **Примечание** Рекомендуется проверить соседний узел и, если требуется, восстановить его связность и работоспособность. **Совет** Чтобы убрать сообщение о смене статуса в паре, запустите ручную синхронизацию конфигураций по кнопке `Синхронизировать`.
`Последнее изменение`	Дата и время последнего изменения в паре, например смены ролей узлов.
`Узел`	Идентификация узла пары, на котором открыт веб-интерфейс Angie ADC: • `Текущий` — узел, на котором в данный момент открыт веб-интерфейс Angie ADC со свойствами пары; • `Соседний` — второй узел пары.
`IP-адрес узла`	IP-адрес узла, используемый для взаимодействия в паре. **Предупреждение** Не рекомендуется изменять настройки интерфейсов узлов, объединенных в пару высокой доступности, иначе пара может потерять связность и работоспособность.
`Роль узла`	Роль узла пары: • `Основной` — обрабатывает трафик (находится в режиме Active). • `Резервный` — находится в режиме ожидания (Standby).

4.1.4.2 Обновление конфигурации и синхронизация

После внесения изменений в конфигурацию основного узла необходимо вручную запустить синхронизацию пары, чтобы перенести внесенные изменения на резервный узел.

Чтобы обновить конфигурацию на узлах пары, выполните следующие действия:

1. Внесите необходимые изменения в конфигурацию основного узла.
2. Откройте веб-интерфейс Angie ADC на любом узле пары.

3. Перейдите в раздел `Высокая доступность и кластеризация` → `Высокая доступность`.

   Откроется экран просмотра свойств пары.

4. Нажмите `Синхронизировать`.

Конфигурация основного узла будет перенесена на резервный узел, на экране отобразится сообщение `Пара синхронизирована`. Если синхронизация завершится с ошибкой, на экране отобразится сообщение `Ошибка синхронизации`.

На резервном узле перезаписываются следующие файлы и папки:

- конфигурация балансировщика нагрузки;
- сертификаты и ключи балансировщика нагрузки;
- конфигурация маршрутизации (VRRP, BGP, OSPF);
- конфигурация GSLB;
- все файлы в папках `/etc/angie/crt` и `/etc/angie-lb/crt`;
- все файлы в папке `/var/transfer`.

Остальные файлы резервного узла, если они находятся вне указанных папок (например, файл лицензии), удалены не будут.

4.1.4.3 Настройка протокола опроса доступности узлов

Чтобы изменить настройки протокола опроса доступности узлов, выполните следующие действия:

1. Откройте веб-интерфейс Angie ADC на одном из узлов пары.
2. Перейдите в раздел `Высокая доступность и кластеризация` → `Высокая доступность`.

   Откроется экран просмотра узлов, входящих в пару.

3. В блоке `Проверка доступности узлов` укажите следующие данные:

   - `Интервал отправки запросов (мс)`

     Интервал отправки запросов резервным узлом для проверки доступности основного узла. По умолчанию запросы отправляются каждые 250 мс. Допустимый диапазон значений — от 200 до 1000 мс.

   - `Таймаут ожидания ответа (с)`

     Таймаут ожидания ответа от интерфейса основного узла. Если с момента получения последнего успешного ответа прошло больше заданного времени, интерфейс будет считаться недоступным. При недоступности всех интерфейсов основного узла произойдет переключение ролей. По умолчанию — `3` секунды. Допустимый диапазон значений — от 1 до 3 секунд.

4. Нажмите `Сохранить`.

Новые настройки будут применены сразу.

4.1.4.4 Удаление пары

> **Примечание**
>
> Удаление пары возможно только с основного узла.

Чтобы удалить пару, выполните следующие действия:

1. Откройте веб-интерфейс Angie ADC на узле, который является основным в паре на данный момент.

2. Перейдите в раздел `Высокая доступность и кластеризация` → `Высокая доступность`.

   Откроется экран просмотра свойств пары.

3. Нажмите `Расформировать` и подтвердите удаление.

4. На бывшем резервном узле выполните команду *no ha standby*, чтобы снять ограничения роли Standby: до этого его группы VRRP остаются выключенными, а маршруты не анонсируются (см. *Динамическая маршрутизация в паре высокой доступности*).

Конфигурация пары высокой доступности будет удалена. Конфигурации узлов сохранятся, узлы продолжат функционировать независимо друг от друга.

4.1.5 Привязка клиентских сессий

В паре высокой доступности поддерживается привязка клиентских сессий (sticky sessions). При переключении узлов все запросы клиента в рамках одной сессии будут по-прежнему перенаправляться на один и тот же бэкенд-сервер, т. е. клиентские сессии будут сохраняться.

Информация о клиентских сессиях хранится в хранилище сессий Angie ADC. Привязка сессий реализуется с помощью директивы sticky (режим `learn` с `remote_action`). Для включения функции необходимо указать адрес хранилища сессий Angie ADC (`http://127.0.0.1:3380/sticky_session`) в конфигурации балансировщика нагрузки.

Пример конфигурации:

```
http {

    upstream sticky_test {

        server 127.0.0.1:8091 sid=web-server-01;
        server 127.0.0.1:8092 sid=web-server-02;

        sticky learn
            lookup=$http_x_userid
            remote_action=/create_session
            remote_result=$upstream_http_x_sid;
    }

    server {

        listen *:80;

        location / {

            proxy_pass http://sticky_test/;

        }

        location /create_session {

            internal;
            proxy_set_header X-Sticky-Sessid $sticky_sessid;
            proxy_set_header X-Sticky-Sid    $sticky_sid;
            proxy_set_header X-Sticky-Last   $msec;
            proxy_method POST;
            proxy_pass http://127.0.0.1:3380/sticky_session;
            proxy_connect_timeout 1s;
            proxy_read_timeout    1s;
        }
```

```
    }
}
```

4.2 IP-маршрутизация

Angie ADC обеспечивает высокую доступность сервисов средствами маршрутизации: протоколом VRRP и динамической маршрутизацией по BGP и OSPF в вариантах Active-Standby и Active-Active. Также поддерживается статическая маршрутизация, использование протокола BFD для уменьшения времени реакции на события и механизм RHI, который отзывает анонс адреса сервиса при недоступности апстрима.

В этом разделе:

- *VRRP*
- *Настройка динамической маршрутизации*
- *BGP-маршрутизация*
- *OSPF-маршрутизация*
- *Статическая маршрутизация*
- *Использование протокола BFD для уменьшения времени реакции*
- *Настройка RHI*
- *Настройка ECMP*

Примечание

Рекомендуется резервировать все компоненты инфраструктуры. Отказ сопутствующей инфраструктуры (например выход из строя вышестоящего маршрутизатора или сбой серверов) выходит за рамки решения высокой доступности Angie ADC.

Пример отказоустойчивой инфраструктуры:

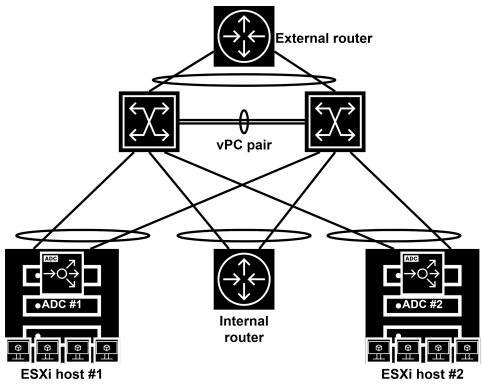


Рис. 8: Рис. 1

4.2.1 VRRP

VRRP (Virtual Router Redundancy Protocol) позволяет нескольким узлам Angie ADC обслуживать общий виртуальный IPv4-адрес (VIP). Узлы с одним VIP образуют группу VRRP. В группе один узел становится Master и обслуживает VIP, остальные — Backup. Если Master перестает участвовать

в VRRP, его роль принимает один из резервных узлов. Так обеспечивается отказоустойчивость в сетях со статической маршрутизацией.

VRRP переносит только VIP. Балансируемый сервис, его сертификаты, доступ к серверам и маршруты нужно настроить на всех узлах, которые могут стать Master. Уже установленные пользовательские соединения при переключении не сохраняются.

4.2.1.1 Где настраивается VRRP

- Группы VRRP создаются, изменяются и удаляются в *CLI*, в режиме `configuration`, командой *vrrp*. Команда меняет группы того узла, к которому подключен CLI, поэтому каждый участник группы настраивается отдельно.
- В веб-интерфейсе группы узла доступны только для просмотра: `Система` → `Сетевые настройки` → вкладка узла → блок `Группы VRRP` (подробнее см. adc_console_system_network). Таблица показывает сохраненную конфигурацию — интерфейс, VRID и VIP — без приоритета, флагов и текущей роли.
- Интерфейс, на котором есть группа VRRP, нельзя удалить или переименовать в веб-интерфейсе, пока группа не удалена в CLI.

Перед созданием группы подготовьте в *сетевых настройках* узла родительский интерфейс (физический, VLAN или bond) и его собственный IPv4-адрес. Сохраните сетевые настройки и дождитесь их применения.

4.2.1.2 Ограничения

- Поддерживается только виртуальный IPv4-адрес, в том числе с VRRPv3.
- В группе один VIP.
- Отслеживания состояния интерфейсов, маршрутов или приложения (VRRP tracking) нет: VIP переходит на резервный узел, только когда Master перестает отправлять анонсы VRRP.
- В *паре высокой доступности* резервный узел (Standby) не участвует в группах VRRP, даже если они включены.
- В паре высокой доступности группы настраиваются на узле Active: синхронизация пары заменяет группы резервного узла группами основного (см. *VRRP*).

Для участников одной группы VRRP использует multicast-адрес `224.0.0.18` и IP-протокол 112 (это номер протокола IP, а не порт TCP или UDP). Участники должны находиться в одном сетевом сегменте; разрешите этот трафик в сети и на межсетевых экранах. Если узлы работают в виртуальной среде, разрешите в ней виртуальные MAC-адреса VRRP (для VMware ESXi см. *Предварительная настройка для VMware ESXi*).

В этом разделе:

- *Предварительная настройка для VMware ESXi*
- *Режим резервирования (Active-Standby)*
- *Режим распределения нагрузки (Active-Active)*
- *Команды VRRP*
- *Диагностика VRRP*

Предварительная настройка для VMware ESXi

Если Angie ADC развернут на VMware ESXi, то для работы VRRP необходимо дополнительно настроить сетевые политики безопасности ESXi и разрешить передачу трафика с портов, участвующих в VRRP.

Настройка VMware ESXi до версии 6.7

Для VMware ESXi версии до версии 6.7 необходимо создать отдельную порт-группу (Port Group) для портов, участвующих в VRRP, и включить для нее настройки **Promiscuous mode** и **Forged Transmits**.

1. Создайте отдельную порт-группу (Port Group) для портов, участвующих в VRRP.

   Пример пути для создания порт-группы: `Host` → `Configure` → `Networking` → `Port Groups` → `Add Port Group`.

2. Задайте следующие значения для передачи трафика при изменении MAC-адреса для новой порт-группы:

   - `Promiscuous Mode` – `Accept`.
   - `Forged transmits` – `Accept`.

   Пример пути для настройки порт-группы: `Host` → `Configure` → `Networking` → `Port Groups` → `<порт_группа>` → `Edit Settings` → `Security`.

3. Обеспечьте размещение виртуальных машин Angie ADC на разных ESXi-хостах кластера. Для этого запретите DRS-перемещение виртуальных машин Angie ADC на один хост с помощью запрещающего правила Anti-Affinity.

   Пример пути для настройки правила: `Host` → `Configure` → `Configuration` → `VM/Host Rules` → `Add`.

   В открывшемся окне заполните необходимые поля и укажите виртуальные машины Angie ADC.

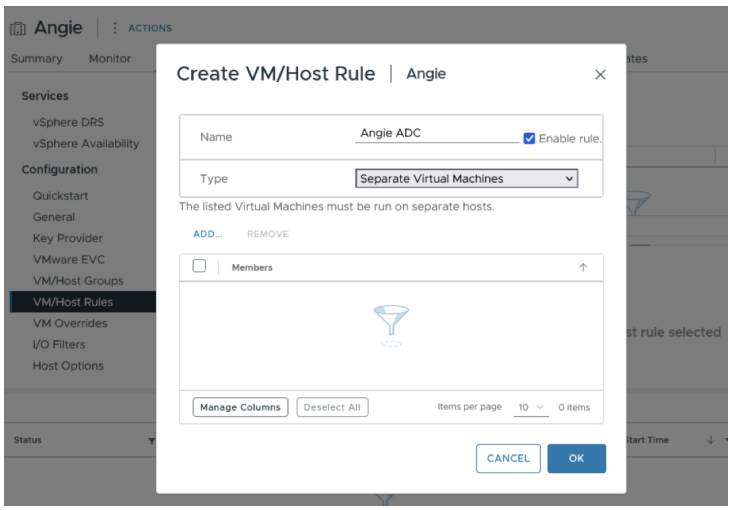


Рис. 1: создание запрещающего правила для ESXi до версии 6.7.

Общая схема будет такой: устройства Angie ADC подключены через отдельную порт-группу, на которой включен режим Promiscuous:

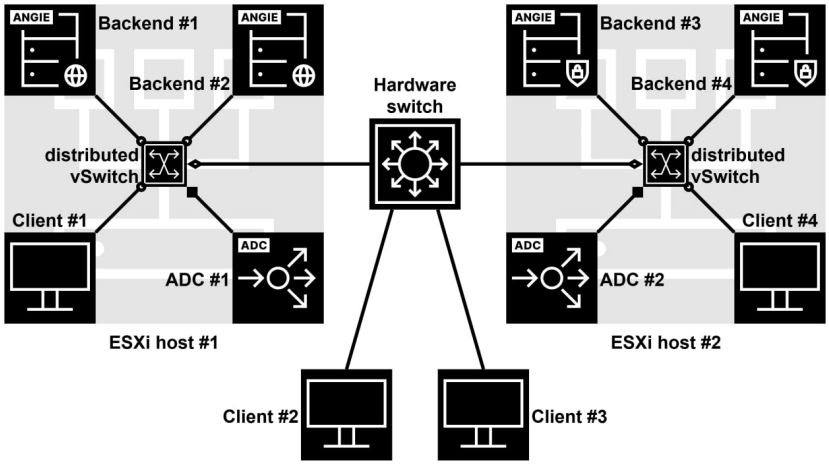


Рис. 2: подключение Angie ADC для ESXi до версии 6.7.

Настройка VMware ESXi версии 6.7+

Для VMware ESXi версии 6.7+ необходимо настроить обычную порт-группу (Port Group) для портов, участвующих в VRRP, и включить для нее настройки **Forged Transmits** и **MAC Learning**.

1. Подключитесь к vCenter Server и перейдите `Inventory` → `Networks`.
2. Выберите DSwitch и щелкните правой кнопкой мыши по нужной порт-группе. В контекстном меню выберите пункт `Edit Settings` → `Security`.
3. Задайте следующие значения для передачи трафика при изменении MAC-адреса:
   - `Promiscuous Mode` – `Reject`.
   - `MAC address changes` – `Reject`.
   - `Forged transmits` – `Accept`.
4. В блоке `MAC Learning` установите `Status` в значение `Enabled`.

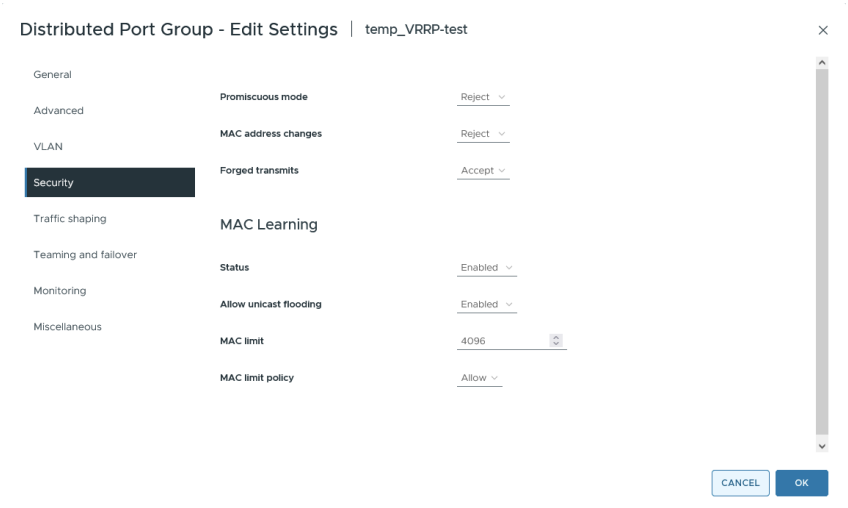


Рис. 3: настройка порт-группы на ESXi 6.7+.

Общая схема будет такой: устройства Angie ADC подключены через обычные порт-группы, при этом включена политика, разрешающая подмену MAC-адресов в Distributed Virtual Port Group (DVPG.macManagementPolicy=yes):

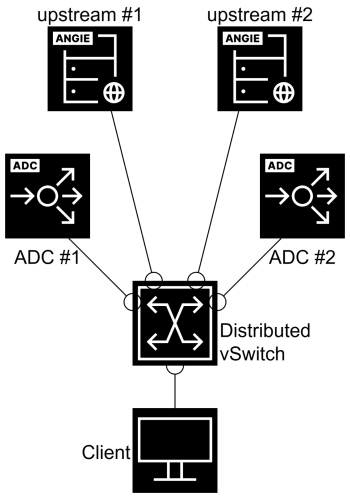


Рис. 4: подключение Angie ADC для ESXi версии 6.7+.

Режим резервирования (Active-Standby)

В этом разделе описана настройка высокой доступности с использованием протокола VRRP в режиме резервирования (Active-Standby). Для настройки используется *интерфейс командной строки (CLI) Angie ADC*.

Также можно посмотреть следующие статьи:

- *Настройка режима распределения нагрузки (Active-Active) с помощью протокола VRRP*;
- *Команды VRRP*;
- *Диагностика VRRP*.

Введение

Для обеспечения отказоустойчивости нужны две системы балансировки Angie ADC — основная и резервная. Резервная система Angie ADC будет принимать нагрузку при отказе основной. Автоматическое переключение между двумя системами балансировки Angie ADC можно реализовать с помощью протокола VRRP. Пример настройки приведен ниже.

Примечание

Резервирование других сетевых компонентов (маршрутизаторы, коммутаторы, межсетевые экраны) выходит за рамки настоящей статьи.

Пример типового участка сети с системами балансировки Angie ADC (ADC #1 и ADC #2):

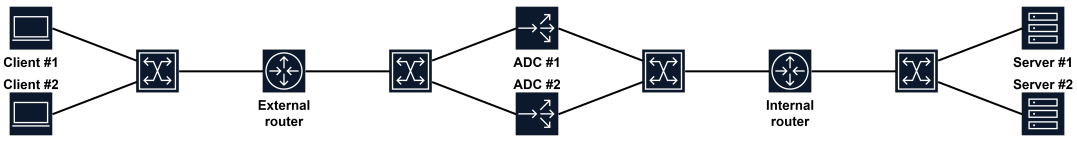


Рис. 1

Добавим *IP-адресацию*:

- В сегменте сети, куда подключаются External router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.0.0/24`.

- В сегменте сети, куда подключаются Internal router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.1.0/24`.
- Четвертый октет адреса для каждого устройства (в рамках соответствующей подсети) показан на схеме ниже.

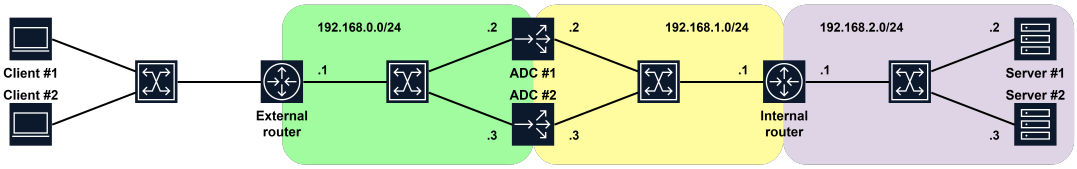


Рис. 2

Адресация клиентов не приводится, так как в данном случае мы будем считать, что их адреса формально не определены, то есть, они могут подключаться из любой сети, включая сеть интернет. Для этого на ADC #1 и ADC #2 необходимо указать адрес правого интерфейса маршрутизатора External router (`192.168.0.1`) в качестве шлюза по умолчанию.

Адрес сервиса может быть задан на *интерфейсе lo* каждой системы балансировки, либо это может быть виртуальный адрес, используемый протоколом VRRP. Первый способ будет более гибким.

Если адрес сервиса задан на интерфейсе `lo` (на схеме ниже это адрес `2.2.2.2`), необходимо добавить статический маршрут на этот адрес на маршрутизаторе External router. Причем в качестве next-hop необходимо использовать виртуальный адрес VRRP, за счет чего достигается отказоустойчивость решения.

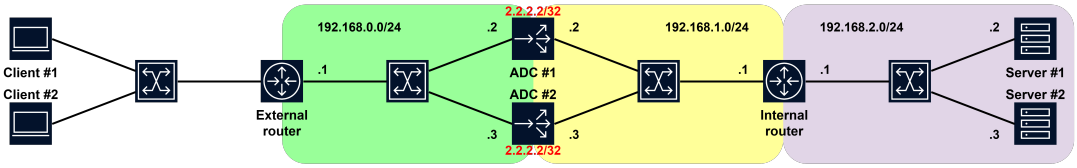


Рис. 3

При использовании виртуального адреса VRRP в качестве адреса сервиса (на схеме ниже это `192.168.0.10`) настройка соответствующих статических маршрутов на маршрутизаторе External router не требуется. Виртуальный адрес VRRP находится в одной подсети с интерфейсами маршрутизатора с точки зрения маршрутизатора External router.

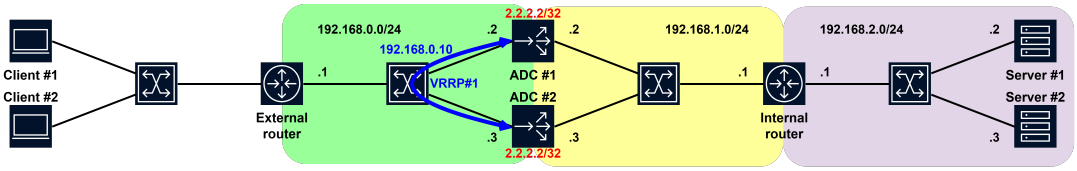


Рис. 4

Также допускается использование VRRP и при работе системы балансировки Angie ADC в «одноруком» режиме.

Обработка типовых сбоев

Ниже описаны сценарии работы Angie ADC при сбоях.

Полный отказ ADC #1

При полном отказе или отключении от сети ADC #1 происходят перевыборы VRRP-мастера. Переключение на резервную систему ADC #2 производится автоматически. Никакие дополнительные настройки не требуются.

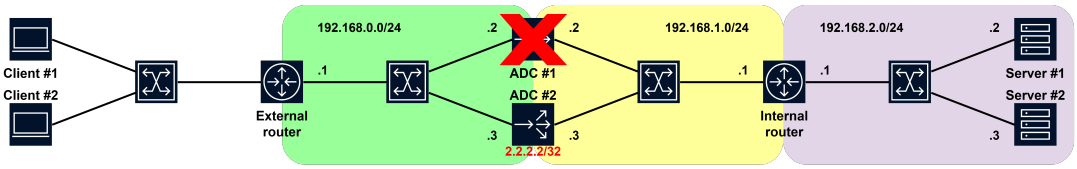


Рис. 5

Отказ внешнего интерфейса ADC #1

Предлагаемая схема не предполагает возможности отслеживания частичных отказов и реагирования на них (пример ниже).

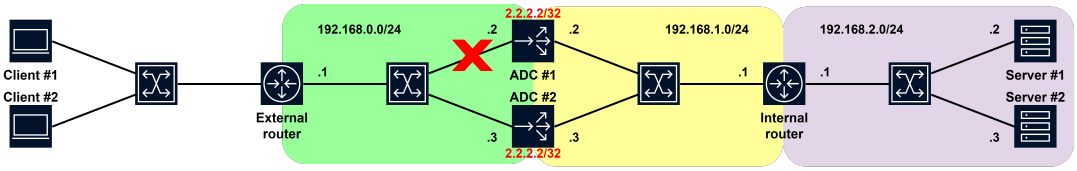


Рис. 6

В случае частичного отказа, как на схеме выше, ADC #1 перестает рассылать сообщения VRRP. ADC #2 начинает считать себя мастером, что заставляет виртуальную машину отвечать на ARP-запросы об адресе `192.168.0.10`, а также обрабатывать пользовательский трафик. Обратный трафик (от серверов в сторону клиентов) будет проходить через ADC #2, так как ADC #2 устанавливает сессии до серверов с адреса своего внутреннего интерфейса.

Примечание

IP transparency на данном этапе обеспечить невозможно. Для работы IP transparency требуется наличие маршрута по умолчанию на маршрутизаторе Internal router. Если прописать маршрут по умолчанию через ADC #1, то отказ внешнего интерфейса ADC #1 приведет к невозможности доставки трафика и его отбрасыванию (black hole). Решить эту проблему можно за счет использования протокола VRRP как на внешнем, так и на внутреннем интерфейсах. Причем состояние групп должно быть согласованным, то есть если для внешней сети мастером является система балансировки ADC #2, то и для внутренней сети ADC #2 также должна являться мастером.

Отказ линка между ADC #1 и Internal router

Отказ линка между ADC #1 и маршрутизатором Internal router более сложная ситуация: если ADC #1 сохраняет за собой роль мастера, то трафик от клиентов до серверов будет все еще передаваться через ADC #1, хотя реальные сервера для системы балансировки ADC #1 уже недостижимы. Таким образом, мы получаем классический пример black hole:

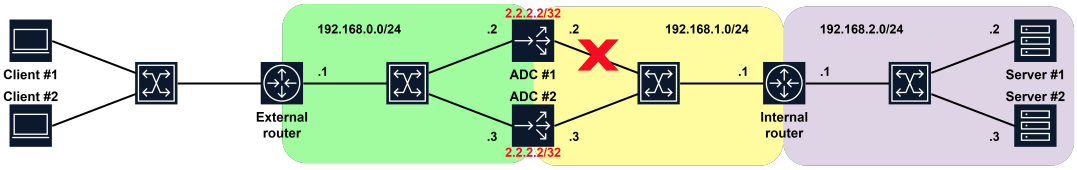


Рис. 7

Чтобы избежать этой проблемы, необходимо, чтобы ситуация отказа только одного из линков была невозможной, т. е. нужно обеспечить отказоустойчивое подключение к сети для хоста виртуализации, на котором работает ADC.

Рекомендованная схема подключения:

- Объединить в одну LAG-группу все физические интерфейсы хоста виртуализации и использовать этот виртуальный LAG-интерфейс в качестве транка, то есть передавать по нему тегированными несколько виртуальных сетей (один VLAN для external сети, второй VLAN для internal сети).
- Для резервирования коммутаторов можно использовать технологию vPC или стекирование, пример представлен на схеме ниже.

Из соображений простоты на схеме не отображено резервирование внешнего и внутреннего маршрутизаторов.

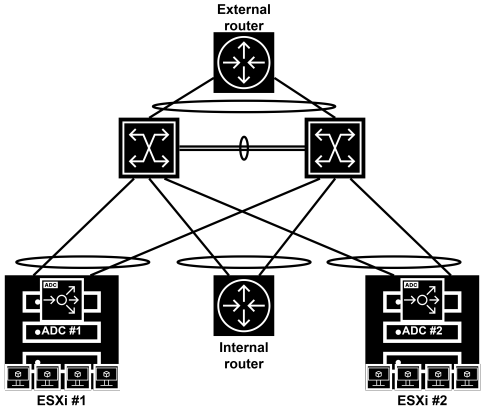


Рис. 8

Примечание

Отслеживания (VRRP tracking) в Angie ADC нет: при таком отказе ADC #1 остается Master. Поэтому важно, чтобы отказ только одного из линков был невозможен.

Настройка VRRP

Перед настройкой задайте на обоих узлах собственные адреса интерфейса `ens33` (в примере `192.168.0.2/24` на ADC #1 и `192.168.0.3/24` на ADC #2). Каждый узел настраивается отдельно: подключитесь к *CLI* нужного узла и перейдите в режим `configuration`. В *паре высокой доступности* настраивайте группы на узле Active: синхронизация пары заменяет группы резервного узла группами основного. Каждая команда применяется сразу, дождитесь ее завершения.

Создание группы

Группа создается командой с VIP; остальные параметры необязательны. На обоих узлах выполните:

```
$$ configuration
## vrrp 1 interface ens33 address 192.168.0.10/24
```

Версия 3, интервал анонсов 1000 мс и включенный preempt используются по умолчанию. Полный список параметров см. в *Команды VRRP*.

Приоритет

Чтобы Master была система ADC #1, задайте ей приоритет выше, чем у ADC #2. Приоритет по умолчанию — 100.

На ADC #1:

```
## vrrp 1 interface ens33 priority 110
```

На ADC #2:

```
## vrrp 1 interface ens33 priority 90
```

Проверьте сохраненные группы на обоих узлах:

```
## vrrp show
```

Preempt

Параметр `preempt` включен по умолчанию: восстановившийся узел с большим приоритетом инициирует перевыборы и забирает роль Master. Если автоматический возврат на ADC #1 не нужен, выключите вытеснение на нем:

```
## no vrrp 1 interface ens33 preempt
```

Чтобы ни один узел не вытеснял другой, выполните эту команду на обоих. Резервный узел принимает VIP при отказе Master независимо от этого параметра. Включить вытеснение снова:

```
## vrrp 1 interface ens33 preempt
```

Маршрут на маршрутизаторе

Если адрес сервиса задан на интерфейсе `lo`, на внешнем маршрутизаторе задайте статический маршрут к нему через VIP, например:

```
External(config)#ip route 2.2.2.2 255.255.255.255 192.168.0.10
```

Проверка работы

Текущую роль узла показывает команда `show vrrp` в основном режиме CLI (вне режима `configuration`).

Убедимся, что ADC #1 является мастером:

```
$$ show vrrp interface ens33 1 summary
Interface VRID Priority IPv4 IPv6 State (v4) State (v6)
------------------------------------------------------------------------
ens33 1 110 1 0 Master Backup
```

Убедимся, что ADC #2 не обладает ролью мастера:

```
$$ show vrrp interface ens33 1 summary
Interface VRID Priority IPv4 IPv6 State (v4) State (v6)
------------------------------------------------------------------------
ens33 1 90 1 0 Backup Backup
```

Отключим теперь систему балансировки ADC #1 и убедимся, что ADC #2 приняла на себя роль мастера:

```
$$ show vrrp interface ens33 1 summary
Interface VRID Priority IPv4 IPv6 State (v4) State (v6)
------------------------------------------------------------------------
ens33 1 90 1 0 Master Backup
```

Примечание

В момент переезда роли Master на вторую систему балансировки ADC возможны кратковременные перерывы обработки трафика, вызванные задержками обнаружения падения активной ноды. Характерное время переключения ~3 секунды. Ускорить процедуру переключения можно за счет уменьшения параметра `advertisement-interval` (см. *Команды VRRP*).

Заново включим систему балансировки ADC #1. При включенной опции `preempt` (по умолчанию) ADC #1 снова становится Master, при выключенной Master остается ADC #2 (см. *Preempt*).

Состояние параметра `preempt` и другие сведения о группе выводит команда:

```
$$ show vrrp interface ens33 1
Virtual Router ID 1
Protocol Version 3
Autoconfigured No
Shutdown No
Interface ens33
VRRP interface (v4) vrrp4-ens33-1
VRRP interface (v6) None
Primary IP (v4) 192.168.0.3
Primary IP (v6) ::
Virtual MAC (v4) 00:00:5e:00:01:01
Virtual MAC (v6) 00:00:5e:00:02:01
Status (v4) Master
Status (v6) Initialize
Priority 110
Effective Priority (v4) 110
Effective Priority (v6) 110
Preempt Mode No
Accept Mode Yes
Checksum with IPv4 Pseudoheader Yes
Advertisement Interval 1000 ms
Master Advertisement Interval (v4) Rx 1000 ms (stale)
Master Advertisement Interval (v6) Rx 0 ms (stale)
Advertisements Tx (v4) 1163
Advertisements Tx (v6) 0
Advertisements Rx (v4) 0
Advertisements Rx (v6) 0
Gratuitous ARP Tx (v4) 1
Neigh. Adverts Tx (v6) 0
State transitions (v4) 2
State transitions (v6) 0
Skew Time (v4) 600 ms
```

```
Skew Time (v6) 0 ms
Master Down Interval (v4) 3600 ms
Master Down Interval (v6) 0 ms
IPv4 Addresses 1
.............................. 192.168.0.10
IPv6 Addresses 0
```

Вне зависимости от того, какая система балансировки активна в данный момент, на маршрутизаторах в ARP-записи об адресе `192.168.0.10` будет один и тот же MAC-адрес: `00-00-5e-00-01-01` (при использовании первой VRRP-группы).

```
External#sho ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.0.10 - 0000.5e00.0101 ARPA GigabitEthernet0/0
```

Это означает, что при отказе одной из систем балансировки и аварийном переключении на вторую, единственное изменение, которое должно произойти в сети – переобучение коммутаторов, то есть потребуется актуализировать таблицы коммутации для адреса `00-00-5e-00-01-01`.

Заключение

С помощью протокола VRRP можно построить отказоустойчивое решение по балансировке нагрузки на сервера там, где использование протоколов динамической маршрутизации невозможно по той или иной причине.

Порядок проверки переключения и устранение типовых проблем описаны в *Диагностика VRRP*.

Режим распределения нагрузки (Active-Active)

В этом разделе описана настройка высокой доступности с использованием протокола VRRP в режиме распределения нагрузки (Active-Active). Для настройки используется *интерфейс командной строки (CLI) Angie ADC*.

Также можно посмотреть следующие статьи:

- *Настройка режима резервирования (Active-Standby) с помощью протокола VRRP*;
- *Команды VRRP*;
- *Диагностика VRRP*.

Введение

Реализация полноценной схемы распределения нагрузки (Active-Active) не предусмотрена протоколом VRRP, но это ограничение можно обойти. Для этого рассмотрим два сценария подключения Angie ADC:

- между клиентами и системами балансировки установлен хотя бы один маршрутизатор;
- между клиентами и системами балансировки нет маршрутизатора.

Подключение Angie ADC с маршрутизатором

Пример сети с маршрутизатором между клиентами и системами балансировки Angie ADC (ADC #1 и ADC #2):

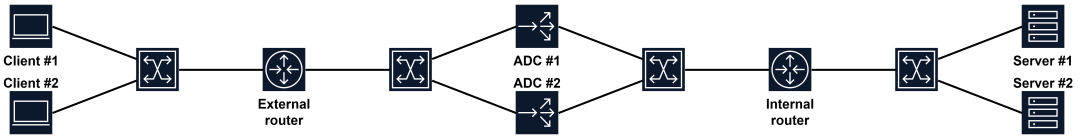


Рис. 1

Добавим *IP-адресацию*:

- В сегменте сети, куда подключаются External router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.0.0/24`.
- В сегменте сети, куда подключаются Internal router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.1.0/24`.
- Четвертый октет адреса для каждого устройства (в рамках соответствующей подсети) показан на схеме ниже.

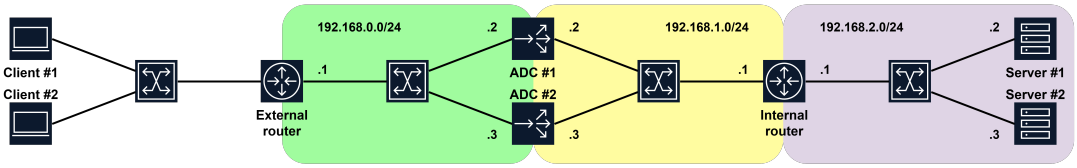


Рис. 2

Адресация клиентов не приводится, так как в данном случае мы будем считать, что их адреса формально не определены, то есть, они могут подключаться из любой сети, включая сеть интернет. Для этого на ADC #1 и ADC #2 необходимо указать адрес правого интерфейса маршрутизатора External router (`192.168.0.1`) в качестве шлюза по умолчанию.

Адрес сервиса может быть задан на каждой системе балансировки на *интерфейсе lo*, либо это может быть VIP группы VRRP.

- Первый способ (рис. 3 – адрес сервиса задан на интерфейсе `lo` и совпадает на обеих системах) будет более гибким, так как позволяет использовать только один IP-адрес для сервиса.
- Во втором случае (используется виртуальный адрес протокола VRRP) необходимо сообщить клиенту, что сервис работает на двух адресах (например, с помощью DNS).
- В третьем случае, если адрес сервиса задан на интерфейсе `lo`, но на системах адреса разные, также потребуется сообщить клиенту, что сервис работает на двух адресах.

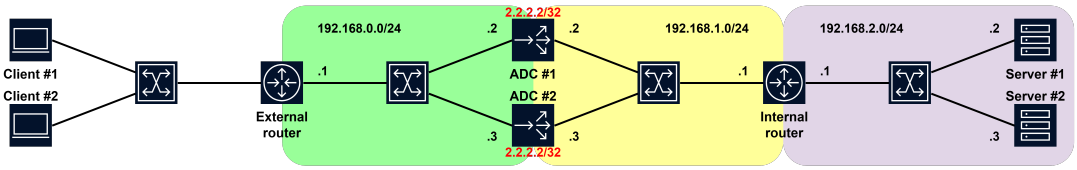


Рис. 3

Если адрес сервиса задан на интерфейсе `lo` (на схеме ниже это адрес `2.2.2.2`), на маршрутизаторе External router нужны статические маршруты на этот адрес через виртуальные адреса обеих групп VRRP (см. ниже).

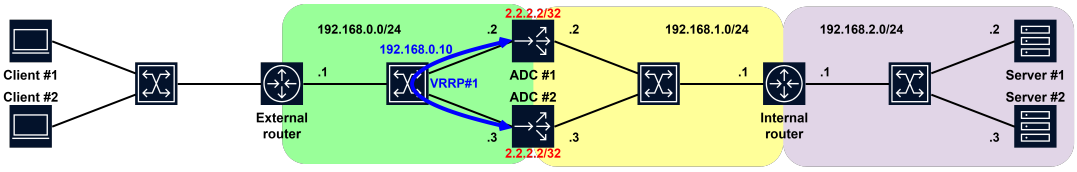


Рис. 4

Настройка режима Active-Active

Чтобы перейти от режима работы Active-Standby к режиму Active-Active, необходимо на том же интерфейсе систем балансировки настроить вторую VRRP группу таким образом, чтобы мастером в ней являлась другая система Angie ADC (достигается за счет опции `priority`). Для второй группы должен быть настроен виртуальный IP-адрес, отличающийся от адреса первой группы.

На схеме ниже вторая группа имеет виртуальный IP-адрес `192.168.0.11`:

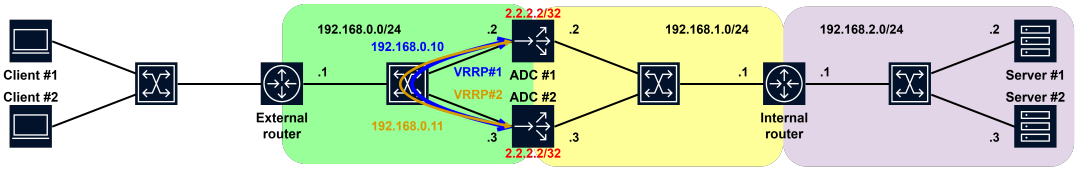


Рис. 5

На стороне маршрутизатора External router должно быть прописано два статических маршрута до префикса `2.2.2.2/32`:

- один с next-hop `192.168.0.10`;
- второй – `192.168.0.11`.

Маршрутизатор External router должен выполнять ECMP-балансировку трафика (часть сессий отправляется в сторону ADC #1, а оставшиеся – в сторону ADC #2).

Ниже приведен пример настройки маршрутизатора Cisco:

```
External(config)#ip route 2.2.2.2 255.255.255.255 192.168.0.10
External(config)#ip route 2.2.2.2 255.255.255.255 192.168.0.11
External(config)#exi
External#sho ip ro 2.2.2.2
Routing entry for 2.2.2.2/32
Known via "static", distance 1, metric 0
Routing Descriptor Blocks:
192.168.0.11
Route metric is 0, traffic share count is 1
* 192.168.0.10
Route metric is 0, traffic share count is 1
External#
```

У VRRP-группы есть виртуальный MAC-адрес (`00:00:5e:00:01:n`, где n – номер группы VRRP, номер виртуального маршрутизатора, в шестнадцатеричном виде). По MAC-адресу коммутатор определяет, для какой из систем балансировок предназначен трафик. Первая группа будет иметь виртуальный MAC-адрес `00:00:5e:00:01:01`, вторая – `00:00:5e:00:01:02`.

Убедиться в этом можно, просмотрев ARP-таблицу на маршрутизаторе External router:

```
External#sho ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.0.1 - ca01.0950.0008 ARPA GigabitEthernet0/0
Internet 192.168.0.10 0 0000.5e00.0101 ARPA GigabitEthernet0/0
Internet 192.168.0.11 0 0000.5e00.0102 ARPA GigabitEthernet0/0
External#
```

ARP-таблица маршрутизатора External router не меняется при отказе одной из систем балансировки нагрузки Angie ADC. Изменения будут на стороне коммутатора. Ниже приводится часть таблицы коммутации, когда обе системы балансировки «живы» и выполняют свои функции:

```
switch#sho mac address-table dynamic vlan 51
Mac Address Table
-------------------------------------------
```

```
Vlan Mac Address Type Ports
----------------------------
51  0000.5e00.0101 DYNAMIC Gi0/7
51  0000.5e00.0102 DYNAMIC Gi0/8
```

Система балансировки ADC #1 подключена к интерфейсу Gi0/7 коммутатора, а система балансировки ADC #2 – к интерфейсу Gi0/8.

При отказе одной из систем балансировки оставшаяся будет иметь обе VRRP-группы в статусе Master. С точки зрения коммутатора это будет выглядеть так, словно оба виртуальных MAC-адреса доступны через один интерфейс.

```
switch#sho mac address-table dynamic vlan 51
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
----------------------------
51 0000.5e00.0101 DYNAMIC Gi0/7
51 0000.5e00.0102 DYNAMIC Gi0/7
```

Подключение Angie ADC без маршрутизатора

Пример схемы сети представлен на рисунке ниже.

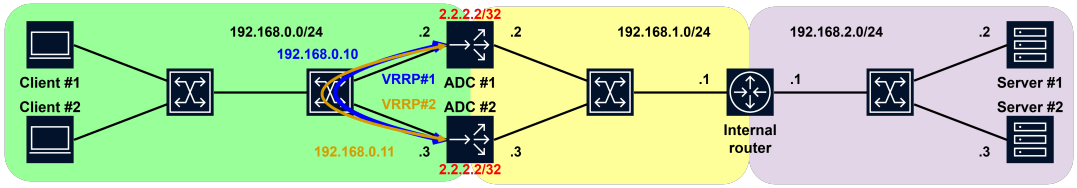


Рис. 6

В данном случае клиенты должны находиться в той же подсети, что и внешние интерфейсы систем балансировки Angie ADC (`192.168.0.0/24`).

Если клиенты Client #1 и Client #2 не имеют выхода в интернет, то тогда на них будет достаточно настроить один из адресов `192.168.0.10` и `192.168.0.11` в качестве шлюза по умолчанию. Тогда половина клиентов будет использовать адрес `192.168.0.10` в качестве шлюза по умолчанию, а вторая половина – `192.168.0.11`.

Если для выхода в интернет используется какое-то отдельное устройство, то на клиентах придется прописать статический маршрут до префикса `2.2.2.2/32`. На половине клиентов в качестве адреса следующего перехода (next-hop) необходимо настроить виртуальный адрес первой группы – `192.168.0.10`, а на оставшихся клиентах – адрес второй группы, `192.168.0.11`.

На схеме ниже желтой и красной стрелками указаны направления на шлюзы по умолчанию.

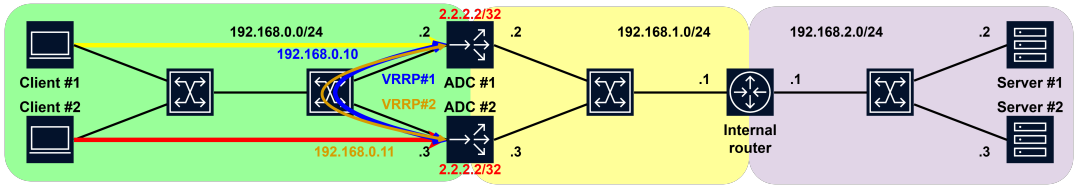


Рис. 7

Использовать ECMP-подход здесь нецелесообразно, так как некоторые клиентские операционные системы могут не поддерживать такую балансировку.

Настройка VRRP

Настройка VRRP на системах балансировки не зависит от того, какая схема подключения используется, с маршрутизатором или без.

Для настройки VRRP необходимо:

- на каждой системе балансировки создать две группы;
- для каждой из групп указать VIP и приоритет так, чтобы в первой группе Master была ADC #1, а во второй — ADC #2.

Все остальные параметры необязательны; полный список см. в *Команды VRRP*.

Группа	VIP	Приоритет ADC #1	Приоритет ADC #2	Предпочтительный Master
1	`192.168.0.10/24`	110	90	ADC #1
2	`192.168.0.11/24`	90	110	ADC #2

Каждый узел настраивается отдельно: подключитесь к *CLI* нужного узла и перейдите в режим `configuration`. В *паре высокой доступности* настраивайте группы на узле Active: синхронизация пары заменяет группы резервного узла группами основного. Каждая команда применяется сразу, дождитесь ее завершения.

Настройка ADC #1:

```
$$ configuration
## vrrp 1 interface ens33 address 192.168.0.10/24
## vrrp 1 interface ens33 priority 110
## vrrp 2 interface ens33 address 192.168.0.11/24
## vrrp 2 interface ens33 priority 90
```

Настройка ADC #2 симметричная:

```
$$ configuration
## vrrp 1 interface ens33 address 192.168.0.10/24
## vrrp 1 interface ens33 priority 90
## vrrp 2 interface ens33 address 192.168.0.11/24
## vrrp 2 interface ens33 priority 110
```

В нормальном состоянии каждая система обслуживает свой VIP, при отказе одной из них оставшаяся обслуживает оба. Оставшаяся система должна выдерживать суммарную нагрузку.

VRRP сам не распределяет запросы между VIP: распределение обеспечивают клиенты, использующие оба адреса, или маршрутизация через два next-hop, как в схемах выше.

Примечание

Схема не применяется к действующей *паре высокой доступности*: резервный узел пары (Standby) не участвует в группах VRRP.

Проверка работы

Текущую роль узла показывает команда `show vrrp` в основном режиме CLI (вне режима `configuration`).

Убедимся, что в стабильном и полностью рабочем состоянии ADC #1 является мастером для первой группы VRRP, а для второй группы мастером является система ADC #2.

Вывод с системы балансировки ADC #1:

```
$$ show vrrp interface ens33 summary
Interface VRID Priority IPv4 IPv6 State (v4) State (v6)
------------------------------------------------------------------------
ens33 1 110 1 0 Master Backup
ens33 2 90 1 0 Backup Backup
```

Вывод с системы балансировки ADC #2:

```
$$ show vrrp interface ens33 summary
Interface VRID Priority IPv4 IPv6 State (v4) State (v6)
------------------------------------------------------------------------
ens33 1 90   1 0 Backup Backup
ens33 2 110   1 0 Master Backup
```

При отказе, например, системы балансировки ADC #2, вывод информации о группах VRRP с системы балансировки ADC #1 будет выглядеть так:

```
$$ show vrrp interface ens33 summary
Interface VRID Priority IPv4 IPv6 State (v4) State (v6)
------------------------------------------------------------------------
ens33 1 110 1 0 Master Backup
ens33 2 90 1 0 Master Backup
```

Заключение

С помощью протокола VRRP можно построить отказоустойчивое решение по балансировке нагрузки на сервера там, где использование протоколов динамической маршрутизации невозможно по той или иной причине.

Проверку переключения и устранение типовых проблем см. в *Диагностика VRRP*.

Команды VRRP

Группы VRRP настраиваются в *CLI* в режиме `configuration`. Команды меняют группы узла, к которому подключен CLI.

Общий вид команды:

```
vrrp <VRID> interface <интерфейс> <параметр> [<значение>]
```

Группу на узле определяет пара «интерфейс + VRID». Имена интерфейсов на разных узлах могут отличаться.

Пример:

```
$$ configuration
## vrrp 1 interface ens33 address 192.168.0.10/24
## vrrp 1 interface ens33 priority 110
## vrrp show
```

Применение изменений

- Каждая команда, которая меняет группу, — отдельное изменение кластерной конфигурации узла. Отдельного шага применения нет: команда передает изменение в кластер и ждет, пока узел его применит.
- Несколько команд не объединяются в одну операцию: если третья команда не выполнена, первые две уже могли примениться. Дождитесь завершения команды и проверьте результат перед следующей.

- Выход из режима `configuration` или закрытие SSH-сессии не отменяет принятое изменение. Настройки сохраняются после перезагрузки.
- Если узел не применил изменение за 120 секунд, команда завершается с ошибкой, а кластер продолжает повторять попытки. Такое изменение можно отменить в веб-интерфейсе (подробнее см. *Команда завершилась по тайм-ауту*).
- В *паре высокой доступности* настраивайте группы на узле Active: синхронизация пары заменяет группы резервного узла группами основного.

Создание и удаление группы

Группа создается командой с `address`:

```
## vrrp 1 interface ens33 address 192.168.0.10/24
```

Если группы нет, команда создает ее сразу включенной, с параметрами по умолчанию. Если группа есть, команда заменяет VIP, остальные параметры сохраняются. Замена VIP затрагивает подключения к прежнему адресу.

Создать группу без адреса, например командой `priority` или `shutdown`, нельзя. Если группа не должна сразу вступить в работу, учитывайте, что между созданием группы и командой `shutdown` она может успеть стать Master.

Группа удаляется явно:

```
## no vrrp 1 interface ens33
```

Команда удаляет группу только на текущем узле; чтобы убрать группу из схемы, повторите ее на остальных участниках. Сброс параметров к значениям по умолчанию группу не удаляет.

Правила адресации

- Интерфейс должен быть описан в *сетевых настройках* узла и иметь собственный IPv4-адрес (статический или по DHCP). Для интерфейса, которого нет в сетевых настройках, команда `vrrp` возвращает ошибку. Для предсказуемой работы используйте статический адрес.
- VIP указывается с длиной префикса, например `192.168.0.10/24`. Обычно длина префикса совпадает с длиной префикса адресов участников.
- VIP должен быть свободен и не совпадать с собственными адресами узлов. Совпадение VIP со статическим IPv4-адресом интерфейса группы отклоняется. Добавлять VIP как обычный адрес интерфейса не нужно.
- Группу нельзя разместить на физическом интерфейсе, входящем в bond: размещайте ее на самом bond или на VLAN-интерфейсе.
- На одном интерфейсе нельзя создать две группы с одним VRID или назначить один VIP разным группам. Группы с разными VRID и VIP на одном интерфейсе допустимы.
- Один VRID можно использовать на разных интерфейсах, если эти группы не конфликтуют в общем сетевом сегменте.

На всех участниках группы задайте одинаковые VIP, длину префикса, VRID, версию протокола, интервал анонсов и режим контрольной суммы. Приоритеты обычно различаются.

Параметры

Параметр	Значения	По умолчанию	Назначение
`<VRID>`	1–255	—	Номер группы (Virtual Router ID).
`address`	IPv4-адрес с длиной префикса	—, обязателен	VIP группы. Повторная команда заменяет VIP.
`priority`	1–254	100	Приоритет узла в группе: Master становится узел с наибольшим приоритетом. Значение 255 зарезервировано и вручную не задается.
`version`	2 или 3	3	Версия протокола VRRP.
`advertisement`	10–40950 мс, кратно 10; для версии 2 — 1000–40000 мс, кратно 1000	1000 мс	Интервал отправки анонсов.
`preempt`	включен или выключен	включен	Узел с большим приоритетом забирает роль Master у узла с меньшим.
`checksum-with`	включен или выключен	включен	Учет псевдозаголовка IPv4 в контрольной сумме VRRPv3. Для VRRPv2 не используется.
`shutdown`	включен или выключен	выключен (группа работает)	Административное выключение группы на этом узле.

Приоритет

```
## vrrp 1 interface ens33 priority 110
## no vrrp 1 interface ens33 priority
```

Вторая команда возвращает приоритет 100. Чтобы Master выбирался предсказуемо, задайте участникам разные приоритеты.

Версия протокола

```
## vrrp 1 interface ens33 version 2
## no vrrp 1 interface ens33 version
```

Вторая команда возвращает версию 3. Перед переходом на версию 2 убедитесь, что интервал анонсов кратен 1000 мс, иначе изменение версии будет отклонено.

Меняйте версию на всех участниках в одно окно работ: пока версии не совпадают, Master могут стать сразу несколько узлов.

Интервал анонсов

```
## vrrp 1 interface ens33 advertisement-interval 500
## no vrrp 1 interface ens33 advertisement-interval
```

Вторая команда возвращает 1000 мс. Меньший интервал ускоряет обнаружение отказа Master, но время переключения сервиса зависит и от сети: измеряйте его на своей сети.

Preempt

```
## vrrp 1 interface ens33 preempt
## no vrrp 1 interface ens33 preempt
```

Первая команда включает вытеснение, вторая — выключает. Без вытеснения восстановившийся узел с большим приоритетом не забирает роль Master у работающего узла. Резервный узел принимает VIP при отказе Master независимо от этого параметра.

Контрольная сумма

```
## vrrp 1 interface ens33 checksum-with-ipv4-pseudoheader
## no vrrp 1 interface ens33 checksum-with-ipv4-pseudoheader
```

Обычно оставляйте значение по умолчанию. При работе с оборудованием другого производителя согласуйте параметр с его настройками.

Выключение группы

```
## vrrp 1 interface ens33 shutdown
## no vrrp 1 interface ens33 shutdown
```

Первая команда выключает группу на текущем узле, сохраняя ее параметры; вторая — включает. Выключение сохраняется после перезагрузки и не затрагивает группу на остальных участниках. Если узел был Master, проверьте, что VIP перешел на резервный узел.

Включение группы не снимает ограничения резервного узла *пары высокой доступности*.

Формы no

В формах `no` числовое значение не указывается.

Команда	Результат
`no vrrp 1 interface ens33 priority`	Приоритет 100
`no vrrp 1 interface ens33 version`	Версия 3
`no vrrp 1 interface ens33 advertisement-interval`	Интервал 1000 мс
`no vrrp 1 interface ens33 preempt`	Preempt выключен
`no vrrp 1 interface ens33 checksum-with-ipv4-pseudoheader`	Псевдозаголовок IPv4 не учитывается
`no vrrp 1 interface ens33 shutdown`	Группа включена
`no vrrp 1 interface ens33`	Группа удалена

Отдельной команды для удаления VIP нет: замените VIP или удалите группу. Форма `no` с параметром для несуществующей группы отклоняется.

Просмотр групп

Сохраненная конфигурация

В режиме `configuration` команда `vrrp show` выводит группы текущего узла в формате JSON:

```
## vrrp show
[
  {
    "link": "ens33",
    "vrid": 1,
```

```
    "address": "192.168.0.10/24",
    "version": "VRRP_VERSION_UNSPECIFIED",
    "priority": 110
  }
]
```

Поля `link`, `vrid`, `address` и `version` выводятся всегда. Остальные параметры, если они не заданы явно, в выводе отсутствуют и имеют значения по умолчанию. Пустой список `[]` означает, что групп нет.

Поле	Значение
`link`	Интерфейс группы
`vrid`	Номер группы
`address`	VIP с длиной префикса
`version`	Версия протокола: `VRRP_VERSION_2` или `VRRP_VERSION_3`, если задана явно; `VRRP_VERSION_UNSPECIFIED`, если не задана (используется версия 3)
`priority`	Заданный приоритет
`advertisement_interval_ms`	Интервал анонсов в миллисекундах
`preempt`	`false` — вытеснение выключено
`checksum_ipv4_pseudoheader`	`false` — псевдозаголовок IPv4 не учитывается
`enabled`	`false` — группа выключена командой `shutdown`

Вывод `vrrp show` не показывает, какую роль узел занимает в группе.

Текущее состояние

Текущую роль узла (Master или Backup) показывает команда *show* в основном режиме CLI; в режиме `configuration` она не работает.

Команда	Что выводит
`show vrrp`	Подробная карточка каждой группы узла
`show vrrp interface <интерфейс> <VRID>`	Подробная карточка одной группы
`show vrrp interface <интерфейс> summary`	Одна строка на каждую группу интерфейса
`show vrrp interface <интерфейс> <VRID> summary`	Одна строка на группу

Пример краткого вывода:

```
$$ show vrrp interface ens3 summary

 Interface   VRID   Priority   IPv4   IPv6   State (v4)   State (v6)
 ------------------------------------------------------------------
 ens3        1      110        1      0      Master       Backup
```

Столбец	Значение
`Interface`	Интерфейс группы
`VRID`	Номер группы
`Priority`	Приоритет узла в группе
`IPv4`, `IPv6`	Число виртуальных адресов каждого семейства
`State (v4)`, `State (v6)`	Состояние IPv4- и IPv6-части группы

Как читать роль:

- Роль узла определяет IPv4-часть: смотрите столбец `State (v4)`. У групп Angie ADC нет виртуальных IPv6-адресов, поэтому IPv6-часть не запускается: в кратком выводе `State (v6)` всегда `Backup`, а в подробной карточке `Status (v6)` — `Initialize`.
- В кратком выводе есть только два значения. `Master` означает, что узел обслуживает VIP. `Backup` означает все остальное: резервный режим, а также выключенную или еще не запущенную группу.
- Чтобы отличить резервный режим от незапущенной группы, смотрите `Status (v4)` в подробной карточке: `Master`, `Backup` или `Initialize`.
- Признак работающего Master на резервном узле — растущий счетчик `Advertisements Rx (v4)` в подробной карточке: узел получает анонсы.
- После создания группы, ее включения или пропажи Master узел остается Backup, пока не истечет интервал `Master Down Interval` (около 3,6 с при параметрах по умолчанию). Затем узел становится Master, если его приоритет выше или Master пропал. Поэтому после изменения проверяйте роль через несколько секунд.
- Наличие VIP в списке адресов узла роль не подтверждает: роль показывает только `show vrrp`.

VLAN, bond и домены маршрутизации

VLAN

Сначала создайте VLAN-интерфейс и задайте ему IPv4-адрес, затем укажите его имя в команде:

```
## vrrp 10 interface ens33.100 address 192.168.100.10/24
```

Bond

Если IPv4-адрес задан на bond, укажите bond, а не входящие в него интерфейсы:

```
## vrrp 10 interface bond0 address 192.168.100.10/24
```

Домен маршрутизации

Отдельного параметра для домена маршрутизации у команды нет: группа работает в *домене маршрутизации* своего интерфейса. Поместите интерфейс в домен маршрутизации в сетевых настройках узла, дождитесь применения и создайте группу обычной командой. Имя домена маршрутизации задается на каждом узле отдельно и не связывает узлы между собой: участникам нужен общий сетевой сегмент.

Имя виртуального интерфейса

Для каждой группы на узле создается виртуальный интерфейс вида `vrrp4-<интерфейс>-<VRID>`. Если имя получается длиннее 15 символов, оно заменяется сокращенным, поэтому определяйте группу по интерфейсу и VRID, а не по имени виртуального интерфейса.

Диагностика VRRP

Здесь описано, как проверить работу групп VRRP и переключение VIP и что делать, если настройка или работа не удается. Команды настройки см. в *Команды VRRP*.

Проверка работы

Настройки на участниках

На каждом участнике группы выполните *vrrp show* в режиме `configuration` и сверьте интерфейс, VIP, VRID, версию, интервал анонсов, preempt и выключение группы. Значения версии

`VRRP_VERSION_UNSPECIFIED` и `VRRP_VERSION_3` означают одну и ту же версию протокола. Наличие групп на вкладке каждого узла можно проверить и в веб-интерфейсе: `Система` → `Сетевые настройки` → блок `Группы VRRP`.

Текущая роль

Роль узла в группе показывает команда `show vrrp` в основном режиме CLI (в режиме `configuration` она не работает):

```
$$ show vrrp interface ens33 summary
Interface VRID Priority IPv4 IPv6 State (v4) State (v6)
------------------------------------------------------------------------
ens33 1 110 1 0 Master Backup
```

Роль читайте в столбце `State (v4)`; `State (v6)` о роли ничего не говорит. После создания или включения группы узел несколько секунд остается Backup, поэтому проверяйте роль не раньше чем через несколько секунд после изменения. Подробнее о выводе см. *Просмотр групп*.

Сохраненная конфигурация и текущая роль — разные сведения: наличие группы в `vrrp show` и VIP в списке адресов узла не подтверждают, что узел — Master.

Доступ к сервису

Проверяйте сервис из сети, откуда приходят реальные запросы. Например, для HTTPS-сервиса `app.example.com` на VIP `192.168.0.10` выполните на клиентском хосте:

```
$ curl --resolve app.example.com:443:192.168.0.10 https://app.example.com/
```

Успешный ответ приложения проверяет больше, чем `ping`: доступность VIP, прием соединения и обработку запроса.

Анонсы VRRP

Анонсы группы в стабильном состоянии отправляет Master. Чтобы увидеть их, перейдите в контекст *diagnostics* и захватите пакеты IP-протокола 112 на интерфейсе группы:

```
$$ diagnostics
(diagnostics)$$ tcpdump -i ens33 -c 10 -nn -v "ip proto 112"
```

Для VLAN укажите его имя, например `ens33.100`. В выводе сопоставьте VRID, адрес источника и приоритет с настройками узлов; если на интерфейсе несколько групп, различайте их по VRID. Пакеты одного источника не доказывают, что резервный узел их получает: при сомнениях захватите анонсы на обоих участниках.

Переключение VIP

Проверка для двух узлов, где ADC #1 — Master, ADC #2 — Backup:

1. Убедитесь, что ADC #2 настроен и получает анонсы ADC #1.
2. Запустите с клиента повторяющиеся запросы к сервису.
3. На ADC #1 выключите группу:

   ```
   ## vrrp 1 interface ens33 shutdown
   ```

4. Через несколько секунд убедитесь, что ADC #2 стал Master и новые запросы проходят.
5. На ADC #1 включите группу:

   ```
   ## no vrrp 1 interface ens33 shutdown
   ```

6. Если на ADC #1 включен preempt и его приоритет выше, убедитесь, что роль Master вернулась на ADC #1. Если preempt выключен, роль Master должна остаться у ADC #2.

Такая проверка подтверждает переход VIP при выключении группы. Отказ узла и потерю сетевого соединения проверяйте отдельно, в предусмотренное для этого окно работ. Длительные пользовательские сессии при переключении не сохраняются; проверяйте их отдельно.

Для *пары высокой доступности* выключение группы на узле Active не заменяет проверку переключения пары: пока второй узел остается Standby, он не принимает VIP.

Если настройка не удается

Команда отклонена

Исправьте указанную причину и повторите команду.

Проблема	Что проверить
Группа создается без адреса	Первой командой должна быть `vrrp <VRID> interface <интерфейс> address <IPv4/префикс>`
Неизвестный интерфейс	Описан ли интерфейс в сетевых настройках именно текущего узла; если нет, сначала настройте его
У интерфейса нет IPv4-адреса	Собственный IPv4-адрес интерфейса группы (статический или по DHCP)
VIP совпадает с адресом интерфейса	Выделите отдельный свободный VIP
Интерфейс входит в bond	Настройте группу на bond или на VLAN-интерфейсе
Недопустимое значение	VRID 1–255, приоритет 1–254, версия 2 или 3, VIP — IPv4-адрес с префиксом
Недопустимый интервал	Диапазон 10–40950 мс и кратность 10 мс; для версии 2 — кратность 1000 мс
Форма `no` для несуществующей группы	Проверьте группы командой `vrrp show`
Команда не распознается	Используйте ключевые слова `interface` и `address`; в формах `no` значение параметра не указывается (см. *Команды VRRP*)

Команда завершилась по тайм-ауту

CLI ждет применения изменения до 120 секунд. Тайм-аут не отменяет изменение: кластер продолжает его применять, и оно может блокировать следующие изменения конфигурации.

1. Сохраните идентификатор изменения и сообщение об ошибке из CLI.
2. Откройте веб-интерфейс и найдите карточку текущего изменения конфигурации. Проверьте его состояние и причину повторных попыток.
3. Если причину можно устранить, устраните ее и дождитесь завершения.
4. Если изменение нужно отменить, нажмите в карточке `Отменить применение` и подтвердите отмену. Дождитесь ее завершения.
5. Если веб-интерфейс недоступен, отмените изменение в локальном мастере `adc-bootstrap`: в меню управления сетью выберите `Review or cancel pending changes`, выберите изменение и подтвердите отмену.
6. Перед повторной настройкой проверьте сохраненную конфигурацию и доступность VIP.

Отмена затрагивает одно изменение целиком. Каждая команда VRRP — отдельное изменение, поэтому отмена последнего не отменяет предыдущие.

Кнопка `Сбросить` в форме сетевых настроек сбрасывает только несохраненные правки формы.

Если изменение сети отрезало узел от управления, автоматического отката нет: для восстановления нужен доступ к локальной консоли узла.

Группа есть, но VIP не работает

Проверьте по порядку:

1. Создана ли группа на нужном узле и применено ли изменение.
2. Не выключена ли группа командой `shutdown`.
3. Не ограничен ли узел ролью Standby *пары высокой доступности*, в том числе после ее расформирования (см. *no ha standby*).
4. Работают ли интерфейс группы, его VLAN или bond и собственный IPv4-адрес.
5. Совпадают ли параметры группы у участников.
6. Доходят ли анонсы между узлами (см. *Анонсы VRRP*).
7. Разрешены ли виртуальные MAC-адреса и их перемещение в виртуальной и физической сети (для VMware ESXi см. *Предварительная настройка для VMware ESXi*).
8. Настроен ли сервис на узле, который принял VIP, и доступны ли ему серверы.
9. Корректны ли маршруты, домены маршрутизации и обратный путь к клиенту.

Оба узла считают себя Master

Узлы, которые не получают или не принимают анонсы друг друга, одновременно обслуживают VIP. Проверьте сетевую связность между участниками, VLAN, VRID, VIP, версию протокола, интервал анонсов и режим контрольной суммы. Захватите анонсы на обоих узлах.

Если конфликт уже нарушает работу, временно выключите группу на одном из узлов, исправьте причину и повторите проверку. Убедитесь, что оставшийся узел действительно обслуживает сервис.

VIP не перешел после отказа серверной сети

VRRP не проверяет состояние приложения, upstream или сетевых путей, а отслеживания (VRRP tracking) нет. VIP переходит на резервный узел, только когда Master перестает отправлять анонсы. Отказы клиентского и серверного интерфейсов, маршрутов и приложения проверяйте отдельно: проверки полного выключения узла для них недостаточно.

Проверка после обновления

После обновления с версии, где VRRP настраивался в отдельном CLI на порту 2022, проверьте:

- все ожидаемые группы есть в `vrrp show` на каждом узле;
- сохранились VIP, приоритеты, версии, интервалы, preempt и выключение групп;
- в веб-интерфейсе группы видны на вкладках нужных узлов;
- в паре высокой доступности корректны соответствия интерфейсов, синхронизация и роли узлов;
- VIP обслуживает нужный узел, запросы проходят и переключение работает;
- настройки и поведение сохраняются после перезагрузки.

Значения, заданные в прежнем CLI командами `vrrp default ...`, перенесены в параметры каждой существующей группы. Общих параметров для всех групп нет: каждая группа настраивается отдельно.

Настраивайте VRRP только командами CLI: правки файлов конфигурации и изменения через `vtysh` перезаписываются при применении кластерной конфигурации.

4.2.2 Настройка динамической маршрутизации

BGP и OSPF настраиваются в *CLI*, в режиме `configuration`, командой *routing*. Команда меняет настройки того узла, к которому подключен CLI, поэтому каждый узел настраивается отдельно. Каждая команда — отдельное изменение кластерной конфигурации: CLI ждет его применения на узле.

```
$$ configuration
## routing prefix-list vip seq 5 permit 192.0.2.10/32
## routing route-map vip permit 10 match-prefix-list vip
## routing bgp asn 65001
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp redistribute connected route-map vip
```

Конфигурацию узла целиком формирует Angie ADC из кластерной конфигурации. Правки перезаписываются при следующем применении.

Порядок настройки:

1. Интерфейсы и их адреса задаются в *сетевых настройках* узла.
2. Адреса сервисов, которые нужно анонсировать, задаются на *интерфейсе lo* с префиксом `/32`.
3. Списки префиксов (`routing prefix-list`) и карты маршрутов (`routing route-map`) создаются до того, как на них сошлются BGP или OSPF.
4. BGP запускается командой `routing bgp asn <номер>`, процесс OSPF — командой `routing ospf <номер>`; затем задаются остальные параметры.

Поддерживается один процесс BGP в домене маршрутизации по умолчанию с адресным семейством IPv4 unicast и до 10 процессов OSPFv2. В области OSPF указывается номером, например `0`.

Удаление выполняется в обратном порядке: сначала протоколы, затем карты маршрутов, затем списки префиксов. Например, `no routing bgp` удаляет BGP целиком, `no routing ospf 1` — процесс OSPF 1.

4.2.2.1 Просмотр

Сохраненные настройки выводит команда `routing show` в режиме `configuration` (в формате JSON). Состояние протоколов показывают команды *show* в основном режиме CLI, например:

```
$$ show ip bgp summary
$$ show ip bgp
$$ show ip ospf neighbor
$$ show ip ospf database external self-originate
$$ show ip route
```

4.2.3 BGP-маршрутизация

В этом разделе описана настройка BGP-маршрутизации для обеспечения высокой доступности в режиме резервирования (Active-Standby) и в режиме распределения нагрузки (Active-Active). BGP и OSPF настраиваются в CLI командой *routing* (общие правила см. в *Настройка динамической маршрутизации*).

В этом разделе:

- *Режим резервирования (Active-Standby)*
- *Режим распределения нагрузки (Active-Active)*

4.2.3.1 Резервирование с помощью протокола BGP (Active-Standby)

Введение

В этом разделе описана настройка высокой доступности с использованием протокола BGP в режиме резервирования (Active-Standby). Узлы Angie ADC настраиваются в CLI командой *routing* (общие правила см. в *Настройка динамической маршрутизации*).

В качестве протокола динамической маршрутизации используется BGPv4 для адресного семейства IPv4 unicast; другие адресные семейства в Angie ADC не поддерживаются.

В рассматриваемом примере Angie ADC #1 выполняет функции активной системы балансировки трафика, а Angie ADC #2 остается в резерве.

Пример типового участка сети с системами балансировки Angie ADC (ADC #1 и ADC #2) представлен на схеме:

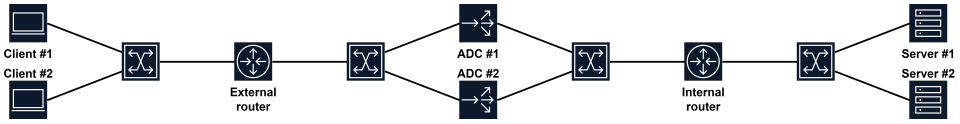


Рис. 1

Добавим IP-адресацию:

- В сегменте сети, куда подключаются External router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.0.0/24`.
- В сегменте сети, куда подключаются Internal router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.1.0/24`.
- Четвертый октет адреса для каждого устройства (в рамках соответствующей подсети) показан на схеме ниже.

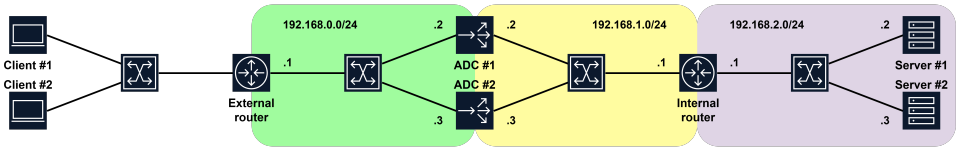


Рис. 2

Адресация клиентов не приводится, так как в данном случае мы будем считать, что их адреса формально не определены, то есть они могут подключаться из любой сети, включая сеть интернет. Для этих целей External router будет анонсировать маршрут по умолчанию по BGP для ADC #1 и ADC #2. В данном документе будем использовать только одну автономную систему BGP №65001.

> **Примечание**
>
> Автономная система BGP — логическое объединение устройств в сети для маршрутизации через протокол BGP.

BGP-сессии

Устанавливаемые BGP-сессии представлены на схеме:

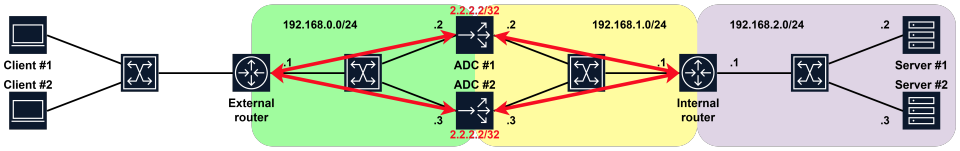


Рис. 3

Красным цветом на схеме отмечены IP-адреса виртуальных серверов. Это те адреса, к которым подключаются клиенты снаружи. Системы балансировки должны анонсировать маршруты до этих виртуальных серверов в сторону External router, причем маршрут через ADC #1 должен быть более предпочтительным. Добиться этого можно разными способами, манипулируя атрибутами пути в BGP.

Так как все BGP-взаимодействие производится строго в рамках одной автономной системы, мы будем использовать атрибут Local preference (чем больше, тем лучше) для выбора наиболее оптимального пути. Трафик от серверов в сторону клиента должен проходить через ту же систему балансировки, что и трафик от клиентов к серверам. Добиться этого можно также путем манипулирования значением атрибута Local preference для префикса `0.0.0.0/0`.

Обработка типовых сбоев

Ниже описаны сценарии работы Angie ADC при сбоях.

Полный отказ ADC #1

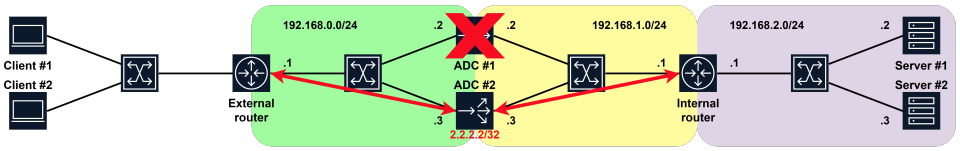


Рис. 4

При полном отказе или отключении от сети ADC #1 разрываются обе BGP-сессии с ADC #1. Через ADC #1 не проходят никакие объявления маршрутов. Остается связь по BGP только с ADC #2. Переключение на резервную систему ADC #2 производится автоматически. Никакие дополнительные настройки не требуются.

Отказ внешнего интерфейса ADC #1

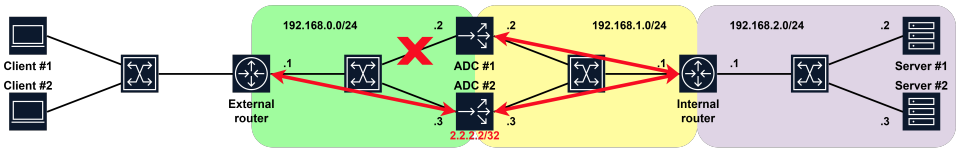


Рис. 5

В этом случае разрывается BGP-сессия между ADC #1 и External router. ADC #1 теперь не может объявить маршрут до адреса виртуального сервера в сторону External router. Несмотря на наличие BGP-сессии между ADC #1 и Internal router, ADC #1 не отправляет маршрут по умолчанию в сторону Internal router, так как сама не получает его от External router из-за сбоя линка. Таким образом, Internal router видит маршрут по умолчанию только через ADC #2, а External router получает маршрут до адреса виртуального сервера только через полностью работающий ADC #2.

Отказ линка между ADC #1 и Internal router

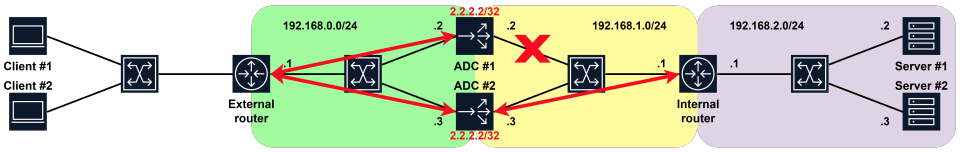


Рис. 6

Если BGP-сессия между External router и ADC #1 сохраняется, то ADC #1 будет продолжать анонсировать маршрут до адреса виртуального сервера, хотя реальные серверы для ADC #1 уже недостижимы. Таким образом, мы получаем классический black hole для трафика. Чтобы избежать этого, анонсирование маршрутов до виртуальных серверов должно быть условным, то есть ADC #1 анонсирует маршрут до адреса виртуального сервера, только если в BGP-таблице присутствуют префиксы, соответствующие подсетям реальных серверов.

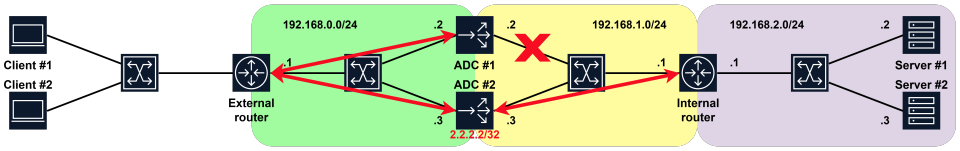


Рис. 7

Настройка маршрутизации

Приведем ключевые настройки маршрутизации для External router, Internal router, ADC #1 и ADC #2.

Примечание

В этой схеме ADC #1 и ADC #2 — самостоятельные узлы с разными настройками маршрутизации. Синхронизация *пары высокой доступности* копирует маршрутизацию узла Active на узел Standby целиком, поэтому для пары используйте схему из *BGP*.

Ключевые настройки маршрутизации для External router

```
hostname external
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
!Интерфейс в сторону систем балансировки
router bgp 65001
 neighbor 192.168.0.2 remote-as 65001
!Сессия с ADC#1
 neighbor 192.168.0.2 default-originate
!Анонсирование маршрута по умолчанию
 neighbor 192.168.0.3 remote-as 65001
!Сессия с ADC#2
 neighbor 192.168.0.3 default-originate
!Анонсирование маршрута по умолчанию
end
```

Ключевые настройки маршрутизации для Internal router

```
hostname internal
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!Интерфейс в сторону систем балансировки
interface GigabitEthernet1/0
ip address 192.168.2.1 255.255.255.0
!Интерфейс в сторону подсети с реальными серверами
router bgp 65001
 network 192.168.2.0 mask 255.255.255.0
!Добавление информации о подсети с реальными серверами в BGP
 neighbor 192.168.1.2 remote-as 65001
!Сессия с ADC#1
 neighbor 192.168.1.3 remote-as 65001
!Сессия с ADC#2
end
```

Ключевые настройки маршрутизации Angie ADC #1

Интерфейсы задаются в *сетевых настройках* узла: `ens37` — `192.168.0.2/24` (в сторону External router), `ens38` — `192.168.1.2/24` (в сторону Internal router). Адрес виртуального сервера `2.2.2.2/32` задается на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing prefix-list vip seq 5 permit 2.2.2.2/32
## routing prefix-list servers seq 5 permit 192.168.2.0/24
## routing route-map 2clients permit 10 match-prefix-list vip local-preference 150
## routing route-map 2clients deny 20
## routing route-map fromclients permit 10 local-preference 150
## routing route-map servers permit 10 match-prefix-list servers
## routing bgp asn 65001
## routing bgp network 2.2.2.2/32
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp neighbor 192.168.0.1 route-reflector-client
## routing bgp neighbor 192.168.0.1 route-map fromclients in
## routing bgp neighbor 192.168.0.1 route-map 2clients out
## routing bgp neighbor 192.168.0.1 advertise-map 2clients exist-map servers
## routing bgp neighbor 192.168.1.1 remote-as 65001
## routing bgp neighbor 192.168.1.1 route-reflector-client
## routing bgp neighbor 192.168.1.1 next-hop-self force
```

Назначение команд:

- список префиксов `vip` описывает адрес виртуального сервера, `servers` — подсеть реальных серверов;
- карта `2clients` пропускает в сторону External router только адрес виртуального сервера и задает ему Local preference; остальные префиксы запрещает запись `deny 20`;
- карта `fromclients` задает Local preference маршрутам, полученным от External router, в том числе маршруту по умолчанию;
- `advertise-map 2clients exist-map servers` — условный анонс: адрес виртуального сервера отправляется External router, только пока в BGP-таблице есть маршрут, соответствующий карте `servers`;
- `route-reflector-client` разрешает передачу префиксов между двумя iBGP-соседями;

- `next-hop-self force` подставляет собственный адрес в атрибут next-hop, в том числе для отраженных префиксов.

Ключевые настройки маршрутизации Angie ADC #2

Интерфейсы задаются в *сетевых настройках* узла: `ens37` — `192.168.0.3/24` (в сторону External router), `ens38` — `192.168.1.3/24` (в сторону Internal router). Адрес виртуального сервера `2.2.2.2/32` задается на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing prefix-list vip seq 5 permit 2.2.2.2/32
## routing prefix-list servers seq 5 permit 192.168.2.0/24
## routing route-map 2clients permit 10 match-prefix-list vip local-preference 50
## routing route-map 2clients deny 20
## routing route-map fromclients permit 10 local-preference 50
## routing route-map servers permit 10 match-prefix-list servers
## routing bgp asn 65001
## routing bgp network 2.2.2.2/32
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp neighbor 192.168.0.1 route-reflector-client
## routing bgp neighbor 192.168.0.1 route-map fromclients in
## routing bgp neighbor 192.168.0.1 route-map 2clients out
## routing bgp neighbor 192.168.0.1 advertise-map 2clients exist-map servers
## routing bgp neighbor 192.168.1.1 remote-as 65001
## routing bgp neighbor 192.168.1.1 route-reflector-client
## routing bgp neighbor 192.168.1.1 next-hop-self force
```

Настройки отличаются от ADC #1 адресами интерфейсов и меньшим значением Local preference (50), поэтому маршруты через ADC #2 менее предпочтительны.

Проверка работы

Выполним проверку работы системы маршрутизации, когда ADC #1 и ADC #2 находятся в полностью работоспособном состоянии.

Примечание

В листингах ниже отсутствуют префиксы, не относящиеся к обсуждаемым вопросам отказоустойчивости.

Маршрутизатор External router видит маршрут к адресу виртуального сервера через обе системы балансировки, однако маршрут через ADC #1 является более предпочтительным:

```
external#sho ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
```

```
B        2.2.2.2 [200/0] via 192.168.0.2, 02:06:11
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/0
L        192.168.0.1/32 is directly connected, GigabitEthernet0/0
external#sho ip bg
BGP table version is 9, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
     0.0.0.0          0.0.0.0                                0 i
 *>i 2.2.2.2/32       192.168.0.2              0    150      0 i
 * i                  192.168.0.3              0     50      0 i
```

Маршрутизатор Internal router видит маршрут по умолчанию через обе системы балансировки, однако маршрут через ADC #1 является более предпочтительным:

```
internal#sho ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

B*    0.0.0.0/0 [200/0] via 192.168.1.2, 02:12:37
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet1/0
L        192.168.2.1/32 is directly connected, GigabitEthernet1/0
internal#sho ip bgp
BGP table version is 12, local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0          192.168.1.2              0    150      0 i
 * i                  192.168.1.3              0     50      0 i
 *>  192.168.2.0/24   0.0.0.0                  0         32768 i
```

Отключим теперь линк между ADC #1 и Internal router (например, отключим адаптер `ens38` в среде виртуализации) и проверим маршрутизацию.

Изучим теперь таблицу маршрутизации и BGP-таблицу на маршрутизаторе External router. Несмотря на наличие BGP-сессии до каждой из систем балансировки, только по одной сессии прилетает маршрут на адрес виртуального сервера – от ADC #2:

```
external#sho ip bg su
BGP router identifier 11.11.11.11, local AS number 65001
BGP table version is 8, main routing table version 8
2 network entries using 296 bytes of memory
2 path entries using 128 bytes of memory
2/1 BGP path/bestpath attribute entries using 272 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 696 total bytes of memory
BGP activity 3/1 prefixes, 4/2 paths, scan interval 60 secs
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/
↪PfxRcd
192.168.0.2     4            1     156     150        8    0    0 00:07:29        0
192.168.0.3     4            1     157     150        8    0    0 00:07:29        1
external#sho ip bg
BGP table version is 8, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
     0.0.0.0          0.0.0.0                              0 i
 *>i 2.2.2.2/32       192.168.0.3              0     50      0 i
external#sho ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
      2.0.0.0/32 is subnetted, 1 subnets
B        2.2.2.2 [200/0] via 192.168.0.3, 00:04:36
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/0
L        192.168.0.1/32 is directly connected, GigabitEthernet0/0
```

И теперь маршрутная информация со стороны Internal router:

```
internal#sho ip bgp
BGP table version is 8, local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0          192.168.1.3              0     50      0 i
 *>  192.168.2.0/24   0.0.0.0                  0         32768 i
internal#sho ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is 192.168.1.3 to network 0.0.0.0
B*    0.0.0.0/0 [200/0] via 192.168.1.3, 00:00:49
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
C        192.168.2.0/24 is directly connected, GigabitEthernet1/0
L        192.168.2.1/32 is directly connected, GigabitEthernet1/0
```

Применение с IP transparency

Все описанное выше относится к режиму работы Angie ADC с включенной опцией IP transparency. При включенной опции IP Transparency Angie ADC сохраняет исходный адрес отправителя в IP-пакетах, позволяя серверам на сетевом уровне различать клиентские подключения.

Очень часто администраторы систем балансировки отключают эту опцию, в этом случае Angie ADC будет выполнять не только dNAT, но sNAT над трафиком, приходящим от клиентов. Если система балансировки Angie ADC выполняет sNAT, то в этом случае маршрутизация несколько упрощается, так как в этом случае нет необходимости анонсировать на Internal router маршрут по умолчанию. Если ADC #1 и ADC #2 выполняют sNAT в разные адреса, то в этом случае нет необходимости заботиться о том, с какими значениями Local preference (и иными атрибутами пути) маршруты до соответствующих адресов попадают на Internal router.

4.2.3.2 Распределение нагрузки с помощью протокола BGP (Active-Active)

Введение

В этом разделе описана настройка высокой доступности с использованием протокола BGP в режиме распределения нагрузки (Active-Active). Узлы Angie ADC настраиваются в CLI командой *routing* (общие правила см. в *Настройка динамической маршрутизации*).

В качестве протокола динамической маршрутизации используется BGPv4 для адресного семейства IPv4 unicast; другие адресные семейства в Angie ADC не поддерживаются.

В рассматриваемом примере устройства Angie ADC #1 и Angie ADC #2 выполняют функции активной системы балансировки трафика одновременно. Для динамического исключения одного из Angie ADC из работы в случае сбоя (технические проблемы, потери связности и так далее) можно использовать *механизм RHI (Route Health Injection)*.

Пример типового участка сети с системами балансировки Angie ADC (ADC #1 и ADC #2) представлен на схеме:

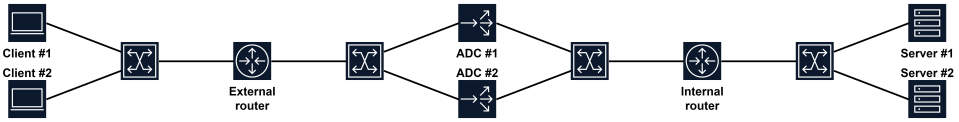


Рис. 1

Добавим IP-адресацию:

- В сегменте сети, куда подключаются External router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.0.0/24`.
- В сегменте сети, куда подключаются Internal router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.1.0/24`.

- Четвертый октет адреса для каждого устройства (в рамках соответствующей подсети) показан на схеме ниже.

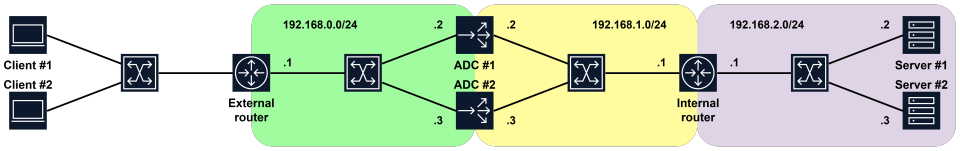


Рис. 2

Адресация клиентов не приводится, так как в данном случае мы будем считать, что их адреса формально не определены, то есть они могут подключаться из любой сети, включая сеть интернет. Для этих целей External router будет анонсировать маршрут по умолчанию по BGP для ADC #1 и ADC #2.

BGP-сессии

Устанавливаемые BGP-сессии представлены на схеме:

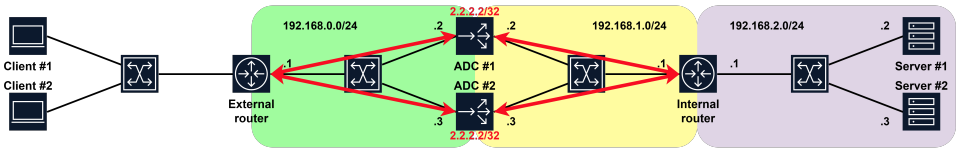


Рис. 3

Красным цветом на схеме отмечены IP-адреса виртуальных серверов. Это те адреса, к которым подключаются клиенты снаружи. ADC #1 и ADC #2 должны анонсировать маршруты до этих виртуальных серверов в сторону External router, причем маршруты через ADC #1 и ADC #2 должны иметь схожие атрибуты пути, чтобы маршрутизатор External router мог выполнить распределение трафика между ними.

Трафик внутри пользовательской сессии от серверов должен возвращаться строго через ту же систему балансировки, через которую он проходил до этого. Добиться этого можно с помощью механизма *SNAT*, когда адрес клиента подменяется на адрес интерфейса системы балансировки.

Обработка типовых сбоев

Ниже описаны сценарии работы Angie ADC при сбоях.

Полный отказ ADC #1

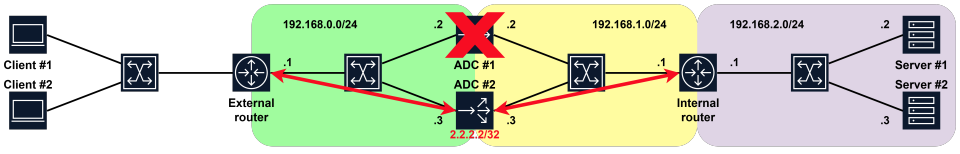


Рис. 4

При полном отказе или отключении от сети ADC #1 разрываются обе BGP-сессии с ADC #1. Через ADC #1 не проходят никакие объявления маршрутов. Остается связь по BGP только с ADC #2. Отключение ADC #1 происходит автоматически. Никакие дополнительные действия не требуются.

Отказ внешнего интерфейса ADC #1

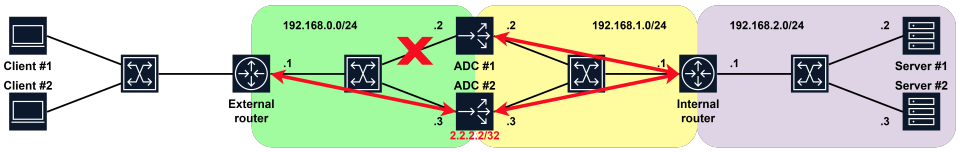


Рис. 5

В этом случае разрывается BGP-сессия между ADC #1 и External router. ADC #1 теперь не может объявить маршрут до адреса виртуального сервера в сторону External router, а пользовательский трафик будет распределяться только на систему балансировки ADC #2. Так как клиентские сессии устанавливаются снаружи, трафик всех вновь устанавливаемых сессий будет проходить только через ADC #2.

Отказ линка между ADC #1 и Internal router

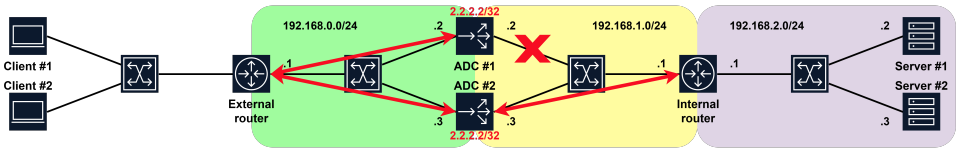


Рис. 6

Если BGP-сессия между External router и ADC #1 сохраняется, то ADC #1 будет продолжать анонсировать маршрут до адреса виртуального сервера, хотя реальные серверы для ADC #1 уже недостижимы. Таким образом, мы получаем классический black hole для трафика. Чтобы избежать этого, анонсирование маршрутов до виртуальных серверов должно быть условным. То есть ADC #1 должен отозвать маршрут до адреса виртуального сервера при падении тестов RHI:

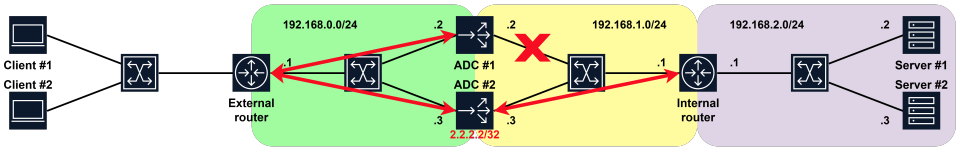


Рис. 7

RHI отзывает только префиксы, которые анонсируются через карту маршрутов со списком префиксов, привязанным к апстриму. Префиксы, заданные командой `routing bgp network`, анонсируются безусловно: в примерах топологий ниже анонс для краткости задан именно так. Чтобы анонс адреса виртуального сервера зависел от состояния апстрима, вместо `routing bgp network 2.2.2.2/32` задайте, например:

```
## routing prefix-list vip seq 5 permit 2.2.2.2/32 upstream myapp1
## routing route-map vip permit 10 match-prefix-list vip
## routing bgp redistribute connected route-map vip
```

Подробнее см. *Настройка RHI*.

Настройка маршрутизации

При настройке BGP-маршрутизации необходимо указывать собственный номер автономной системы.

Примечание

Автономная система BGP — логическое объединение устройств в сети для маршрутизации через протокол BGP.

Ниже приведены примеры трех распространенных топологий настройки маршрутизации во внешнем сегменте сети. Настройка маршрутизации во внутреннем сегменте выполняется аналогично.

Примечание

В список обязательных команд для некоторых платформ необходимо включить команду задания ограничения на максимальное количество путей, между которыми производится ECMP-балансировка.

Пример такой команды для маршрутизаторов Cisco на базе IOS и IOS-XE:

```
platform loadbalance max-paths 2
```

Топология #1

В топологии #1 все три устройства (External router, ADC #1 и ADC #2) принадлежат одной автономной системе:

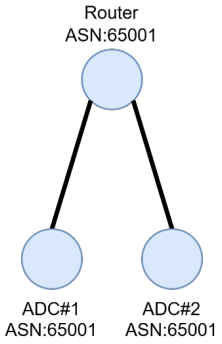


Рис. 8

Обычно на ADC #1 не нужны маршруты, объявляемые со стороны ADC #2. Если для конкретной сети вам нужно, чтобы ADC#1 знал маршруты, которые объявляет ADC #2 (или наоборот), то тогда на маршрутизаторе необходимо создать RR-кластер (Route Reflector cluster). Это позволит обойти ограничение на передачу префиксов, накладываемое правилом BGP split-horizon.

Примечание

Правило BGP split-horizon запрещает отправлять полученные от iBGP-соседа маршруты в сторону другого iBGP-соседа, защищая таким образом от зацикливания маршрутов.

Создание RR-кластера поможет также в ситуации, когда перед маршрутизатором External router расположен другой маршрутизатор, находящийся в той же самой автономной системе.

Ключевые настройки маршрутизации для External router

На примере маршрутизатора Cisco Systems на базе IOS или IOS-XE:

```
!Имя устройства
hostname external
```

```
interface GigabitEthernet0/0
!Интерфейс в сторону систем балансировки
ip address 192.168.0.1 255.255.255.0
router bgp 65001
!Сессия с ADC#1
neighbor 192.168.0.2 remote-as 65001
!Сессия с ADC#2
neighbor 192.168.0.3 remote-as 65001
address-family ipv4
!Включение соседа
neighbor 192.168.0.2 activate
!Включение соседа
neighbor 192.168.0.3 activate
!Анонсирование маршрута по умолчанию
neighbor 192.168.0.2 default-originate
!Анонсирование маршрута по умолчанию
neighbor 192.168.0.3 default-originate
!Добавление соседа в RR-кластер
neighbor 192.168.0.2 route-reflector-client
!Добавление соседа в RR-кластер
neighbor 192.168.0.3 route-reflector-client
!Указание максимального количества iBGP путей, между которыми будет выполняться␣
↪балансировка
maximum-paths ibgp 2
end
```

Ключевые настройки маршрутизации Angie ADC #1

Интерфейс `ens33` в сторону External router — `192.168.0.2/24` (задается в *сетевых настройках*). Адреса виртуальных серверов задаются на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## set system interface lo ip address 3.3.3.3/32
## routing bgp asn 65001
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp network 2.2.2.2/32
## routing bgp network 3.3.3.3/32
```

Ключевые настройки маршрутизации Angie ADC #2

Интерфейс `ens33` в сторону External router — `192.168.0.3/24` (задается в *сетевых настройках*). Адреса виртуальных серверов задаются на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## set system interface lo ip address 4.4.4.4/32
## routing bgp asn 65001
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp network 2.2.2.2/32
## routing bgp network 4.4.4.4/32
```

Проверка работы

```
external#sho ip bgp
BGP table version is 4, local router ID is 192.168.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network Next Hop Metric LocPrf Weight Path
0.0.0.0 0.0.0.0 0 i
*mi 2.2.2.2/32 192.168.0.2 0 100 0 i
*>i 192.168.0.3 0 100 0 i
external#sho ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
2.0.0.0/32 is subnetted, 1 subnets
B 2.2.2.2 [200/0] via 192.168.0.2, 00:12:23
[200/0] via 192.168.0.3, 00:12:23
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
```

Выводы просмотровых команд сокращены для краткости. Для тестирования работы RR-кластера мы завели на ADC #1 адрес `3.3.3.3/32`, а на ADC #2 — `4.4.4.4/32`.

Ниже представлены BGP-таблица и таблица маршрутизации от ADC #2:

```
$$ show ip bgp
BGP table version is 8, local router ID is 4.4.4.4, vrf id 0
Default local pref 100, local AS 65001
Status codes: s suppressed, d damped, h history, u unsorted, * valid, > best, =␣
↪multipath,
i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network Next Hop Metric LocPrf Weight Path
*>i 0.0.0.0/0 192.168.0.1  0 100 0 i
*> 2.2.2.2/32 0.0.0.0(adc2) 0 32768 i
* i 192.168.0.2  0 100 0 i
*>i 3.3.3.3/32 192.168.0.2  0 100 0 i
*> 4.4.4.4/32 0.0.0.0(adc2)   0 32768 i
Displayed 4 routes and 5 total paths
$$ show ip bgp 3.3.3.3
BGP routing table entry for 3.3.3.3/32, version 7
Paths: (1 available, best #1, table default)
Not advertised to any peer
Local
192.168.0.2 from 192.168.0.2 (3.3.3.3)
Origin IGP, metric 0, localpref 100, valid, internal, bestpath-from-AS Local, best␣
↪(First path received)
Originator: 3.3.3.3, Cluster list: 192.168.0.1
```

```
Last update: Mon Apr 21 19:47:21 2025
$$ show ip route
Codes: K - kernel route, C - connected, L - local, S - static,
R - RIP, O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, F - PBR,
f - OpenFabric, t - Table-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure
B 0.0.0.0/0 [200/0] via 192.168.0.1, ens33, weight 1, 00:03:35
L * 2.2.2.2/32 is directly connected, lo, 00:40:12
C>* 2.2.2.2/32 is directly connected, lo, 00:40:12
B>* 3.3.3.3/32 [200/0] via 192.168.0.2, ens33, weight 1, 00:03:35
L * 4.4.4.4/32 is directly connected, lo, 00:40:12
C>* 4.4.4.4/32 is directly connected, lo, 00:40:12
C>* 192.168.0.0/24 is directly connected, ens33, 00:40:13
L>* 192.168.0.3/32 is directly connected, ens33, 00:40:13
```

Топология #2

В топологии #2 все системы балансировки (Angie ADC #1 и Angie ADC #2) принадлежат одной автономной системе, а маршрутизатор External router – другой:

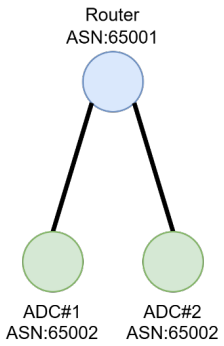


Рис. 9

Обычно на ADC #1 не нужны маршруты, объявляемые со стороны ADC #2. Если для конкретной сети вам нужно, чтобы ADC #1 знал маршруты, которые объявляет ADC #2 (или наоборот), то тогда на системе балансировки нагрузки надо разрешить прием маршрутов, содержащих собственный номер автономной системы в атрибуте `AS-PATH`.

Ключевые настройки маршрутизации для External router

На примере маршрутизатора Cisco Systems на базе IOS или IOS-XE:

```
!Имя устройства
hostname external
!Интерфейс в сторону систем балансировки
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
router bgp 65001
!Сессия с ADC#1
neighbor 192.168.0.2 remote-as 65002
!Сессия с ADC#2
neighbor 192.168.0.3 remote-as 65002
address-family ipv4
!Включение соседа
neighbor 192.168.0.2 activate
```

```
!Включение соседа
neighbor 192.168.0.3 activate
!Анонсирование маршрута по умолчанию
neighbor 192.168.0.2 default-originate
!Анонсирование маршрута по умолчанию
neighbor 192.168.0.3 default-originate
!Указание максимального количества eBGP путей, между которыми будет выполняться␣
↪балансировка
maximum-paths 2
end
```

Ключевые настройки маршрутизации Angie ADC #1

Интерфейс `ens33` в сторону External router — `192.168.0.2/24` (задается в *сетевых настройках*). Адреса виртуальных серверов задаются на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## set system interface lo ip address 3.3.3.3/32
## routing bgp asn 65002
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp network 2.2.2.2/32
## routing bgp network 3.3.3.3/32
## routing bgp neighbor 192.168.0.1 allowas-in origin
```

Команда `allowas-in origin` разрешает принимать от External router маршруты, в атрибуте `AS-PATH` которых есть собственный номер автономной системы, если они порождены в этой автономной системе.

Ключевые настройки маршрутизации Angie ADC #2

Интерфейс `ens33` в сторону External router — `192.168.0.3/24` (задается в *сетевых настройках*). Адреса виртуальных серверов задаются на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## set system interface lo ip address 4.4.4.4/32
## routing bgp asn 65002
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp network 2.2.2.2/32
## routing bgp network 4.4.4.4/32
## routing bgp neighbor 192.168.0.1 allowas-in origin
```

Проверка работы

```
external#sho ip bgp
BGP table version is 11, local router ID is 192.168.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network Next Hop Metric LocPrf Weight Path
0.0.0.0 0.0.0.0 0 i
*> 2.2.2.2/32 192.168.0.2   0 0 65002 i
*m 192.168.0.3   0 0 65002 i
external#sho ip ro
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
2.0.0.0/32 is subnetted, 1 subnets
B 2.2.2.2 [20/0] via 192.168.0.2, 00:13:18
[20/0] via 192.168.0.3, 00:13:18
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
```

Выводы просмотровых команд сокращены для краткости.

Для тестирования команды `allowas-in` мы завели на ADC #1 адрес `3.3.3.3/32`, а на ADC #2 — `4.4.4.4/32`.

Ниже представлены BGP-таблица и таблица маршрутизации от ADC #2:

```
$$ show ip bgp
BGP table version is 4, local router ID is 2.2.2.2, vrf id 0
Default local pref 100, local AS 65002
Status codes: s suppressed, d damped, h history, u unsorted, * valid, > best, =␣
↪multipath,
i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network Next Hop Metric LocPrf Weight Path
*> 0.0.0.0/0 192.168.0.1  0 65001 i
*> 2.2.2.2/32 0.0.0.0(adc2)  0 32768 i
* 192.168.0.2 0 65001 65002 i
*> 3.3.3.3/32 192.168.0.2 0 65001 65002 i
*> 4.4.4.4/32 0.0.0.0(adc2) 0 32768 i
* 192.168.0.1 0 65001 65002 i
Displayed 4 routes and 6 total paths
$$ show ip route
Codes: K - kernel route, C - connected, L - local, S - static,
R - RIP, O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, F - PBR,
f - OpenFabric, t - Table-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure
B 0.0.0.0/0 [20/0] via 192.168.0.1, ens33, weight 1, 00:07:26
L * 2.2.2.2/32 is directly connected, lo, 00:12:14
C>* 2.2.2.2/32 is directly connected, lo, 00:12:14
B>* 3.3.3.3/32 [20/0] via 192.168.0.2, ens33, weight 1, 00:01:02
L * 4.4.4.4/32 is directly connected, lo, 00:06:43
C>* 4.4.4.4/32 is directly connected, lo, 00:06:43
C>* 192.168.0.0/24 is directly connected, ens33, 00:12:15
L>* 192.168.0.3/32 is directly connected, ens33, 00:12:15
```

Топология #3

Все три устройства (External router, ADC #1 и ADC #2) принадлежат разным автономным системам:

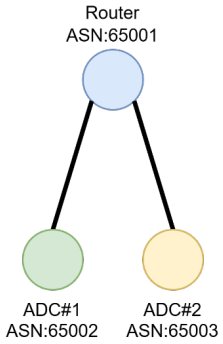


Рис. 10

Обычно маршрутизаторы Cisco не балансируют трафик до подсети, известной через соседей из разных автономных систем. Чтобы обойти данное ограничение, необходимо изменить поведение по умолчанию маршрутизатора BGP с помощью следующей команды:

```
bgp bestpath as-path multipath-relax
```

Ключевые настройки маршрутизации для External router

На примере маршрутизатора Cisco Systems на базе IOS или IOS-XE:

```
!Имя устройства
hostname external
!Интерфейс в сторону систем балансировки
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
router bgp 65001
!Команда, разрешающая выполнять балансировку для префиксов, полученных из разных ASN
bgp bestpath as-path multipath-relax
!Сессия с ADC#1
neighbor 192.168.0.2 remote-as 65002
!Сессия с ADC#2
neighbor 192.168.0.3 remote-as 65003
address-family ipv4
!Включение соседа
neighbor 192.168.0.2 activate
!Включение соседа
neighbor 192.168.0.3 activate
!Анонсирование маршрута по умолчанию
neighbor 192.168.0.2 default-originate
!Анонсирование маршрута по умолчанию
neighbor 192.168.0.3 default-originate
!Указание максимального количества eBGP путей, между которыми будет выполняться␣
↪балансировка
maximum-paths 2
end
```

Ключевые настройки маршрутизации Angie ADC #1

Интерфейс `ens33` в сторону External router — `192.168.0.2/24` (задается в *сетевых настройках*). Адреса виртуальных серверов задаются на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing bgp asn 65002
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp network 2.2.2.2/32
```

Ключевые настройки маршрутизации Angie ADC #2

Интерфейс `ens33` в сторону External router — `192.168.0.3/24` (задается в *сетевых настройках*). Адреса виртуальных серверов задаются на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing bgp asn 65003
## routing bgp neighbor 192.168.0.1 remote-as 65001
## routing bgp network 2.2.2.2/32
```

Проверка работы

```
external#sho ip bgp
BGP table version is 11, local router ID is 192.168.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network Next Hop Metric LocPrf Weight Path
0.0.0.0 0.0.0.0 0 i
*> 2.2.2.2/32 192.168.0.2 0 0 65002 i
*m 192.168.0.3 0 0 65003 i
external#sho ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
2.0.0.0/32 is subnetted, 1 subnets
B 2.2.2.2 [20/0] via 192.168.0.2, 00:10:22
[20/0] via 192.168.0.3, 00:16:07
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
```

Выводы просмотровых команд сокращены для краткости.

Применение с IP transparency

Все описанное выше относится к режиму работы Angie ADC с выключенной опцией IP transparency. В этом случае Angie ADC будет выполнять проксирование клиентских запросов с подменой адресов источника и получателя. Если Angie ADC подменяет адрес клиента, то при маршрутизации нет необходимости анонсировать на Internal router маршрут по умолчанию. Если ADC #1 и ADC #2 используют разные адреса для подмены адреса клиента, то нет необходимости заботиться о том, с какими значениями Local preference (и иными атрибутами пути) маршруты до соответствующих адресов попадают на Internal router.

При включении опции IP Transparency Angie ADC будет сохранять исходный адрес отправителя в IP-пакетах, позволяя серверам на сетевом уровне различать клиентские подключения.

Заключение

Система балансировки нагрузки Angie ADC может работать в любой из перечисленных топологий. Каждый вариант имеет свои особенности настройки и работы, о чем следует помнить при проектировании и настройке информационной системы.

4.2.4 OSPF-маршрутизация

В этом разделе описана настройка OSPF-маршрутизации для обеспечения высокой доступности в режиме резервирования (Active-Standby) и в режиме распределения нагрузки (Active-Active). BGP и OSPF настраиваются в CLI командой *routing* (общие правила см. в *Настройка динамической маршрутизации*).

В этом разделе:

- *Режим резервирования (Active-Standby)*
- *Режим распределения нагрузки (Active-Active)*

4.2.4.1 Резервирование с помощью протокола OSPF (Active-Standby)

Введение

В этом разделе описана настройка высокой доступности с использованием протокола OSPF в режиме резервирования (Active-Standby). Узлы Angie ADC настраиваются в CLI командой *routing* (общие правила см. в *Настройка динамической маршрутизации*).

В качестве протокола динамической маршрутизации используется OSPFv2 для адресного семейства IPv4 unicast; OSPFv3 и IPv6 в Angie ADC не поддерживаются.

Для обеспечения отказоустойчивости нужны две системы балансировки Angie ADC — основная и резервная. Резервная система Angie ADC будет принимать нагрузку при отказе основной.

Пример типового участка сети с системами балансировки Angie ADC (ADC #1 и ADC #2):

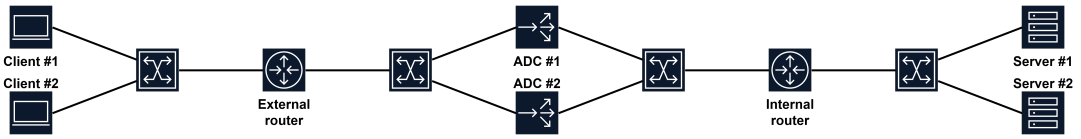


Рис. 1

Добавим *IP-адресацию*:

- В сегменте сети, куда подключаются External router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.0.0/24`.
- В сегменте сети, куда подключаются Internal router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.1.0/24`.

- Четвертый октет адреса для каждого устройства (в рамках соответствующей подсети) показан на схеме ниже.

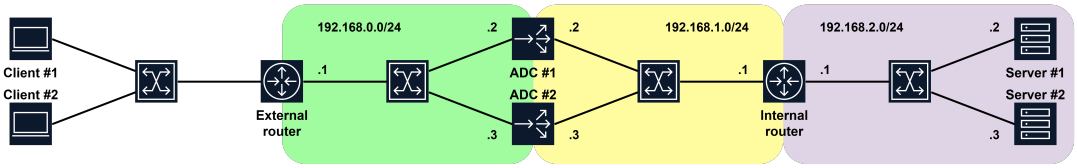


Рис. 2

Адресация клиентов не приводится, так как в данном случае мы будем считать, что их адреса формально не определены, то есть, они могут подключаться из любой сети, включая сеть интернет. Для этих целей External router будет анонсировать маршрут по умолчанию по OSPF для ADC #1 и ADC #2. Мы будем использовать OSPF-домен, включающий в себя четыре устройства: External router, Internal router, ADC #1 и ADC #2.

Красным текстом на схеме ниже отмечены *IP-адреса виртуальных серверов*. Это те адреса, к которым подключаются клиенты снаружи. Системы балансировки Angie ADC должны анонсировать маршруты до этих виртуальных серверов в сторону External router, причем маршрут через ADC #1 должен быть более предпочтительным. Добиться этого можно разными способами, например, манипулируя значением метрики внешнего маршрута в OSPF. Чем больше значение метрики, тем менее предпочтительный маршрут. В данном документе мы будем вручную задавать косты для интерфейсов системы балансировки.

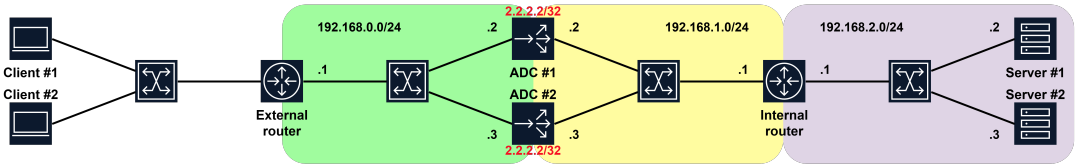


Рис. 3

Трафик от серверов в сторону клиента должен проходить через ту же систему балансировки, что и трафик от клиентов к серверам. Добиться этого можно также путем манипулирования значением метрики для префикса `0.0.0.0/0`. Манипуляции с маршрутом по умолчанию нужны при включении опции IP transparency. В противном случае трафик и так будет возвращаться через ту же систему балансировки, так как поведение ADC напоминает операцию sNAT.

Обработка типовых сбоев

Ниже описаны сценарии работы Angie ADC при сбоях.

Полный отказ ADC #1

В этом случае оба OSPF-соседства с ADC #1 разрываются, никакие объявления маршрутов через ADC #1 не пролетают. Остается связь по OSPF только с ADC #2. То есть, переключение на резервную систему производится полностью автоматически, никакие дополнительные настройки не требуются.

Красными стрелками обозначены рабочие OSPF-соседства:

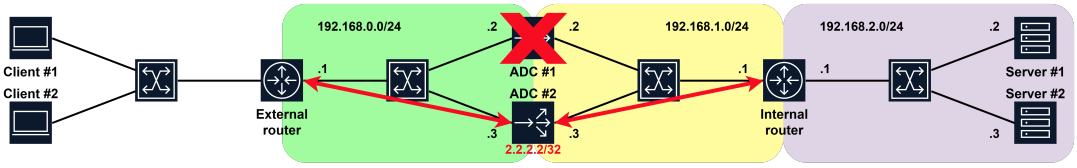


Рис. 4

Отказ внешнего интерфейса ADC #1

Пример частичного отказа — отказ линка между ADC #1 и External router — представлен на схеме ниже.

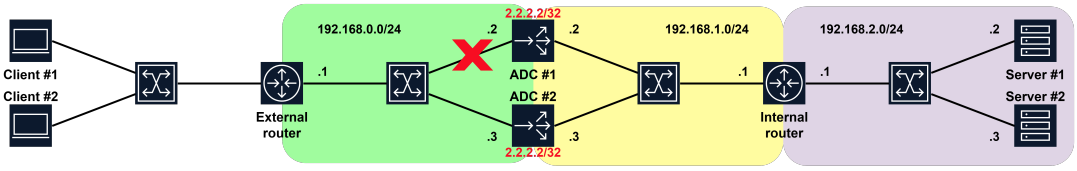


Рис. 5

В случае обозначенного на схеме отказа линка разрывается OSPF-сессия между ADC #1 и External router. ADC #1 теперь не может объявить маршрут до адреса виртуального сервера в сторону External router напрямую. Internal router рассчитывает маршрут по умолчанию только через ADC #2, а External router считает маршрут до адреса виртуального сервера только через полностью работающий ADC #2.

Отказ линка между ADC #1 и Internal router

Отказ линка между ADC #1 и Internal router более сложная ситуация: если OSPF-соседство между External router и ADC #1 сохраняется, то ADC #1 будет продолжать анонсировать маршрут до адреса виртуального сервера, хотя реальные сервера для системы балансировки ADC #1 уже недостижимы.

Таким образом, мы получаем классический пример black hole для трафика:

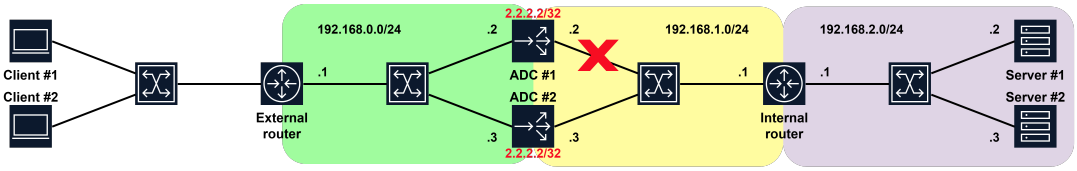


Рис. 6

Избежать этого можно двумя способами: отзывать анонс адреса сервиса при недоступности апстрима (*RHI*) или исключить отказ одного линка отказоустойчивым подключением к сети хоста виртуализации, на котором работает ADC.

Рекомендованная схема такого подключения:

- Объединить в одну LAG-группу все физические интерфейсы хоста виртуализации и использовать этот виртуальный LAG-интерфейс в качестве транка, то есть передавать по нему тегированными несколько виртуальных сетей (один VLAN для external сети, второй VLAN для internal сети).
- Для резервирования коммутаторов можно использовать технологию vPC или стекирование, пример представлен на схеме ниже.

Из соображений простоты на схеме не отображено резервирование внешнего и внутреннего маршрутизаторов.

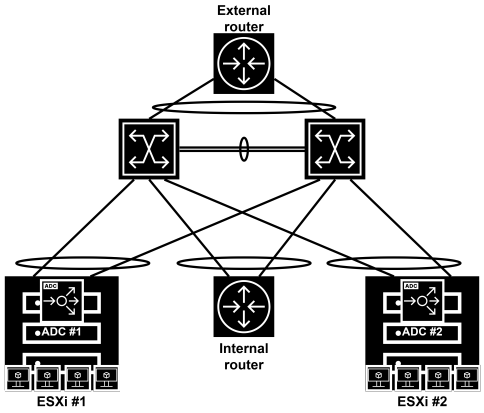


Рис. 7

Настройки маршрутизации

Приведем ключевые настройки маршрутизации для External router, Internal router, ADC #1 и ADC #2.

Примечание

В этой схеме ADC #1 и ADC #2 — самостоятельные узлы с разными настройками маршрутизации. Синхронизация *пары высокой доступности* копирует маршрутизацию узла Active на узел Standby целиком, поэтому для пары используйте схему из *OSPF*.

Ключевые настройки маршрутизации для External router

```
hostname external
!Имя устройства
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
!Интерфейс в сторону систем балансировки
router ospf 1
 network 192.168.0.0 0.0.0.255 area 0
!Включение OSPF на интерфейсе в сторону систем балансировки
 default-information originate always
!Анонсирование маршрута по умолчанию
end
```

Ключевые настройки маршрутизации для Internal router

```
hostname internal
!Имя устройства
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!Интерфейс в сторону систем балансировки
interface GigabitEthernet1/0
ip address 192.168.2.1 255.255.255.0
!Интерфейс в сторону подсети с реальными серверами
router ospf 1
 redistribute connected subnets
!добавление в OSPF информации о подсети с серверами
 network 192.168.1.0 0.0.0.255 area 0
```

```
!Включение OSPF на интерфейсе в сторону систем балансировки
end
```

Ключевые настройки маршрутизации системы балансировки ADC #1

Интерфейсы задаются в *сетевых настройках* узла: `ens33` — `192.168.0.2/24` (в сторону External router), `ens37` — `192.168.1.2/24` (в сторону Internal router). Адрес виртуального сервера `2.2.2.2/32` задается на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing prefix-list c2o seq 5 permit 2.2.2.2/32
## routing route-map c2o permit 10 match-prefix-list c2o
## routing ospf 1
## routing ospf 1 router-id 2.2.2.2
## routing ospf 1 interface ens33 area 0
## routing ospf 1 interface ens33 cost 10
## routing ospf 1 interface ens37 area 0
## routing ospf 1 redistribute connected metric 10 route-map c2o
```

Назначение команд:

- `interface ... area 0` включает OSPF на интерфейсах, `cost` задает стоимость интерфейса вручную;
- список префиксов и карта маршрутов `c2o` отбирают для OSPF только адрес виртуального сервера;
- `router-id` задается вручную: иначе ADC #1 и ADC #2 могут выбрать одинаковый идентификатор, например общий адрес на `lo`;
- `redistribute connected metric 10` добавляет адрес виртуального сервера в OSPF; метрика 10 делает ADC #1 более предпочтительным next-hop, чем ADC #2.

Ключевые настройки маршрутизации системы балансировки ADC #2

Интерфейсы задаются в *сетевых настройках* узла: `ens33` — `192.168.0.3/24` (в сторону External router), `ens37` — `192.168.1.3/24` (в сторону Internal router). Адрес виртуального сервера `2.2.2.2/32` задается на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing prefix-list c2o seq 5 permit 2.2.2.2/32
## routing route-map c2o permit 10 match-prefix-list c2o
## routing ospf 1
## routing ospf 1 router-id 22.22.22.22
## routing ospf 1 interface ens33 area 0
## routing ospf 1 interface ens33 cost 100
## routing ospf 1 interface ens37 area 0
## routing ospf 1 redistribute connected metric 20 route-map c2o
```

Настройки отличаются от ADC #1 адресами интерфейсов, идентификатором маршрутизатора, стоимостью интерфейса `ens33` (100) и метрикой (20), поэтому путь через ADC #2 менее предпочтителен.

Проверка работы

Выполним проверку работы системы маршрутизации, когда ADC #1 и ADC #2 находятся в полностью работоспособном состоянии.

Примечание

В листингах ниже отсутствуют префиксы, не относящиеся к обсуждаемым вопросам отказоустойчивости.

Маршрутизатор External router видит маршрут к адресу виртуального сервера через обе системы балансировки, однако маршрут через ADC #1 является более предпочтительным.

```
external#sho ip ro os
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
      2.0.0.0/32 is subnetted, 1 subnets
O E2     2.2.2.2 [110/10] via 192.168.0.2, 00:41:28, GigabitEthernet0/0
external#sho ip os da ex 2.2.2.2
            OSPF Router with ID (192.168.0.1) (Process ID 1)
                Type-5 AS External Link States
  Routing Bit Set on this LSA in topology Base with MTID 0

  LS age: 898
  Options: (No TOS-capability, No DC, Upward)
  LS Type: AS External Link
  Link State ID: 2.2.2.2 (External Network Number )
  Advertising Router: 2.2.2.2
  LS Seq Number: 80000003
  Checksum: 0xAA0C
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 10
        Forward Address: 0.0.0.0
        External Route Tag: 0

  LS age: 885
  Options: (No TOS-capability, No DC, Upward)
  LS Type: AS External Link
  Link State ID: 2.2.2.2 (External Network Number )
  Advertising Router: 22.22.22.22
  LS Seq Number: 80000003
  Checksum: 0xB4A7
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 20
```

```
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

Маршрутизатор Internal router видит маршрут по умолчанию (путь через ADC #1 является более предпочтительным).

```
internal#sho ip ro os
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 192.168.1.2, 00:43:21, GigabitEthernet0/0
internal#sho ip os da ext 0.0.0.0
            OSPF Router with ID (192.168.2.1) (Process ID 1)
                Type-5 AS External Link States
  Routing Bit Set on this LSA in topology Base with MTID 0
  LS age: 992
  Options: (No TOS-capability, DC, Upward)
  LS Type: AS External Link
  Link State ID: 0.0.0.0 (External Network Number )
  Advertising Router: 192.168.0.1
  LS Seq Number: 80000003
  Checksum: 0x2521
  Length: 36
  Network Mask: /0
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 1
        Forward Address: 0.0.0.0
        External Route Tag: 1
```

Отключим теперь ADC #1 полностью и проверим маршрутизацию.

Маршрутизатор Internal router:

```
internal#sho ip ro os
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is 192.168.1.3 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 192.168.1.3, 00:01:08, GigabitEthernet0/0
```

Маршрутизатор External router:

```
external#sho ip ro os
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override
Gateway of last resort is not set
     2.0.0.0/32 is subnetted, 1 subnets
O E2     2.2.2.2 [110/10] via 192.168.0.3, 00:00:10, GigabitEthernet0/0
```

После возвращения в строй системы балансировки ADC #1 маршрутизация через это устройство восстанавливается.

Заключение

Все описанное выше относится к режиму работы системы балансировки трафика с включенной опцией IP transparency. При опции IP Transparency Angie ADC сохраняет исходный адрес отправителя в IP-пакетах, позволяя серверам на сетевом уровне различать клиентские подключения. Очень часто администраторы систем балансировки отключают эту опцию, в этом случае Angie ADC будет выполнять не только dNAT, но sNAT над трафиком, приходящим от клиентов. Если система балансировки выполняет sNAT, то в этом случае маршрутизация несколько упрощается, так как в этом случае нет необходимости анонсировать в сторону Internal router маршрут по умолчанию. Если ADC #1 и ADC #2 выполняют sNAT в разные адреса, то в этом случае нет необходимости заботиться о том, с какими значениями метрики маршруты до соответствующих адресов попадают на маршрутизатор Internal router, так как анонсы будут уникальными.

4.2.4.2 Распределение нагрузки с помощью протокола OSPF (Active-Active)

Введение

В этом разделе описана настройка высокой доступности с использованием протокола OSPF в режиме распределения нагрузки (Active-Active). Узлы Angie ADC настраиваются в CLI командой *routing* (общие правила см. в *Настройка динамической маршрутизации*).

В качестве протокола динамической маршрутизации используется OSPFv2 для адресного семейства IPv4 unicast; OSPFv3 и IPv6 в Angie ADC не поддерживаются.

Для обеспечения распределения нагрузки между ADC нужны две системы балансировки Angie, работающие параллельно и одновременно. Пример типового участка сети с системами балансировки Angie ADC (ADC #1 и ADC #2):

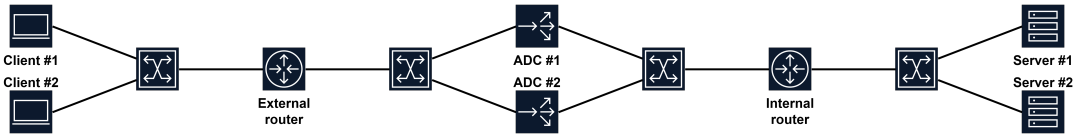


Рис. 1

Добавим *IP-адресацию*:

- В сегменте сети, куда подключаются External router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.0.0/24`.
- В сегменте сети, куда подключаются Internal router, ADC #1 и ADC #2, будет использоваться подсеть `192.168.1.0/24`.
- Четвертый октет адреса для каждого устройства (в рамках соответствующей подсети) показан на схеме ниже.

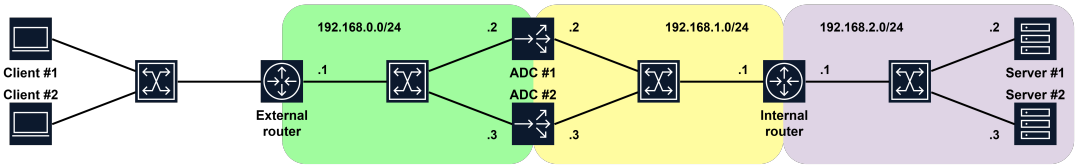


Рис. 2

Адресация клиентов не приводится, так как в данном случае мы будем считать, что их адреса формально не определены, то есть, они могут подключаться из любой сети, включая сеть интернет. Для этих целей External router будет анонсировать маршрут по умолчанию по OSPF для ADC #1 и ADC #2. Мы будем использовать OSPF-домен, включающий в себя четыре устройства: External router, Internal router, ADC #1 и ADC #2.

Красным текстом на схеме ниже отмечены *IP-адреса виртуальных серверов*. Это те адреса, к которым подключаются клиенты снаружи. Чтобы маршрутизатор External router мог выполнить распределение трафика между системами балансировки Angie ADC (см. ECMP – Equal-Cost Multi-Path), они должны одинаково анонсировать маршруты до виртуальных серверов в сторону External router (должны совпадать типы маршрутов и косты).

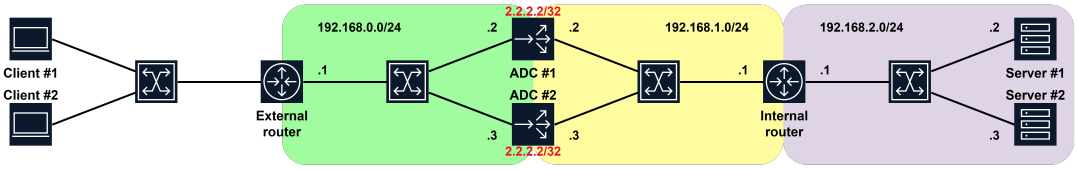


Рис. 3

Трафик внутри пользовательской сессии от серверов должен возвращаться строго через ту же систему балансировки, через которую он проходил до этого. Добиться этого можно с помощью механизма *SNAT*, когда адрес клиента подменяется на адрес интерфейса системы балансировки.

Обработка типовых сбоев

Ниже описаны сценарии работы Angie ADC при сбоях.

Полный отказ ADC #1

В этом случае оба OSPF-соседства с ADC #1 разрываются, никакие объявления маршрутов через ADC #1 не пролетают. Остается связь по OSPF только с ADC #2. То есть, переключение на резервную систему производится полностью автоматически, никакие дополнительные настройки не требуются.

Красными стрелками обозначены рабочие OSPF-соседства:

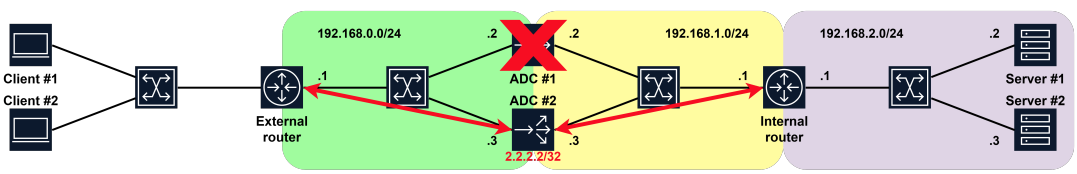


Рис. 4

Отказ внешнего интерфейса ADC #1

Пример такого отказа представлен на схеме ниже.

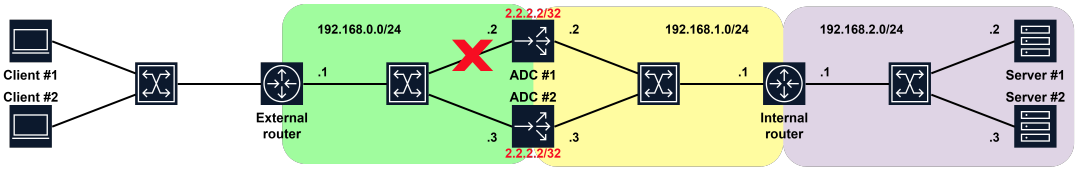


Рис. 5

В случае обозначенного на схеме отказа линка разрывается OSPF-сессия между ADC #1 и External router. ADC #1 теперь не может объявить маршрут до адреса виртуального сервера в сторону External router напрямую. Internal router получает маршруты до адресов, которые используются в SNAT от обеих систем балансировки, однако трафик от клиентов, прошедший через ADC #2, будет возвращаться тем же путем (так же через ADC #2), так как ADC #1 и ADC #2 используют уникальные адреса для SNAT.

Отказ линка между ADC #1 и Internal router

Отказ линка между ADC #1 и Internal router более сложная ситуация: если OSPF-соседство между External router и ADC #1 сохраняется, то ADC #1 будет продолжать анонсировать маршрут до адреса виртуального сервера, хотя реальные сервера для системы балансировки ADC #1 уже недостижимы.

Таким образом, мы получаем классический пример black hole для трафика:

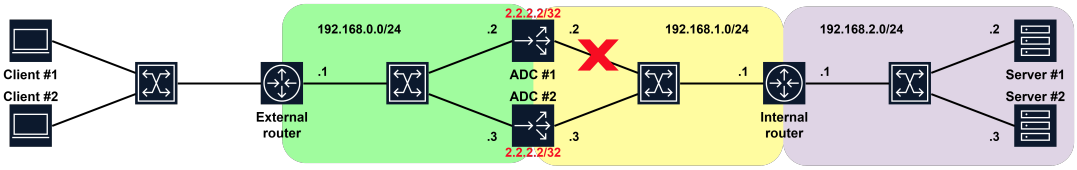


Рис. 6

Избежать этого можно двумя способами: отзывать анонс адреса сервиса при недоступности апстрима (*RHI*) или исключить отказ одного линка отказоустойчивым подключением к сети хоста виртуализации, на котором работает ADC.

Рекомендованная схема такого подключения:

- Объединить в одну LAG-группу все физические интерфейсы хоста виртуализации и использовать этот виртуальный LAG-интерфейс в качестве транка, то есть передавать по нему тегированными несколько виртуальных сетей (один VLAN для внешней (external) сети, второй VLAN для внутренней (internal) сети).
- Для резервирования коммутаторов можно использовать такие технологии как vPC, VSS или стекирование, пример представлен на схеме ниже.

Из соображений простоты на схеме не отображено резервирование внешнего и внутреннего маршрутизаторов.

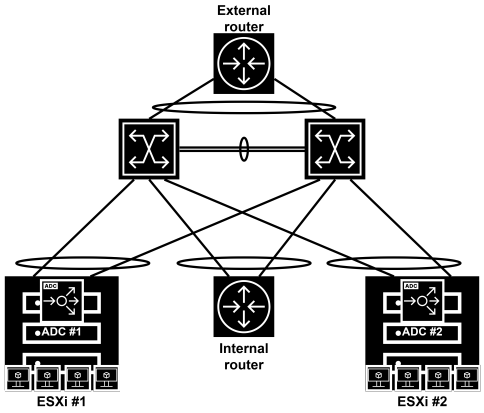


Рис. 7

Предупреждение

Маршрутизатор, выполняющий ECMP-балансировку, и обе системы Angie ADC могут располагаться в одной OSPF-зоне или в разных. Если при этом маршрутизатор является OSPF ABR (Area Border Router), а ADC #1 и ADC #2 находятся в разных OSPF-зонах (видны через разные интерфейсы ABR), то ECMP-балансировка может не поддерживаться некоторыми вендорами сетевого оборудования.

Такой дизайн сети не рекомендуется:

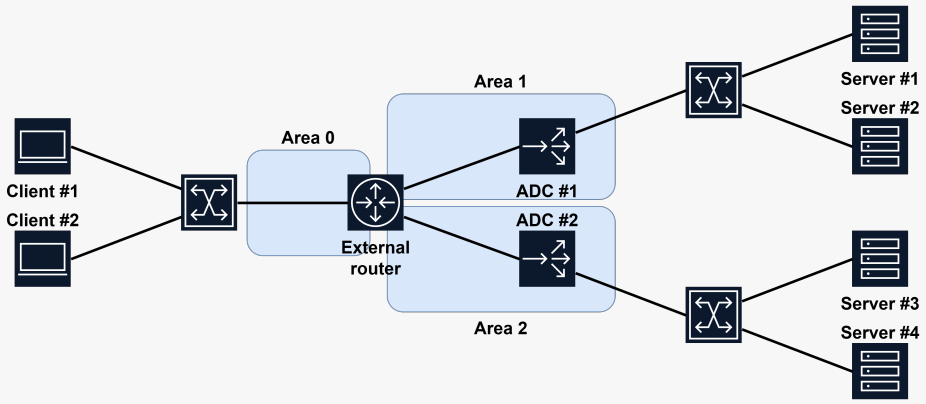


Рис. 8

Настройки маршрутизации

Приведем ключевые настройки маршрутизации для External router, Internal router, ADC #1 и ADC #2.

Ключевые настройки маршрутизации для External router

```
!Имя устройства
hostname external
!Интерфейс в сторону систем балансировки
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
router ospf 1
!Включение OSPF на интерфейсе в сторону систем балансировки
network 192.168.0.0 0.0.0.255 area 0
```

```
!Анонсирование маршрута по умолчанию
default-information originate always
end
```

Ключевые настройки маршрутизации для Internal router

```
!Имя устройства
hostname internal
!Интерфейс в сторону систем балансировки
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
!Интерфейс в сторону подсети с реальными серверами
interface GigabitEthernet1/0
ip address 192.168.2.1 255.255.255.0
router ospf 1
!Добавление в OSPF информации о подсети с серверами
redistribute connected subnets
!Включение OSPF на интерфейсе в сторону систем балансировки
network 192.168.1.0 0.0.0.255 area 0
end
```

Ключевые настройки маршрутизации системы балансировки ADC #1

Интерфейсы задаются в *сетевых настройках* узла: `ens33` — `192.168.0.2/24` (в сторону External router), `ens37` — `192.168.1.2/24` (в сторону Internal router). Адрес виртуального сервера `2.2.2.2/32` задается на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing prefix-list c2o seq 5 permit 2.2.2.2/32
## routing route-map c2o permit 10 match-prefix-list c2o
## routing ospf 1
## routing ospf 1 router-id 2.2.2.2
## routing ospf 1 interface ens33 area 0
## routing ospf 1 interface ens37 area 0
## routing ospf 1 redistribute connected route-map c2o
```

Список префиксов и карта маршрутов `c2o` отбирают для OSPF только адрес виртуального сервера. Идентификатор маршрутизатора задается вручную: иначе ADC #1 и ADC #2 могут выбрать одинаковый, например общий адрес на `lo`. Стоимость интерфейсов и метрика не задаются, поэтому пути через оба узла равноценны.

Ключевые настройки маршрутизации системы балансировки ADC #2

Интерфейсы задаются в *сетевых настройках* узла: `ens33` — `192.168.0.3/24` (в сторону External router), `ens37` — `192.168.1.3/24` (в сторону Internal router). Адрес виртуального сервера `2.2.2.2/32` задается на *интерфейсе lo*.

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing prefix-list c2o seq 5 permit 2.2.2.2/32
## routing route-map c2o permit 10 match-prefix-list c2o
## routing ospf 1
## routing ospf 1 router-id 22.22.22.22
## routing ospf 1 interface ens33 area 0
## routing ospf 1 interface ens37 area 0
## routing ospf 1 redistribute connected route-map c2o
```

Настройки отличаются от ADC #1 только адресами интерфейсов и идентификатором маршрутизатора.

Проверка работы

Выполним проверку работы системы маршрутизации, когда ADC #1 и ADC #2 находятся в полностью работоспособном состоянии.

Примечание

В листингах ниже отсутствуют префиксы, не относящиеся к обсуждаемым вопросам отказоустойчивости.

Маршрутизатор External router видит маршрут к адресу виртуального сервера через обе системы балансировки.

```
external#sho ip ro os
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
2.0.0.0/32 is subnetted, 1 subnets
O E2     2.2.2.2 [110/20] via 192.168.0.2, 00:41:28, GigabitEthernet0/0
via 192.168.0.3, 00:41:15, GigabitEthernet0/0
external#sho ip os da ex 2.2.2.2
OSPF Router with ID (192.168.0.1) (Process ID 1)
Type-5 AS External Link States
Routing Bit Set on this LSA in topology Base with MTID 0

LS age: 898
Options: (No TOS-capability, No DC, Upward)
LS Type: AS External Link
Link State ID: 2.2.2.2 (External Network Number )
Advertising Router: 2.2.2.2
LS Seq Number: 80000003
Checksum: 0xAA0C
Length: 36
Network Mask: /32
Metric Type: 2 (Larger than any link state path)
MTID: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 0

LS age: 885
Options: (No TOS-capability, No DC, Upward)
LS Type: AS External Link
Link State ID: 2.2.2.2 (External Network Number )
Advertising Router: 22.22.22.22
LS Seq Number: 80000003
Checksum: 0xB4A7
```

```
Length: 36
Network Mask: /32
Metric Type: 2 (Larger than any link state path)
MTID: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 0
```

По умолчанию Angie ADC будет устанавливать соединение с апстрим-сервером с адреса того интерфейса, через который этот сервер достижим, в соответствии с таблицей маршрутизации (`192.168.1.2` для ADC #1 и `192.168.1.3` для ADC #2). Оба адреса принадлежат подсети `192.168.1.0/24`, которая для маршрутизатора Internal router является непосредственно подключенной (Directly Connected). Анонсировать другие адреса не нужно. При использовании пула SNAT добавьте адреса пула в список префиксов, чтобы узел анонсировал и их (см. *Настройка пула SNAT (SNAT Pool)*).

Отключим теперь ADC #1 полностью и проверим маршрутизацию.

Маршрутизатор External router:

```
external#sho ip ro os
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
2.0.0.0/32 is subnetted, 1 subnets
O E2     2.2.2.2 [110/20] via 192.168.0.3, 01:40:10, GigabitEthernet0/0
```

После возвращения в строй ADC #1 маршрутизация через это устройство восстанавливается.

Применение с IP transparency

Все описанное выше относится к режиму работы системы балансировки трафика с отключенной опцией IP transparency. При включении опции IP Transparency Angie ADC сохраняет исходный адрес отправителя в IP-пакетах, позволяя серверам на сетевом уровне различать клиентские подключения. Однако в этом случае маршрутизатор Internal router будет возвращать трафик через неправильную систему балансировки. Исходный адрес клиента может быть передан серверу либо с помощью заголовка X-FORWARDED-FOR, либо с помощью специального proxy protocol.

4.2.5 Статическая маршрутизация

Статические маршруты и правила маршрутизации задаются в веб-интерфейсе Angie ADC на странице `Система` → `Сетевые настройки` отдельно для каждого узла.

- Статические маршруты задаются в блоке `Маршруты`, см. *Маршруты*.
- Правила маршрутизации, которые направляют трафик с указанных адресов источника в отдельную таблицу маршрутизации, задаются в блоке `Правила маршрутизации`, см. *Правила маршрутизации*.

4.2.5.1 Пример

Чтобы трафик из сети `10.21.20.0/24` уходил через шлюз `10.90.90.90`, а остальной трафик узла маршрутизировался по основной таблице:

1. Перейдите в раздел `Система` → `Сетевые настройки`.

2. Выберите нужный узел.
3. В блоке `Маршруты` добавьте маршрут:
   - `Сеть назначения` — `0.0.0.0/0`;
   - `Тип` — `Обычный`;
   - `Шлюз` — `10.90.90.90`;
   - `Интерфейс` — интерфейс, через который доступен шлюз;
   - `Таблица` — `100`.
4. В блоке `Правила маршрутизации` добавьте правило:
   - `Сеть источника` — `10.21.20.0/24`;
   - `Таблица` — `100`.
5. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

4.2.6 Использование протокола BFD для уменьшения времени реакции

4.2.6.1 Введение

Стандартные таймеры протоколов маршрутизации слишком велики и не подходят для современных сетей. Уменьшить время реакции протокола на какое-либо событие (непрямое падение, indirect failure) можно двумя способами:

- за счет уменьшения значения таймеров (может привести к увеличению нагрузки);
- с помощью специализированного протокола — BFD (предпочтительный способ).

BFD (Bidirectional Forwarding Detection) — это легковесный протокол, используемый для быстрого обнаружения отказов сетевых каналов между двумя устройствами. Он работает независимо и комплементарно к протоколам маршрутизации и помогает быстро определить, что связь между узлами нарушена. Если в инфраструктуре важна быстрая реакция на сбои, BFD значительно уменьшает время сходимости сети, так как позволяет получить субсекундное время реакции.

Как работает BFD?

1. Установление сессии: два сетевых устройства обмениваются контрольными пакетами BFD для установления связи.
2. Мониторинг: оба узла отправляют друг другу небольшие пакеты с фиксированным интервалом.
3. Обнаружение отказа: если один из узлов перестает получать пакеты от соседа в течение заданного времени, соединение объявляется "down".
4. Реакция: протоколы маршрутизации отслеживают состояние BFD-сессий и разрывают свои соединения, что позволяет переключиться на резервный канал менее, чем за секунду после сбоя.

> **Примечание**
>
> Для настройки используется *командная строка Angie ADC CLI*.

4.2.6.2 Настройка с OSPF

Для протокола OSPF поддержка BFD активируется на интерфейсе с помощью команды `ip ospf bfd`.

Пример конфигурации интерфейса:

```
interface ens33
ip address 192.168.0.2/24
ip ospf 1 area 0
ip ospf bfd
ip ospf bfd profile test
```

Если параметры работы протокола BFD на каком-либо интерфейсе должны отличаться от стандартных, то новые параметры можно указать путем привязки профиля.

Протокол OSPF осуществляет динамическое обнаружение соседей на интерфейсе, а затем протокол BFD пытается установить с ними соседство:

```
angie-va# sho bfd peers
BFD Peers:
peer 192.168.0.3 vrf default interface ens33
ID: 192599120
Remote ID: 626157519
Active mode
Status: up
Uptime: 4 second(s)
Diagnostics: ok
Remote diagnostics: ok
Peer Type: dynamic
RTT min/avg/max: 0/0/0 usec
Local timers:
Detect-multiplier: 3
Receive interval: 300ms
Transmission interval: 300ms
Echo receive interval: 50ms
Echo transmission interval: disabled
Remote timers:
Detect-multiplier: 3
Receive interval: 300ms
Transmission interval: 300ms
Echo receive interval: 50ms
```

Протокол BFD может установить сессию с каким-либо соседом через определенный интерфейс и одновременно с этим не установить сессию с другим соседом. Это ожидаемое поведение для соседей, не обладающих поддержкой BFD. OSPF-соединение при этом не разрывается.

Если протокол BFD смог установить сессию с каким-либо из OSPF-соседей, то доступность этого соседа будет определяться с помощью протокола BFD.

Если протокол BFD не смог установить сессию с каким-либо из OSPF-соседей, то доступность этого соседа будет определяться с помощью встроенных механизмов OSPF (протокол Hello). При этом команда `sho bfd peers` будет отображать такого соседа в статусе `down`:

```
angie-va# sho bfd peers
BFD Peers:
peer 192.168.0.3 vrf default interface ens33
ID: 192599120
Remote ID: 0
Active mode
Status: down
Downtime: 4 minute(s), 0 second(s)
Diagnostics: ok
Remote diagnostics: ok
Peer Type: dynamic
RTT min/avg/max: 0/0/0 usec
```

```
Local timers:
Detect-multiplier: 3
Receive interval: 300ms
Transmission interval: 300ms
Echo receive interval: 50ms
Echo transmission interval: disabled
Remote timers:
Detect-multiplier: 3
Receive interval: 1000ms
Transmission interval: 1000ms
Echo receive interval: disabled
```

4.2.6.3 Настройка с BGP

По умолчанию при указании BGP-соседа BFD-сессия между маршрутизаторами не устанавливается.

Пример такой конфигурации:

```
angie-va# sho run
! Часть конфига, не относящаяся к BGP/BFD, удалена для краткости.
router bgp 3
no bgp ebgp-requires-policy
neighbor 192.168.0.2 remote-as 2
exit
!
angie-va# sho ip bg su
IPv4 Unicast Summary:
BGP router identifier 3.3.3.3, local AS number 3 VRF default vrf-id 0
BGP table version 0
RIB entries 0, using 0 bytes of memory
Peers 1, using 24 KiB of memory
Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/
↪PfxRcd   PfxSnt Desc
192.168.0.2     4          2         8         9        0    0    0 00:05:35
↪  0        0 N/A
! BGP сессия успешно установлена, хотя никаких BFD-соседей у системы нет.
Total number of neighbors 1

angie-va# sho bfd pe
BFD Peers:
angie-va#
```

Чтобы активировать установление BFD-сессии с BGP-соседом, установите в секции настройки маршрутизатора BGP опцию `bfd` для соседа:

```
router bgp 2
no bgp ebgp-requires-policy
neighbor 192.168.0.3 remote-as 3
neighbor 192.168.0.3 bfd
exit
```

Чтобы BFD-сессия поднялась, необходимо включить поддержку BFD в настройках процесса маршрутизации BGP с обеих сторон. Еще одним способом является создание BFD-соседа вручную.

BGP-сессия успешно устанавливается и обновления передаются даже в ситуации, когда BFD-сессия не была установлена. Однако, если BFD-сессия была установлена, а затем разорвана, то автоматически будет разорвана и соответствующая BGP-сессия (после чего будут предприняты попытки переустановить BGP-сессию).

```
angie-va# sho bfd peers
BFD Peers:
peer 192.168.0.3 local-address 192.168.0.2 vrf default interface ens33
ID: 2213541843
Remote ID: 0
Active mode
Status: down
Downtime: 5 second(s)
Diagnostics: neighbor signaled session down
Remote diagnostics: neighbor signaled session down
Peer Type: dynamic
RTT min/avg/max: 0/0/0 usec
Local timers:
Detect-multiplier: 3
Receive interval: 300ms
Transmission interval: 300ms
Echo receive interval: 50ms
Echo transmission interval: disabled
Remote timers:
Detect-multiplier: 3
Receive interval: 300ms
Transmission interval: 300ms
Echo receive interval: 50ms

angie-va# sho ip bg su

IPv4 Unicast Summary:
BGP router identifier 2.2.2.2, local AS number 2 VRF default vrf-id 0
BGP table version 0
RIB entries 0, using 0 bytes of memory
Peers 1, using 24 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/
↪PfxRcd   PfxSnt Desc
192.168.0.3     4          3        27        30        0    0    0 00:00:06
↪  0        0 N/A

Total number of neighbors 1
```

4.2.6.4 Настройка с VRRP

На данный момент нет интеграции с BFD.

4.2.6.5 Настройка со статическими маршрутами

Angie ADC поддерживает условное добавление статического маршрута (в зависимости от BFD-статуса соседа, который указан в качестве next-hop). То есть, если BFD-сессия до устройства, адрес которого указан как next-hop, поднимается, то статический маршрут добавляется в таблицу маршрутизации. Если сессия остается в статусе `down` (или падает в процессе эксплуатации позднее), маршрут не добавляется (удаляется) из таблицы маршрутизации.

Добавить статический маршрут с проверкой доступности next-hop по BFD можно, например, с помощью следующей команды:

```
ip route 3.3.3.3/32 192.168.0.3 bfd
```

Сразу после создания такого статического маршрута соответствующая BFD-сессия находится в статусе `down`:

```
angie-va# sho bfd pee
BFD Peers:
peer 192.168.0.3 vrf default
ID: 1753656330
Remote ID: 0
Active mode
Status: down
Downtime: 6 second(s)
Diagnostics: ok
Remote diagnostics: ok
Peer Type: dynamic
RTT min/avg/max: 0/0/0 usec
Local timers:
Detect-multiplier: 3
Receive interval: 300ms
Transmission interval: 300ms
Echo receive interval: 50ms
Echo transmission interval: disabled
Remote timers:
Detect-multiplier: 3
Receive interval: 1000ms
Transmission interval: 1000ms
Echo receive interval: disabled
```

Чтобы сессия поднялась, на соседе нужно либо настроить собственный статический маршрут с указанием адреса исходящего интерфейса в качестве next-hop, либо вручную создать статический пир, соответствующий системе балансировки (см. ниже).

4.2.6.6 Настройка независимого пира

Во всех приведенных выше случаях пир создавался динамически по требованию протокола динамической маршрутизации или в момент создания соответствующего статического маршрута. Ручное создание BFD-пира может потребоваться, например, в ситуации, когда необходимо поменять параметры работы какого-то одного соседа из группы автоматически обнаруженных.

Переход к созданию и настройке отдельного пира из режима конфигурирования протокола BFD:

```
angie-va# conf t
angie-va(config)# bfd
angie-va(config-bfd)# peer
A.B.C.D   IPv4 peer address
X:X::X:X  IPv6 peer address
angie-va(config-bfd)# peer
```

Некоторые настройки необходимо задать в момент создания пира (интерфейс, локальный адрес, multihop и vrf), остальные параметры можно будет изменить потом.

```
angie-va(config-bfd)# peer 192.168.0.3
<cr>
interface      Interface information
local-address  Configure local address
multihop       Configure multihop
vrf            Configure VRF
angie-va(config-bfd)# peer 192.168.0.3
angie-va(config-bfd-peer)#
detect-multiplier  Configure peer detection multiplier
echo               Configure peer echo intervals
echo-interval      Configure peer echo intervals
echo-mode          Configure echo mode
```

```
end                End current mode and change to enable mode
exit               Exit current mode and down to previous mode
find               Find CLI command matching a regular expression
list               Print command list
minimum-ttl        Expect packets with at least this TTL
no                 Negate a command or set its defaults
output             Direct vtysh output to file
passive-mode       Don't attempt to start sessions
profile            Use BFD profile settings
quit               Exit current mode and down to previous mode
receive-interval   Configure peer receive interval
shutdown           Disable BFD peer
transmit-interval  Configure peer transmit interval
```

После того, как с одной из сторон такой пир сконфигурирован, он будет находиться в статусе `down`, пока не будет создан симметричный пир с "противоположной" стороны.

4.2.6.7 Профиль

Чтобы создать новый профиль, отредактировать или удалить существующий профиль, необходимо перейти из режима глобальной конфигурации в режим настройки протокола BFD, а дальше уже либо удалять профиль, либо переходить в режим создания или настройки конкретного профиля.

```
angie-va(config)# bfd
angie-va(config-bfd)#
end      End current mode and change to enable mode
exit     Exit current mode and down to previous mode
find     Find CLI command matching a regular expression
list     Print command list
no       Negate a command or set its defaults
output   Direct vtysh output to file
peer     Configure peer
profile  BFD profile.
quit     Exit current mode and down to previous mode
angie-va(config-bfd)# profile
BFDPROF  BFD profile name.
test
angie-va(config-bfd)# no profile test
angie-va(config-bfd)# profile test_new
angie-va(config-bfd-profile)#
detect-multiplier  Configure peer detection multiplier
echo               Configure peer echo intervals
echo-interval      Configure peer echo interval
echo-mode          Configure echo mode
end                End current mode and change to enable mode
exit               Exit current mode and down to previous mode
find               Find CLI command matching a regular expression
list               Print command list
minimum-ttl        Expect packets with at least this TTL
no                 Negate a command or set its defaults
output             Direct vtysh output to file
passive-mode       Don't attempt to start sessions
quit               Exit current mode and down to previous mode
receive-interval   Configure peer receive interval
shutdown           Disable BFD peer
transmit-interval  Configure peer transmit interval
angie-va(config-bfd-profile)#
```

4.2.7 Настройка RHI

RHI (Route Health Injection) управляет анонсом адресов сервисов по протоколам динамической маршрутизации BGP и OSPF в зависимости от состояния апстримов балансировщика нагрузки. Пока апстрим доступен, Angie ADC анонсирует префикс адреса сервиса; когда апстрим становится недоступен, префикс отзывается и трафик сервиса уходит на другие узлы. Апстрим считается недоступным, если все его серверы не прошли проверки работоспособности (health probes).

4.2.7.1 Как это работает

Префикс адреса сервиса — это запись *списка префиксов*, привязанная к апстриму. Пока апстрим доступен, запись разрешает префикс (`permit`); когда апстрим недоступен, запись запрещает его (`deny`). Карта маршрутов, которая ссылается на этот список, пропускает префикс в BGP или OSPF только в первом случае.

Пока состояние апстрима неизвестно (например, имя апстрима указано с ошибкой или для него не настроены проверки), префикс не анонсируется.

После восстановления апстрима префикс возвращается в анонс в зависимости от политики возврата:

- `automatic` — автоматически;
- `manual` (по умолчанию) — префикс остается отозванным, пока его не вернут вручную (см. *Возврат отозванного префикса*). Так узел не начинает снова принимать трафик, пока администратор не проверит апстрим.

Для работы RHI необходимо:

1. Задать адрес сервиса на *интерфейсе lo* узла.
2. Настроить проверки работоспособности апстрима (см. *Настройка балансировщика нагрузки*).
3. Привязать префикс адреса сервиса к апстриму (см. *Привязка префиксов к апстримам*).
4. Настроить анонс префикса по BGP или OSPF через карту маршрутов, которая ссылается на список префиксов (см. *Анонс по BGP* и *Анонс по OSPF*).

4.2.7.2 Настройка балансировщика нагрузки

Конфигурация балансировщика нагрузки настраивается в веб-интерфейсе Angie ADC (см. *инструкцию*).

Для работы RHI необходимо настроить следующие параметры:

- *upstream_probe*;
- параметры для получения информации о состоянии балансировщика нагрузки.

Пример

Приведены только строки, добавленные в дефолтную конфигурацию.

```
### Часть конфигурации опущена для краткости
}
### Бэкенды
upstream myapp1 {
    zone myapp1 1m;
    server server1;
    server server2;
}
### Переменная для health probe
map $upstream_status $good {
    200     "1";
}
```

```
server {
### Часть конфигурации опущена для краткости
    location / {
        proxy_pass http://myapp1;
        # Апстрим-пробы
        upstream_probe myapp1_probe
            interval=1s
            test=$good
            essential
            mode=always;
    }
### Часть конфигурации опущена для краткости
}
}
```

4.2.7.3 Привязка префиксов к апстримам

В веб-интерфейсе

1. Откройте веб-интерфейс Angie ADC и перейдите в раздел `Управление трафиком` → `Конфигурация RHI`.

   Откроется окно настройки RHI.

2. Задайте префиксы. Для этого нажмите `Добавить` и укажите следующие параметры:

   - `VIP-адрес (CIDR)` — адрес сервиса в формате `X.X.X.X/mask`, например `2.2.2.2/32`. Значение должно быть уникальным в рамках одного префикс-листа.
   - `Приоритет` — номер записи в префикс-листе (`seq`), определяющий порядок обработки записей: запись с меньшим номером обрабатывается первой. Значение должно быть уникальным в рамках одного префикс-листа.
   - `Имя префикс-листа` — имя списка префиксов, на который ссылается карта маршрутов. Если списка с таким именем нет, он будет создан.
   - `Имя апстрима` — апстрим, от состояния которого зависит анонс префикса.

3. Установите флажок `Объявлять префиксы при восстановлении апстримов`, если хотите, чтобы Angie ADC автоматически возвращал префиксы в анонс при восстановлении работоспособности апстримов (политика `automatic`). Флажок задает политику сразу для всех префиксов на странице. Если флажок снят, отозванный префикс остается отозванным, пока его не вернут кнопкой `Вернуть`. По умолчанию флажок снят.

4. Нажмите `Сохранить`.

   Изменение передается в кластерную конфигурацию и применяется на узле.

Отозванный префикс отмечен на странице как `Отозван`.

Чтобы удалить префикс, нажмите значок удаления напротив него и сохраните изменения. Запись удаляется из списка префиксов, а опустевший список — целиком. Если на удаленный список еще ссылается карта маршрутов, измените или удалите эту карту (`no routing route-map <имя>`).

В CLI

Привязка к апстриму задается параметрами `upstream` и `recovery` команды *routing prefix-list* в режиме `configuration`:

```
$$ configuration
## routing prefix-list myapp1_pair seq 5 permit 2.2.2.2/32 upstream myapp1 recovery␣
↪manual
```

Без параметра `recovery` используется политика `manual`. Префиксы, привязанные в CLI, видны на странице `Конфигурация RHI`, и наоборот.

4.2.7.4 Анонс по BGP

В примере адрес сервиса `2.2.2.2/32` анонсируется eBGP-соседу `10.0.0.1` из AS 2:

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing prefix-list myapp1_pair seq 5 permit 2.2.2.2/32 upstream myapp1
## routing route-map myapp1_pair permit 10 match-prefix-list myapp1_pair
## routing bgp asn 1
## routing bgp neighbor 10.0.0.1 remote-as 2
## routing bgp redistribute connected route-map myapp1_pair
```

Проверка

Angie ADC должен увидеть свои объявления:

```
$$ show ip bgp
BGP table version is 14, local router ID is 2.2.2.2, vrf id 0
Default local pref 100, local AS 1
Status codes:  s suppressed, d damped, h history, u unsorted, * valid, > best, =␣
↪multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

    Network          Next Hop            Metric LocPrf Weight Path
*>  2.2.2.2/32       0.0.0.0                  0         32768 ?

Displayed 1 routes and 1 total paths
```

Соседний маршрутизатор должен увидеть объявления от Angie ADC:

```
abstract-router# sh ip bgp
BGP table version is 14, local router ID is 10.0.0.1, vrf id 0
Default local pref 100, local AS 2
Status codes:  s suppressed, d damped, h history, u unsorted, * valid, > best, =␣
↪multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

    Network          Next Hop            Metric LocPrf Weight Path
*>  2.2.2.2/32       10.21.20.6               0             0 1 ?

Displayed 1 routes and 1 total paths
```

Когда апстрим `myapp1` недоступен, префикс `2.2.2.2/32` пропадает из обеих таблиц.

4.2.7.5 Анонс по OSPF

В примере OSPF включен на интерфейсе `ens33` (адрес `192.168.0.20/24` задается в *сетевых настройках*):

```
$$ configuration
## set system interface lo ip address 2.2.2.2/32
## routing prefix-list myapp1_pair seq 5 permit 2.2.2.2/32 upstream myapp1
## routing route-map myapp1_pair permit 10 match-prefix-list myapp1_pair
## routing ospf 1
## routing ospf 1 router-id 192.168.0.20
## routing ospf 1 interface ens33 area 0
## routing ospf 1 redistribute connected route-map myapp1_pair
```

Проверка

Если серверы апстрима доступны, Angie ADC анонсирует внешнюю LSA для префикса:

```
$$ show ip ospf 1 database external self-originate
OSPF Instance: 1
       OSPF Router with ID (192.168.0.20)
                AS External Link States
  LS age: 28
  Options: 0x2  : *|-|-|-|-|-|E|-
  LS Flags: 0xb
  LS Type: AS-external-LSA
  Link State ID: 2.2.2.2 (External Network Number)
  Advertising Router: 192.168.0.20
  LS Seq Number: 80000001
  Checksum: 0x139b
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

Если серверы апстрима недоступны:

```
$$ show ip ospf 1 database external self-originate
OSPF Instance: 1
       OSPF Router with ID (192.168.0.20)
                AS External Link States
  LS age: 3600
  Options: 0x2  : *|-|-|-|-|-|E|-
  LS Flags: 0x8b
  LS Type: AS-external-LSA
  Link State ID: 2.2.2.2 (External Network Number)
  Advertising Router: 192.168.0.20
  LS Seq Number: 80000001
  Checksum: 0x139b
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

При отзыве префикса OSPF устанавливает для LSA значение `LS age`, равное `3600`, сообщая соседям, что LSA устарела и ее нужно перестать использовать. Через некоторое время LSA удаляется из LSDB.

4.2.7.6 Возврат отозванного префикса

При политике `manual` префикс, отозванный после отказа апстрима, остается отозванным и после восстановления апстрима. Отозванные префиксы выводит команда `routing show withdrawn` в режиме `configuration`:

```
## routing show withdrawn
prefix-list myapp1_pair seq 5 2.2.2.2/32 upstream myapp1
```

Чтобы вернуть префикс в анонс, нажмите `Вернуть` напротив него на странице `Конфигурация RHI` или выполните команду:

```
## no routing prefix-list myapp1_pair seq 5 withdrawn
```

Возврат не меняет конфигурацию: префикс снова анонсируется, пока апстрим доступен, и при следующем отказе отзывается снова.

4.2.8 Настройка ECMP

В этой статье рассматривается:

- ECMP-распределение трафика со стороны сетевого оборудования между несколькими узлами Angie ADC;
- распределение трафика самой системой балансировки Angie ADC между несколькими путями в сторону клиентов или серверов.

В конце также будет рассмотрена возможность UCMP-балансировки.

ECMP (Equal-Cost Multi-Path) – это механизм, который позволяет равномерно распределять трафик между несколькими путями, если они имеют одинаковую стоимость (метрику). В контексте Angie ADC это означает, что входящий трафик может приходить на разные узлы Angie ADC, а также сама система балансировки Angie ADC может отправлять трафик через разные пути с одинаковой стоимостью.

Такой подход может использоваться:

- Если необходимо распределять трафик в сторону серверов или клиентов между несколькими доступными путями.
- При горизонтальном масштабировании Angie ADC, когда трафик распределяется между несколькими узлами Angie ADC с помощью сетевого оборудования, а затем узлы Angie ADC распределяют пользовательские сессии между конечными серверами.

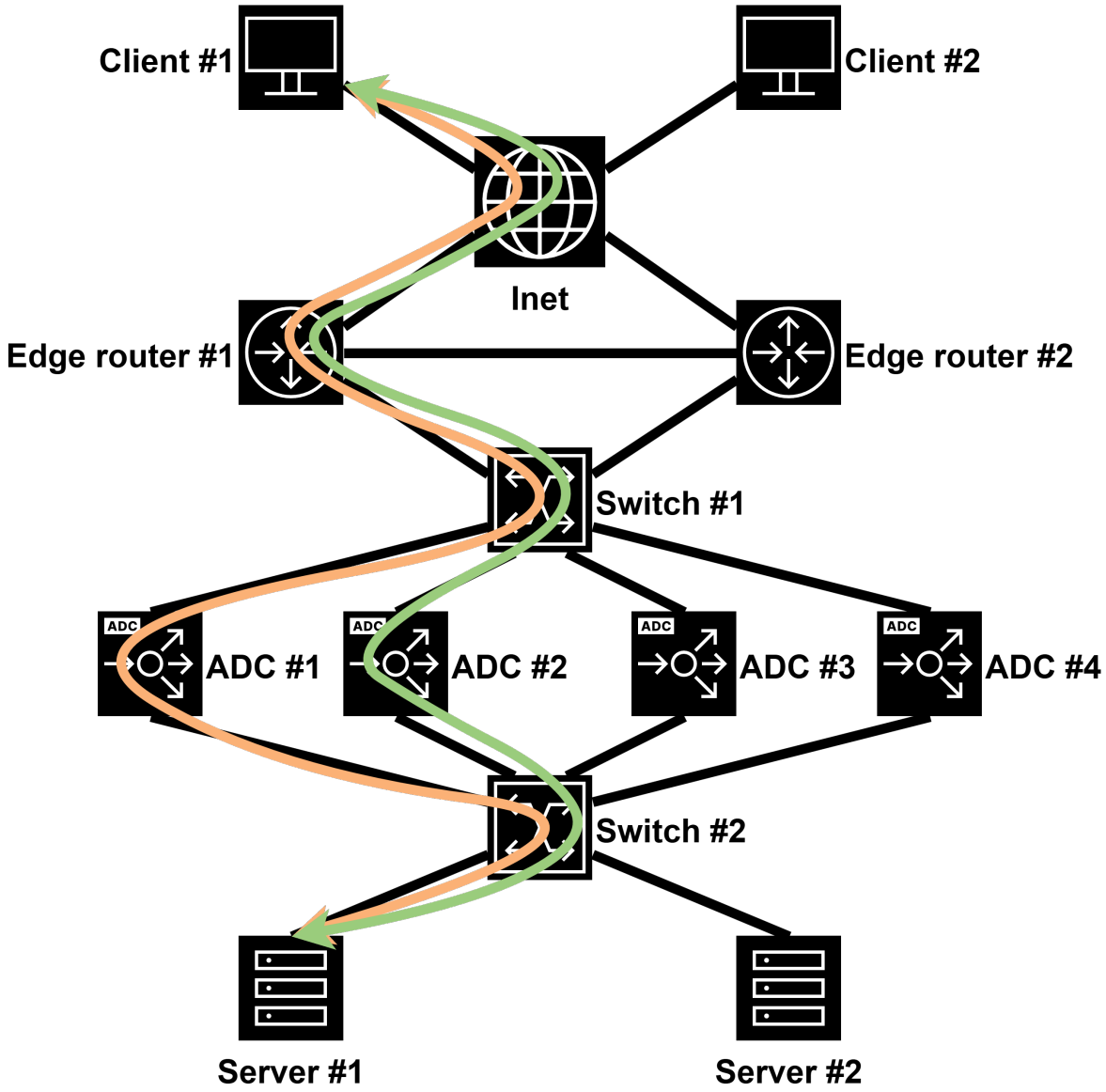
Angie ADC поддерживает ECMP-балансировку между 64 путями.

4.2.8.1 Распределение трафика между несколькими Angie ADC

Чтобы трафик успешно передавался в Angie ADC по нескольким путям с одинаковой стоимостью, узлы Angie ADC должны «видеть» всю сессию полностью. То есть, весь прямой трафик в рамках одной сессии (первый поток) должен попадать на одну систему балансировки. Обратный трафик также должен возвращаться на нее, благодаря использованию адресов или пулов SNAT.

Трафик второй сессии (второй поток) может распределиться на другую систему балансировки, но будет полностью обрабатываться в ней.

Пример:


Client #1
Client #2
Inet
Edge router #1
Edge router #2
Switch #1
ADC
ADC #1
ADC #2
ADC #3
ADC #4
Switch #2
Server #1
Server #2

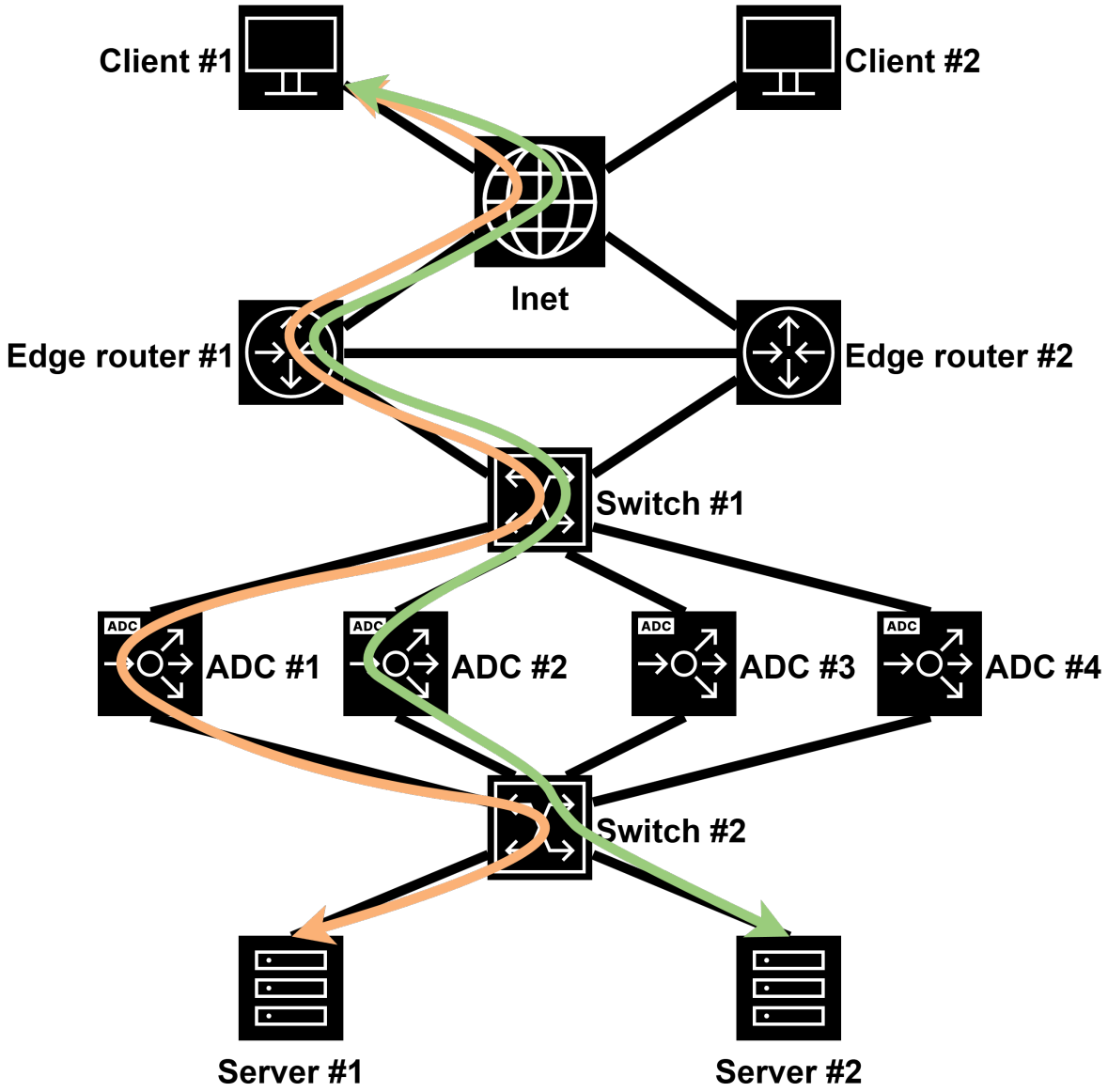


Рис. 1

Первая сессия показана оранжевой стрелкой, вторая – зеленой. Второй Angie ADC может выбрать тот же или другой бэкенд-сервер для обработки пользовательского запроса.

4.2.8.2 Внешнее хранилище sticky

Когда критичным является распределение всех сессий от одного клиента на один бэкенд-сервер, используется механизм sticky. Angie ADC запоминает, куда было отправлено первое соединение от клиента, и все последующие подключения отправляет на этот же сервер. Если вторая сессия обрабатывается другим Angie ADC, который не обладает информацией о sticky, то для sticky можно использовать внешнее хранилище информации. В качестве такого хранилища может выступать используемый или выделенный узел Angie ADC.

Алгоритм использования внешнего хранилища для sticky будет таким:

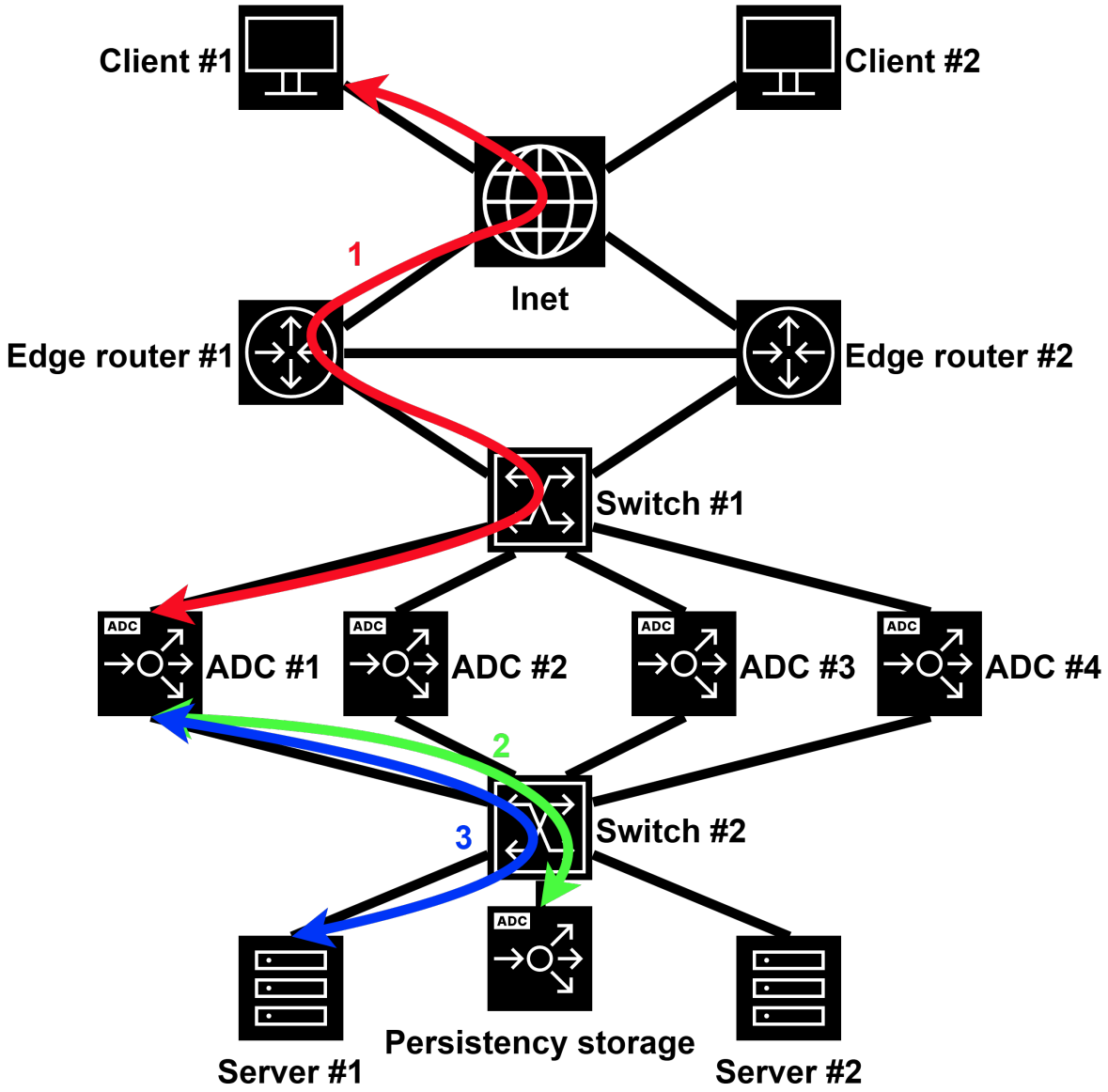
1. Пограничный маршрутизатор распределяет входящее подключение на один из узлов Angie ADC.
2. Получив пользовательский запрос, Angie ADC #1 выбирает сервер для перенаправления запроса (в соответствии с настроенным методом балансировки) и отправляет сообщение в хранилище sticky. Так как это первое подключение со стороны клиента, Angie ADC #1 сохраняет

sticky в хранилище и подтверждает правильность распределения.

3. Angie ADC #1 устанавливает вторую часть подключения (до бэкенд-сервера). Теперь пользовательское соединение полностью установлено и готово к работе.
4. Клиент устанавливает вторую сессию, которая попадает на Angie ADC #3.
5. Angie ADC #3 выбирает сервер для перенаправления запроса (в соответствии с настроенным методом балансировки) и отправляет сообщение в хранилище sticky. Если сервер, на который предлагается распределить нагрузку, совпадает с тем, который записан в хранилище, то хранилище подтверждает выбор системы балансировки. Если предложенный сервер не совпадает с записанным, то хранилище возвращает хэш-сумму «правильного» сервера.
6. Система балансировки Angie ADC #3 установит новую сессию в соответствии с ответом, полученным от хранилища.

Таким образом, клиент всегда будет устанавливать соединения с одним и тем же бэкенд-сервером.

Пример (стрелки пронумерованы в соответствии с шагами выше):



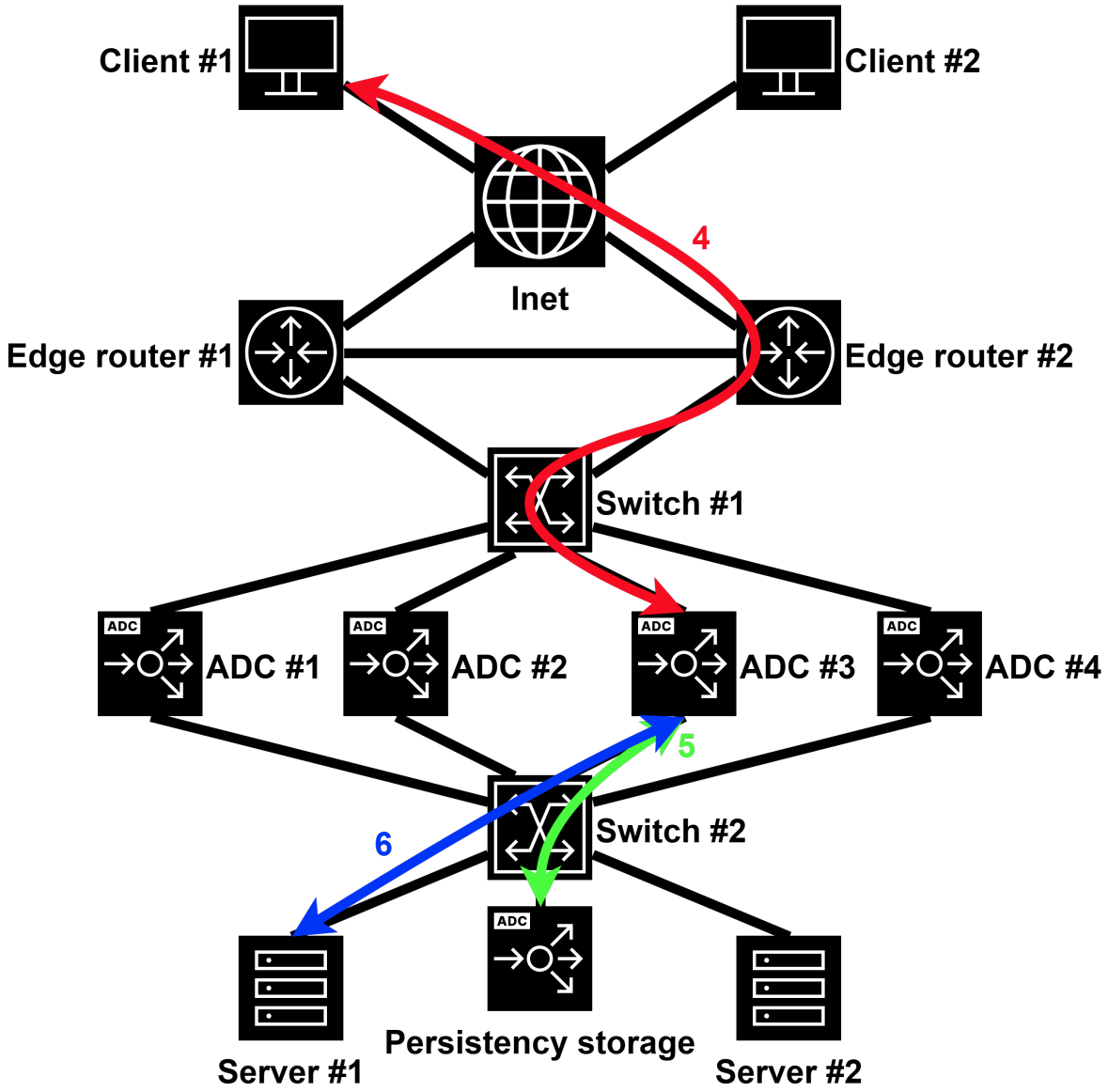


Рис. 2

4.2.8.3 Распределение трафика между несколькими маршрутизаторами

Ниже приведен пример небольшой корпоративной сети, где из соображений отказоустойчивости или для преодоления ограничений производительности граничных маршрутизаторов реализована схема с двумя независимыми каналами в интернет, которые терминируются на двух независимых маршрутизаторах.

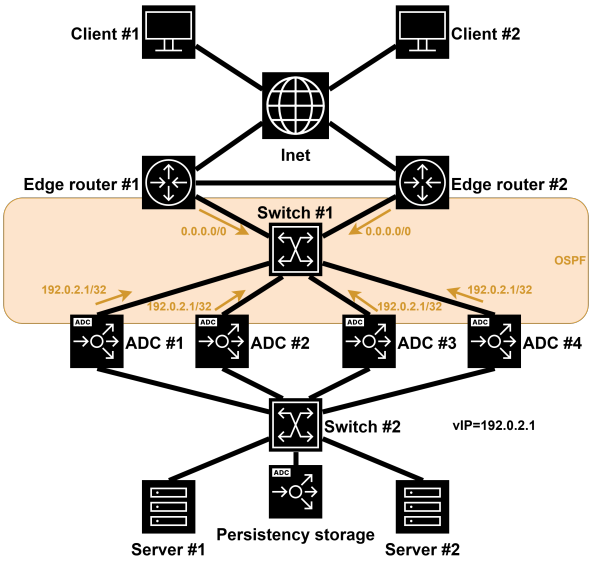


Рис. 3

Каждая из систем балансировки Angie ADC получает маршрут по умолчанию от каждого из граничных маршрутизаторов. Если параметры этих маршрутов одинаковы (для OSPF это типы маршрутов и метрики), то Angie ADC будет равномерно распределять трафик между граничными маршрутизаторами, то есть будет выполнять ECMP-балансировку.

Ниже приведен пример двух маршрутов по умолчанию, полученных с помощью протокола OSPF:

```
$$ show ip route ospf
Codes: K - kernel route, C - connected, L - local, S - static,
R - RIP, O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, F - PBR,
f - OpenFabric, t - Table-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure
O[1]>* 0.0.0.0/0 [110/1] via 192.168.0.201, ens33, weight 1, 00:00:32
* via 192.168.0.202, ens33, weight 1, 00:00:32
```

В операционной системе этот же маршрут виден так:

```
[root@angie-adc1 angie-adc1]# ip r
default nhid 23 proto ospf metric 20
nexthop via 192.168.0.202 dev ens33 weight 1
nexthop via 192.168.0.201 dev ens33 weight 1
```

4.2.8.4 UCMP-балансировка

Некоторые протоколы динамической маршрутизации (например, EIGRP, BGP, IS-IS) поддерживают балансировку по путям с разной стоимостью – UCMP (Unequal Cost Multi-Path). В примере ниже приведен сценарий, реализованный с помощью BGP с использованием Extended Community Bandwidth:

```
angie-adc1# sho ip bgp
BGP table version is 23, local router ID is 192.168.0.153, vrf id 0
Default local pref 100, local AS 1
Status codes: s suppressed, d damped, h history, u unsorted, * valid, > best, =␣
↪multipath,
i internal, r RIB-failure, S Stale, R Removed
```

```
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network Next Hop Metric LocPrf Weight Path
*> 192.0.2.1/32 192.168.0.201 0 0 65002 i
*=   192.168.0.202 0 0 65002 i
Displayed 1 routes and 2 total paths
angie-adc1# sho ip bg 192.0.2.1/32
BGP routing table entry for 192.0.2.1/32, version 23
Paths: (2 available, best #1, table default)
Advertised to non peer-group peers:
192.168.0.201 192.168.0.201
2
192.168.0.202 from 192.168.0.202 (192.168.0.202)
Origin IGP, metric 0, valid, external, multipath, bestpath-from-AS 2, best (Older␣
↪Path)
Extended Community: LB:1:12500000 (100.000 Mbps)
Last update: Fri Feb 28 17:59:16 2025
2
192.168.0.201 from 192.168.0.201 (192.168.0.201)
Origin IGP, metric 0, valid, external, multipath
Extended Community: LB:1:6250000 (50.000 Mbps)
Last update: Fri Feb 28 17:59:16 2025
```

Angie ADC не поддерживает UCMP-балансировку на уровне передачи данных (data-plane), только ECMP. Поэтому возможны два исхода:

- маршрут будет установлен в RIB с балансировкой ECMP;
- маршрут не будет установлен в RIB, что зависит от других настроек протокола BGP.

```
angie-adc1# sho ip ro
Codes: K - kernel route, C - connected, L - local, S - static,
R - RIP, O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, F - PBR,
f - OpenFabric, t - Table-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure
K>* 0.0.0.0/0 [0/100] via 192.168.0.2, ens33, src 192.168.0.153, 01:30:36
B>* 192.0.2.1/32 [20/0] via 192.168.0.201, ens33, weight 1, 00:42:48
*                       via 192.168.0.202, ens33, weight 1, 00:42:48
C>* 192.168.0.0/24 is directly connected, ens33, 01:30:36
L>* 192.168.0.153/32 is directly connected, ens33, 01:30:36
```

Если маршрут устанавливается в RIB, то со стороны операционной системы таблица маршрутизации будет выглядеть так:

```
[root@angie-adc1 etc]# ip r
default via 192.168.0.2 dev ens33 proto dhcp src 192.168.0.153 metric 100
192.0.2.1 nhid 37 proto bgp metric 20
nexthop via 192.168.0.202 dev ens33 weight 1
nexthop via 192.168.0.201 dev ens33 weight 1
192.168.0.0/24 dev ens33 proto kernel scope link src 192.168.0.153 metric 100
```

Если UCMP поддерживает сетевая инфраструктура, такую схему распределения трафика можно использовать на ее стороне. UCMP-балансировка в таком случае может быть полезной, например, когда есть значительный перекос в мощностях систем балансировки, участвующих в обработке трафика:

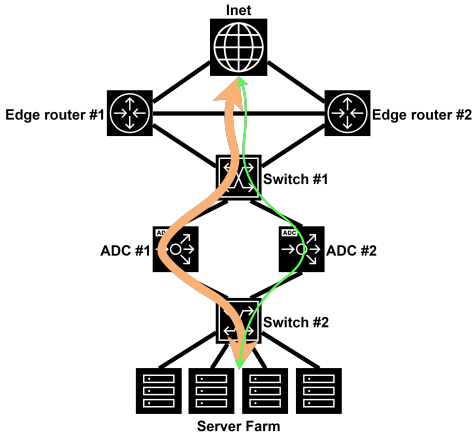

Inet
Edge router #1
Edge router #2
Switch #1
ADC #1
ADC #2
Switch #2
Server Farm

Рис. 4

ГЛАВА 5

Мониторинг и диагностика

Здесь описываются:

- Просмотр статистики балансировщика и системных метрик, мониторинг в Console Light, SNMP и экспорт метрик — см. раздел *Метрики и статистика*.
- Мониторинг доступности узлов и бэкендов кластера — см. раздел *Доступность*.
- Диагностика, сбор логов и обращение в техническую поддержку — см. раздел *Диагностика и логирование*.

5.1 Метрики и статистика

Angie ADC предоставляет широкий спектр возможностей мониторинга:

- статистика балансировщика нагрузки *в веб-интерфейсе*;
- статистика глобальной балансировки (GSLB) *в веб-интерфейсе*;
- мониторинг балансировщика нагрузки *в веб-консоли Console Light* в режиме реального времени;
- системные метрики Angie ADC *в веб-интерфейсе*.

Дополнительно доступны:

- *получение метрик по протоколу SNMP*;
- *экспорт метрик во внешний Prometheus*;
- модуль Prometheus;
- модуль Metric;
- метрики балансировщика нагрузки в API.

5.1.1 Статистика балансировщика нагрузки

Angie ADC предоставляет доступ к детализированным графикам со статистикой по балансировщику нагрузки. Просмотреть статистику можно в разделе `Мониторинг` → `Балансировщик`.

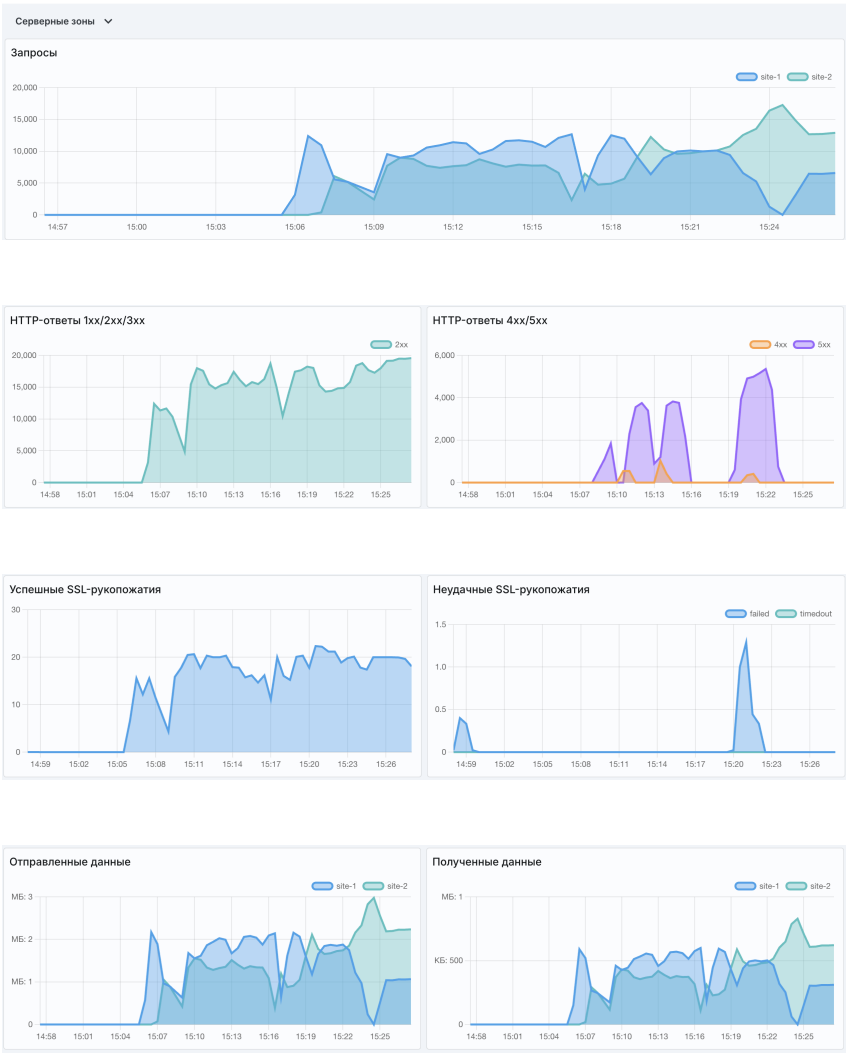
> **Примечание**
>
> Пользователь с ролью `Оператор` может просматривать только метрики тех зон, которые были выделены для него администратором *при предоставлении доступов* к конфигурации балансировщика нагрузки.

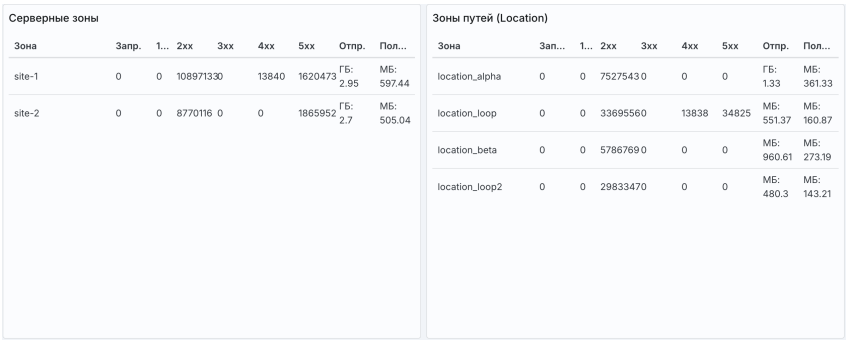
Кнопка `Перейти к интерактивному мониторингу` позволяет перейти в консоль Console Light и просмотреть ключевые показатели нагрузки и производительности сервера в реальном времени. Подробнее см. *Мониторинг в Console Light*. Кнопка доступна только для пользователей с ролями `Администратор` и `Супервизор`.

В раскрывающемся списке `За 30 минут` в верхней части экрана можно выбрать временной период для отображения статистики. Доступные периоды: 30 минут, 3 часа, 6 часов, 12 часов, 24 часа, 48 часов, неделя, две недели.

5.1.1.1 Виджет "Серверные зоны"

Виджет `Серверные зоны` отображает статистику по серверным зонам разделяемой памяти:

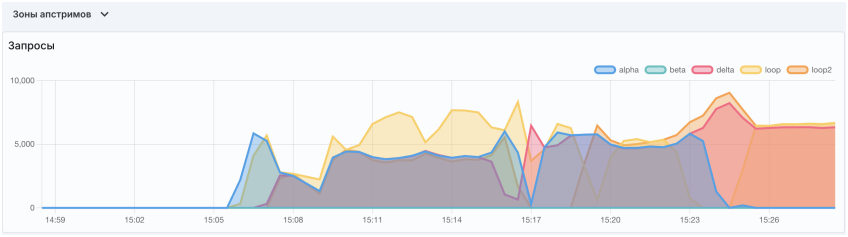


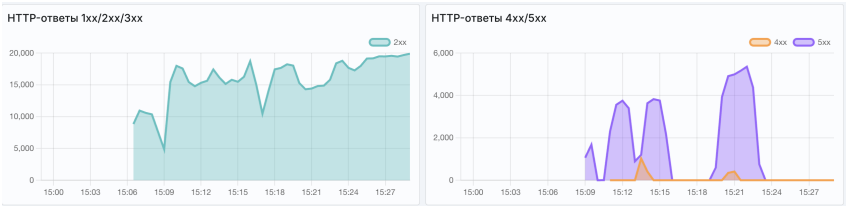


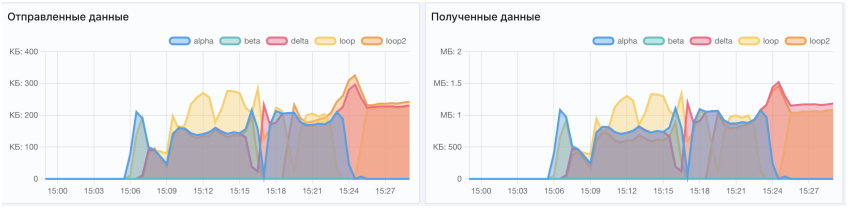
`Запросы`	График числа запросов с разделением по отдельным серверам
`HTTP-ответы 1xx/ 2xx/3xx`	Графики числа HTTP-ответов с определенными кодами состояния с разделением по группам кодов (1xx, 2xx, 3xx)
`HTTP-ответы 4xx/5xx`	Графики числа HTTP-ответов с определенными кодами состояния с разделением по группам кодов (4xx, 5xx)
`Отправленные данные`	График объема отправленных данных с разделением по отдельным серверам
`Полученные данные`	График объема полученных данных с разделением по отдельным серверам
`Успешные SSL-рукопожатия`	График числа успешных SSL-рукопожатий с разделением по отдельным серверам
`Неудачные SSL-рукопожатия`	График числа неудачных SSL-рукопожатий с разделением по отдельным серверам
`Серверные зоны`	Таблица серверных зон со статистикой запросов, ответов и данных с разделением по отдельным зонам
`Зоны путей (Location)`	Таблица зон location со статистикой запросов, ответов и данных с разделением по отдельным location

5.1.1.2 Виджет "Зоны апстримов"

Виджет `Зоны апстримов` отображает статистику по зонам разделяемой памяти для апстримов:







`Запросы`	График числа запросов с разделением по отдельным серверам
`HTTP-ответы 1xx/2xx/3xx`	Графики числа HTTP-ответов с определенными кодами состояния с разделением по группам кодов (1xx, 2xx, 3xx)
`HTTP-ответы 4xx/5xx`	Графики числа HTTP-ответов с определенными кодами состояния с разделением по группам кодов (4xx, 5xx)
`Отправленные данные`	График объема отправленных данных с разделением по отдельным серверам
`Полученные данные`	График объема полученных данных с разделением по отдельным серверам

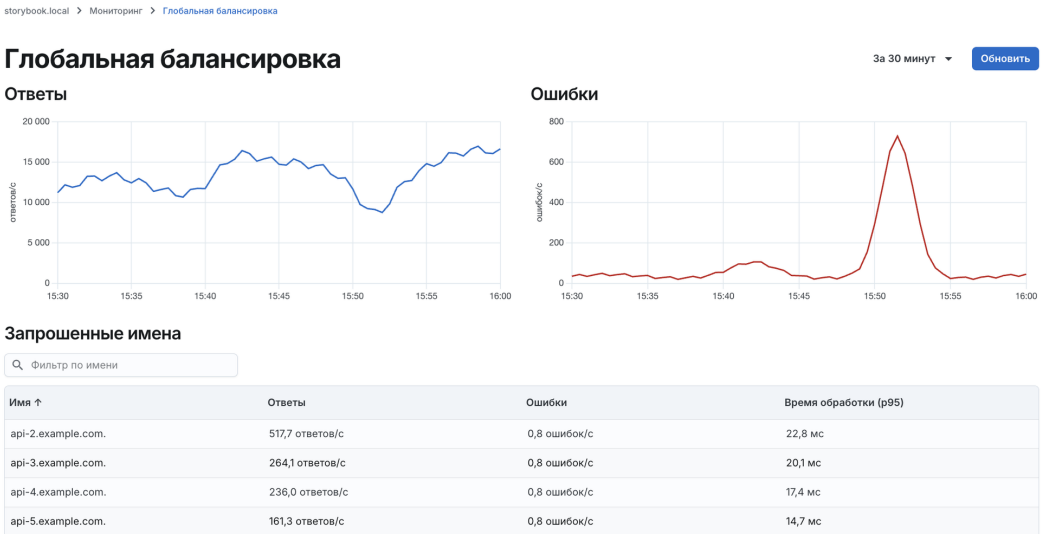
5.1.2 Статистика глобальной балансировки

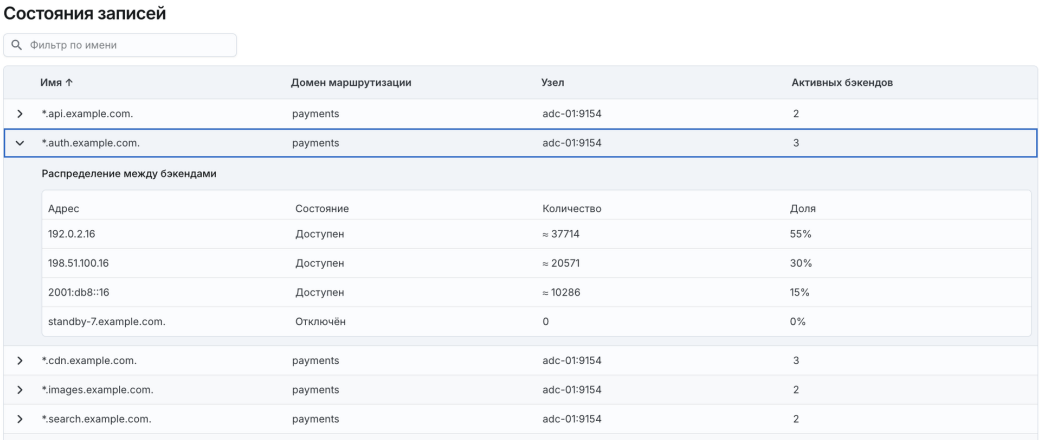
Angie ADC предоставляет статистику по работе *глобальной балансировки* (GSLB): сколько DNS-ответов отправляет GSLB, какие имена запрашивают клиенты, в каком состоянии находятся GSLB-записи и как выборы распределяются между бэкендами. Просмотреть статистику можно в разделе `Мониторинг` → `Глобальная балансировка`.

> **Примечание**
>
> Раздел доступен только пользователям с ролью `Администратор`.

Статистика строится по метрикам GSLB, которые собирает Prometheus.

В раскрывающемся списке `За 30 минут` в верхней части экрана можно выбрать временной период для отображения статистики. Выбранный период применяется ко всем графикам и таблицам на экране. Данные обновляются автоматически каждые 30 секунд. Также можно обновить данные вручную по кнопке `Обновить`.





В верхней части экрана отображаются графики:

`Ответы`	График числа DNS-ответов, отправленных GSLB в секунду, по всем запрошенным именам. Успешно отправленный ответ может не содержать DNS-записей.
`Ошибки`	График числа ошибок в секунду, возникших при отправке DNS-ответа клиенту, по всем запрошенным именам.

5.1.2.1 Запрошенные имена

Таблица `Запрошенные имена` содержит DNS-имена, которые клиенты фактически запрашивали за выбранный период. Для wildcard-записи в таблице отображаются конкретные запрошенные имена: например, запрос `news.example.com.` к записи `*.example.com.` отображается как `news.example.com.`.

`Имя`	Запрошенное DNS-имя
`Ответы`	Среднее число DNS-ответов на запросы этого имени в секунду за выбранный период
`Ошибки`	Среднее число ошибок отправки DNS-ответа на запросы этого имени в секунду за выбранный период
`Время обработки (p95)`	95-й процентиль времени обработки запроса этого имени (в миллисекундах) для запросов, в которых бэкенд был успешно выбран

Таблицу можно отсортировать по любому столбцу.

5.1.2.2 Состояния записей

Таблица `Состояния записей` позволяет просмотреть GSLB-записи, для которых в Prometheus есть метрики. Таблицу можно отсортировать по имени записи.

`Имя`	Имя GSLB-записи
Домен маршрутизации	*Домен маршрутизации*, в котором работает GSLB. Столбец отображается, если GSLB работает в отдельном домене маршрутизации.
`Узел`	Узел Angie ADC, с которого получены метрики записи. Столбец отображается, если метрики получены более чем с одного узла.
`Активных бэкендов`	Число доступных бэкендов записи

> **Примечание**
>
> Метрики удаленной записи могут храниться в Prometheus некоторое время после ее удаления, поэтому запись может отображаться в таблице, даже если ее уже нет в текущей конфигурации GSLB.

Нажав на строку записи, можно просмотреть детальную информацию о бэкендах этой записи.

`Адрес`	Адрес бэкенда
`Состояние`	Состояние бэкенда: `Доступен`, `Недоступен` или `Отключён`
`Количество`	Приблизительное число выборов этого бэкенда за выбранный период
`Доля`	Доля выборов этого бэкенда среди выборов всех бэкендов записи за выбранный период

Количество выборов рассчитывается по данным Prometheus приблизительно, поэтому отображается со знаком приблизительного равенства. Если за выбранный период бэкенды записи не выбирались, вместо таблицы отображается сообщение `За выбранный период учтённых выборов нет`.

5.1.3 Мониторинг состояния системы

Просмотреть информацию о состоянии системы можно в веб-интерфейсе (`Мониторинг` → `Система`).

Системные метрики Angie ADC позволяют отслеживать состояние системы на разных уровнях:

- на уровне ОС (процессор, память, сеть);
- на уровне оборудования (только для аппаратного балансировщика Angie ADC: показания датчиков напряжения, температуры и пр.);
- на уровне хранения (информация о накопителях и их диагностика).

> **Примечание**
>
> На каждом узле Angie ADC отображаются только метрики этого узла.

Экран мониторинга отображает метрики системы и детализированные графики со статистикой за выбранный временной интервал.

В раскрывающемся списке `За 30 минут` в верхней части экрана вы можете изменить временной интервал для отображения статистики. Доступные временные интервалы: 30 минут, 3 часа, 6 часов, 12 часов, 24 часа, 48 часов, неделя, две недели.

5.1.3.1 Сводная инфографика

В верхней части экрана отображается сводная информация о состоянии системы.

`RAM (free)`	Объем свободной оперативной памяти устройства (ГБ)
`ROM (free)`	Объем свободной постоянной памяти устройства (ГБ)
`Fan (avg.)`	Скорость вращения вентиляторов: среднее значение в оборотах в минуту (RPM) по всем вентиляторам устройства
`Temp. (avg.)`	Средняя температура по всем датчикам устройства (по Цельсию)
`Voltage`	Текущее напряжение блоков питания

5.1.3.2 Центральный процессор

`Uptime`	Время непрерывной работы системы с момента последнего запуска.
`CPU (core)`	Количество ядер процессора.
`Load Avg.`	Усредненная загрузка системы за 1 минуту / 5 минут / 15 минут. Интерпретируется относительно числа ядер, например, на сервере с 4 ядрами значение 2.00 означает, что система загружена на 50%.
`CPU (load)` (график)	График использования процессора в процентах за выбранный временной интервал.
`Load Avg.` (график)	График усредненной загрузки системы за 1 минуту / 5 минут / 15 минут за выбранный временной интервал. Интерпретируется относительно числа ядер, например, на сервере с 4 ядрами значение 2.00 означает, что система загружена на 50%.

5.1.3.3 Обработка данных

`Received`	Среднее количество данных, полученных в секунду (КБ/с)
`Transmitted`	Среднее количество данных, переданных в секунду (КБ/с)
`Collisions (avg.)`	Среднее количество коллизий в сети
`Input Packet Errors (avg.)`	Среднее количество ошибок входящих пакетов
`Output Packet Errors (avg.)`	Среднее количество ошибок исходящих пакетов
`Received` (график)	График среднего количества данных, полученных в секунду, за выбранный временной интервал с распределением по интерфейсам
`Transmitted` (график)	График среднего количества данных, переданных в секунду, за выбранный временной интервал с распределением по интерфейсам

5.1.3.4 Сетевые интерфейсы

Таблица `Interfaces` отображает список подключенных интерфейсов.

`Interface`	Имя сетевого интерфейса
`Adminstate`	Состояние сетевого интерфейса, заданное администратором (`up` или `down`)
`Operstate`	Фактическое состояние сетевого интерфейса на данный момент (`up` или `down`)
`Collisions, %`	Процент коллизий за выбранный временной интервал
`Input Packet Errors, %`	Процентная доля принятых пакетов, в которых содержатся ошибки, за выбранный временной интервал
`Output Packet Errors, %`	Процентная доля переданных пакетов, в которых содержатся ошибки, за выбранный временной интервал

5.1.3.5 ОЗУ

`Total`	Объем оперативной памяти, установленной на сервере (ГБ)
`Available`	Объем свободной оперативной памяти (ГБ)
`Used`	Объем используемой оперативной памяти (ГБ)
`ECC correctable errors`	Ошибки памяти, которые были обнаружены и автоматически исправлены (шт.)
`ECC uncorrectable errors`	Обнаруженные ошибки памяти, которые не удалось исправить (шт.)
`RAM (used)`	График использования оперативной памяти в процентах за выбранный временной интервал

5.1.3.6 Файловая система

Круговая диаграмма `Review file system` отображает заполнение файловой системы в процентах (`Used` — использованное пространство, `Free` — свободное пространство).

Таблица `File system` содержит список смонтированных файловых систем и их параметры.

`filesystem`	Имя файловой системы
`type`	Тип файловой системы
`size`	Общий размер файловой системы
`used`	Объем использованного пространства
`avail`	Объем свободного пространства
`use, %`	Процент использования файловой системы
`mountpoint`	Точка монтирования файловой системы

5.1.3.7 Накопители (ROM)

Таблица `ROM (devices)` отображает состояние накопителей.

`smartctl_status`	Состояние накопителя по данным SMART (Self-Monitoring, Analysis and Reporting Technology)
`power_on`	Общее время работы с момента включения
`temp`	Текущая температура
`size`	Объем накопителя
`device`	Имя устройства
`interface`	Тип интерфейса подключения
`model_name`	Модель устройства
`serial_number`	Серийный номер

5.1.3.8 S.M.A.R.T. атрибуты диска

Таблица `Reallocated_Sector_Ct` отображает количество переназначенных (перемещенных в резервную область) секторов диска:

`device`	Имя устройства
`raw`	Необработанное значение атрибута SMART
`thresh`	Пороговое значение, при достижении которого состояние атрибута считается критическим
`value`	Нормализованное текущее значение атрибута
`worst`	Наихудшее нормализованное значение атрибута за выбранный временной интервал

Таблица `Current_Pending_Sector` отображает количество секторов, которые считаются нестабильными и ожидают переназначения:

`device`	Имя устройства
`raw`	Необработанное значение атрибута SMART
`thresh`	Пороговое значение, при достижении которого состояние атрибута считается критическим
`value`	Нормализованное текущее значение атрибута
`worst`	Наихудшее нормализованное значение атрибута за выбранный временной интервал

5.1.3.9 Датчики

Таблица `IPMI (temperature)` отображает список датчиков с температурами. Данные получены через интерфейс IPMI (Intelligent Platform Management Interface):

`Sensor`	Идентификатор датчика температуры
`Temp.`	Текущее значение температуры

Таблица `IPMI (fan)` отображает информацию о вентиляторах. Данные получены через интерфейс IPMI (Intelligent Platform Management Interface):

`Sensor`	Идентификатор датчика вентилятора
`RPM`	Текущая скорость вращения вентилятора в оборотах в минуту (RPM)

Таблица `IPMI (voltage)` отображает параметры напряжения. Данные получены через интерфейс IPMI (Intelligent Platform Management Interface):

`Sensor`	Идентификатор датчика напряжения
`Voltage`	Текущее значение напряжения

Таблица `IPMI (power state)` отображает состояние питания устройств. Данные получены через интерфейс IPMI (Intelligent Platform Management Interface):

`Sensor`	Идентификатор датчика питания
`State`	Текущее состояние питания устройства (`0` — выключено, `1` — включено).

Таблица `IPMI (sensor state)` отображает состояние всех остальных отслеживаемых датчиков, помимо перечисленных выше, в зависимости от типа оборудования. Данные получены через интерфейс IPMI (Intelligent Platform Management Interface):

`Sensor`	Идентификатор датчика
`State`	Текущее значение датчика (`0` или `1`).

5.1.4 Мониторинг в Console Light

Console Light — это консоль для мониторинга активности в реальном времени, отображающая ключевые показатели нагрузки и производительности сервера. Консоль основана на возможностях API-интерфейса Angie ADC; данные мониторинга активности генерируются в реальном времени.

Пример развернутой и настроенной консоли: https://console.angie.software/

При использовании в составе продукта Angie ADC консоль Console Light устанавливается и настраивается автоматически.

5.1.4.1 Переход в Console Light

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Мониторинг` → `Балансировщик`.

   Откроется экран со статистикой для этого балансировщика.

2. В верхней части экрана нажмите кнопку `Перейти к интерактивному мониторингу`.

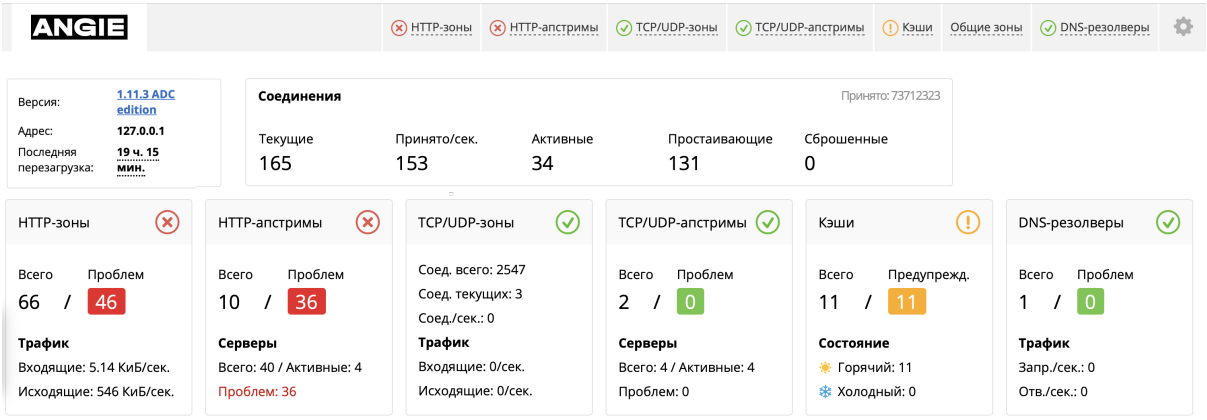
   Откроется облегченная консоль Console Light с данными мониторинга активности в реальном времени для этого балансировщика.

5.1.4.2 Интерфейс

Console Light представляет собой единый экран с набором вкладок, каждая из которых содержит ряд виджетов с данными мониторинга.

> **Совет**
>
> В разделах ниже описания элементов интерфейса даны в порядке слева направо.

5.1.4.3 Вкладка "Angie"



Это основная вкладка, где в сводном виде отображаются основные показатели мониторинга Angie ADC, сведенные на основе данных из нескольких разделов API.

> **Примечание**
>
> Виджеты со статистикой отображаются, если настроены соответствующие блоки в *конфигурации балансировщика нагрузки*.

Виджет "<версия>"

Здесь выводится номер версии Angie ADC, а также адрес сервера и время последней перезагрузки конфигурации.

Виджет "Соединения"

Здесь представлена основная статистика серверных соединений, формируемая на основе раздела API `/status/connections/`:

`Текущие`	Текущее количество соединений
`Принято/сек.`	Число принимаемых за секунду соединений
`Активные`	Число активных соединений
`Простаивающие`	Число соединений в состоянии ожидания
`Сброшенные`	Количество сброшенных соединений

Также доступно:

`Принято`	Общее число соединений, принятых с последней перезагрузки сервера

Виджет "HTTP-зоны"

Предупреждение

Требует задать директиву adc__status_zone в контексте `server` или `location`.

Здесь представлена статистика зон разделяемой памяти контекста `http`, формируемая на основе раздела API `/status/http/server_zones/`:

`Всего`	Общее количество зон
`Проблем`	Количество зон с какими-либо проблемами
`Трафик`	Скорость входящего и исходящего трафика в байтах в секунду

Виджет "HTTP-апстримы"

Предупреждение

Требует задать директиву adc__u_zone в блоке adc__u_upstream в контексте `http`.

Здесь представлена статистика апстримов контекста `http`, формируемая на основе раздела API `/status/http/upstreams/`:

`Всего`	Общее количество апстримов
`Проблем`	Количество апстримов с какими-либо проблемами
`Серверы`	Статистика серверов с разделением по состоянию

Виджет "TCP/UDP-зоны"

Предупреждение

Требует задать следующие директивы:

- `status_zone` в контексте server или stream;
- `limit_conn` в контексте server или stream;
- adc__limit_conn_zone в контексте `stream`.

Пример:

```
stream {

    # ...
    limit_conn_zone $connection zone=limit-conn-stream:10m;

    server {

        # ...
        limit_conn limit-conn-stream 1;
        status_zone foo;
    }
}
```

Здесь представлена статистика зон разделяемой памяти контекста `stream`, формируемая на основе раздела API `/status/stream/server_zones/`:

`Соед. всего`	Общее количество клиентских соединений
`Соед. текущих`	Текущее количество клиентских соединений
`Соед./сек.`	Количество обрабатываемых в секунду соединений

Виджет "TCP/UDP-апстримы"

Предупреждение

Требует задать директиву adc__s_u_zone в блоке adc__s_u_upstream в контексте `stream`.

Здесь представлена статистика апстримов контекста `stream`, формируемая на основе раздела API `/status/stream/upstreams/`:

`Всего`	Общее количество апстримов
`Проблем`	Количество апстримов с какими-либо проблемами
`Серверы`	Статистика серверов с разделением по состоянию

Виджет "Кэши"

Предупреждение

Требует задать зону кэша директивой adc__proxy_cache_path, adc__fastcgi_cache_path, adc__scgi_cache_path или adc__uwsgi_cache_path.

Здесь представлена статистика зон кэша контекста `http`, формируемая на основе раздела API `/status/http/caches/`:

`Всего`	Общее количество зон кэша
`Проблем`	Количество проблемных зон, причем каждый проблемный шард зоны с шардингом учитывается отдельно; если таких нет, но есть зоны с предупреждениями, вместо этой метки выводится `Предупрежд.` и число зон с предупреждениями
`Состояние`	Количество горячих (метаданные загружены) и холодных (метаданные загружаются в память) зон

Зона кэша получает предупреждение, если:

- ее `Коэффициент попадания` на вкладке "Кэши", вычисляемый за временное окно из виджета "Настройки", ниже 30% (у зоны без ответов за это окно он равен 0%);
- ее объем на диске превышает `max_size` не более чем на 5%.

Если объем зоны на диске превышает `max_size` более чем на 5%, зона считается проблемной. Для зоны с шардингом эти проверки объема выполняются для каждого шарда отдельно, а шард с превышением не более чем на 5% дает всей зоне предупреждение.

Виджет "DNS-резолверы"

Предупреждение

Требует задать параметр `status_zone` в директиве `resolver` (HTTP, Stream или Mail).

Здесь представлена статистика DNS-резолверов, формируемая на основе раздела API `/status/resolvers/`:

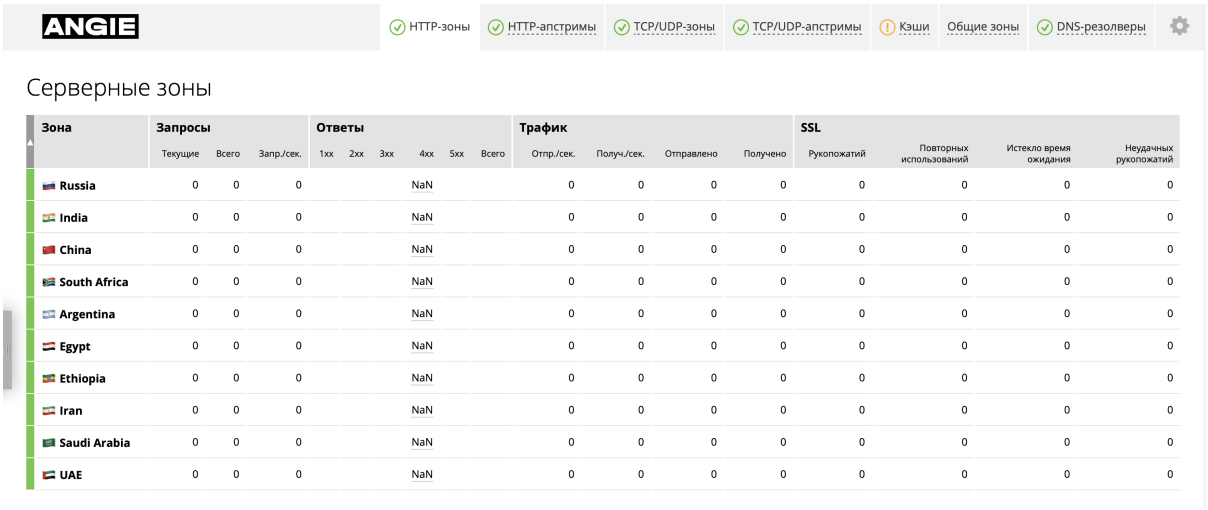
`Всего`	Общее количество зон резолверов
`Проблем`	Количество зон, в которых с момента предыдущего обновления данных число ответов, отличных от `Успешные` (включая тайм-ауты), превысило порог ошибок DNS из виджета "Настройки"; порог задается в процентах от числа запросов зоны за тот же интервал
`Трафик`	Число запросов (`Запр./сек.`) и полученных ответов (`Отв./сек.`, без тайм-аутов) в секунду по всем зонам

5.1.4.4 Вкладка "HTTP-зоны"

Предупреждение

Требует задать директиву adc__status_zone в контексте `server` или `location`.

Раздел "Серверные зоны"

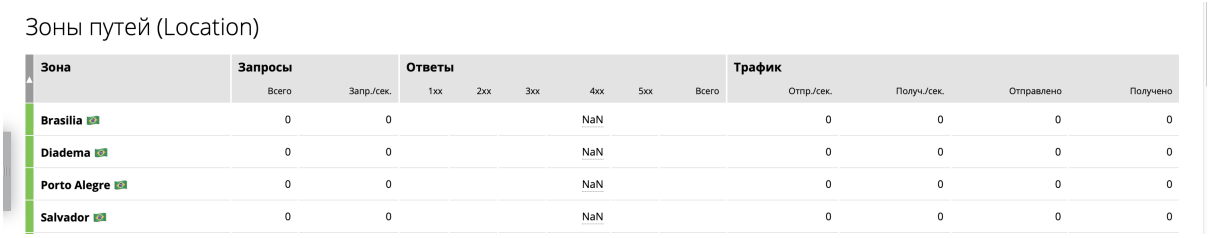


Зона	Запросы			Ответы						Трафик				SSL			
	Текущие	Всего	Запр./сек.	1xx	2xx	3xx	4xx	5xx	Всего	Отпр./сек.	Получ./сек.	Отправлено	Получено	Рукопожатий	Повторных использований	Истекло время ожидания	Неудачных рукопожатий
Russia	0	0	0				NaN			0	0	0	0	0	0	0	0
India	0	0	0				NaN			0	0	0	0	0	0	0	0
China	0	0	0				NaN			0	0	0	0	0	0	0	0
South Africa	0	0	0				NaN			0	0	0	0	0	0	0	0
Argentina	0	0	0				NaN			0	0	0	0	0	0	0	0
Egypt	0	0	0				NaN			0	0	0	0	0	0	0	0
Ethiopia	0	0	0				NaN			0	0	0	0	0	0	0	0
Iran	0	0	0				NaN			0	0	0	0	0	0	0	0
Saudi Arabia	0	0	0				NaN			0	0	0	0	0	0	0	0
UAE	0	0	0				NaN			0	0	0	0	0	0	0	0

Здесь в сводном виде отображается статистика мониторинга зон разделяемой памяти для контекста `server` в `http`, формируемая на основе раздела API `/status/http/server_zones/`. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны **Совет** Щелкните стрелку рядом с пунктом `Зона`, чтобы отсортировать зоны по алфавиту или порядку в конфигурации.
`Запросы`	Общее количество запросов, а также число запросов в секунду
`Ответы`	Количество ответов с разбиением по кодам статуса, а также их общее количество
`Трафик`	Скорость исходящего и входящего трафика в байтах в секунду, а также общие объемы исходящего и входящего трафика в байтах
`SSL`	Суммарные показатели количества: успешных SSL-рукопожатий; повторных использований SSL-сессий; SSL-рукопожатий с истекшим таймаутом; неуспешных SSL-рукопожатий

Раздел "Зоны путей (Location)"


Зоны путей (Location)

Зона	Запросы		Ответы						Трафик			
	Всего	Запр./сек.	1xx	2xx	3xx	4xx	5xx	Всего	Отпр./сек.	Получ./сек.	Отправлено	Получено
Brasilia	0	0				NaN			0	0	0	0
Diadema	0	0				NaN			0	0	0	0
Porto Alegre	0	0				NaN			0	0	0	0
Salvador	0	0				NaN			0	0	0	0

Здесь в сводном виде отображается статистика мониторинга зон разделяемой памяти для контекста `location` в `http`, формируемая на основе раздела API `/status/http/location_zones/`. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны **Совет** Щелкните стрелку рядом с пунктом `Зона`, чтобы отсортировать зоны по алфавиту или порядку в конфигурации.
`Запросы`	Общее количество запросов, а также число запросов в секунду
`Ответы`	Количество ответов с разбиением по кодам статуса, а также их общее количество
`Трафик`	Скорость исходящего и входящего трафика в байтах в секунду, а также общие объемы исходящего и входящего трафика в байтах

Раздел "Зоны ограничения соединений (Limit Conn)"


Зоны ограничения соединений (Limit Conn)

Зона	Передано	Отклонено	Сброшено	Пропущено
limit-conn-http	0	0	0	0

Здесь приведена статистика зон `limit_conn` в контексте `http`, формируемая на основе раздела API `/status/http/limit_conns/`. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны **Совет** Щелкните значок рядом с пунктом `Зона`, чтобы открыть или закрыть график со следующими показателями.
`Передано`	Общее количество проксированных соединений
`Отклонено`	Общее количество сброшенных соединений
`Сброшено`	Общее количество соединений, сброшенных из-за переполнения хранилища зоны
`Пропущено`	Общее количество соединений, переданных с нулевым или превосходящим 255 байт ключом

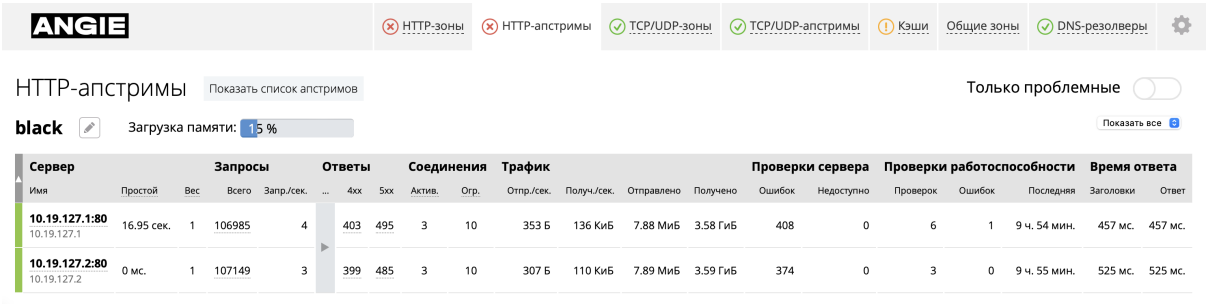
Раздел "Зоны ограничения запросов (Limit Req)"



Здесь приведена статистика зон `limit_req` в контексте `http`, формируемая на основе раздела API `/status/http/limit_reqs/`. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны **Совет** Щелкните значок рядом с пунктом `Зона`, чтобы открыть или закрыть график со следующими показателями.
`Передано`	Общее количество проксированных соединений
`Задержано`	Общее количество задержанных соединений
`Отклонено`	Общее количество сброшенных соединений
`Сброшено`	Общее количество соединений, сброшенных из-за переполнения хранилища зоны
`Пропущено`	Общее количество соединений, переданных с нулевым или превосходящим 255 байт ключом

5.1.4.5 Вкладка "HTTP-апстримы"



Предупреждение

Требует задать директиву adc__u_zone в блоке adc__u_upstream в контексте `http`.

На этой вкладке в сводном виде отображается статистика мониторинга апстримов контекста `http`, формируемая на основе раздела API `/status/http/upstreams/`. В режиме отладки также отображается процент загрузки памяти.

- Кнопка `Показать список апстримов` переключает отображение краткого списка апстримов с указанием числа проблемных апстримов и пиров.
- Переключатель `Только проблемные` включает и отключает режим вывода статистики по проблемным апстримам.
- Раскрывающийся список с правой стороны таблицы каждого апстрима позволяет отфильтровать серверы в определенном состоянии (`Активные`, `Проблемные`, `На проверке`, `Выключенные`, `Занятые`, `Режим ожидания`, `Восстанавливается`, `Разгружаемые`).

Для каждого апстрима, помимо имени и загрузки зоны разделяемой памяти, представлены следующие данные:

`Сервер`	Имена, общее время простоя и веса серверов апстрима **Совет** Щелкните стрелку рядом с пунктом `Сервер`, чтобы отсортировать серверы по их состоянию или порядку в конфигурации.
`Запросы`	Общее количество и скорость обработки запросов
`Ответы`	Количество ответов с разбиением по кодам статуса
`Соединения`	Количество активных соединений и их максимальный предел, если он задан
`Трафик`	Скорость исходящего и входящего трафика в байтах в секунду, а также общие объемы исходящего и входящего трафика в байтах
`Проверки сервера`	Количество неуспешных обращений к серверу и число раз, когда сервер считался недоступным (объект `health` в API)
`Проверки работоспособности`	Общее количество проверок сервера, количество неуспешных проверок, а также время последней проверки
`Время ответа`	Время от начала запроса до отправки первого байта ответа; общее время от начала запроса до завершения отправки всего ответа (объект `health` в API)

5.1.4.6 Вкладка "TCP/UDP-зоны"

Предупреждение

Требует задать следующие директивы:

- `status_zone` в контексте server или stream;
- `limit_conn` в контексте server или stream;
- adc__limit_conn_zone в контексте `stream`.

Пример:

```
stream {

    # ...
    limit_conn_zone $connection zone=limit-conn-stream:10m;

    server {

        # ...
        limit_conn limit-conn-stream 1;
        status_zone foo;
    }
}
```

Раздел "TCP/UDP-зоны"

TCP/UDP-зоны

Зона	Соединения			Сессии				Трафик				SSL		
	Текущих	Всего	Соед./сек.	2xx	4xx	5xx	Всего	Отпр./сек.	Получ./сек.	Отправлено	Получено	Рукопожатий	Неудачных рукопожатий	Повторных использований
sing_chorus	3	403	0	372	0	28	400	0	0	4.41 ГБ	6.51 МБ	375	0	180

Здесь в сводном виде отображается статистика мониторинга зон разделяемой памяти контекста `server` в `stream`, формируемая на основе раздела API `/status/stream/server_zones/`. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны
`Соединения`	Текущее и общее количество соединений, а также число соединений в секунду
`Сессии`	Количество сессий с разбиением по кодам статуса, а также их общее число
`Трафик`	Скорость исходящего и входящего трафика в байтах в секунду, а также общие объемы исходящего и входящего трафика в байтах
`SSL`	Суммарные показатели количества: успешных SSL-рукопожатий; неуспешных SSL-рукопожатий; повторных использований SSL-сессий

Раздел "Зоны ограничения соединений (Limit Conn)"

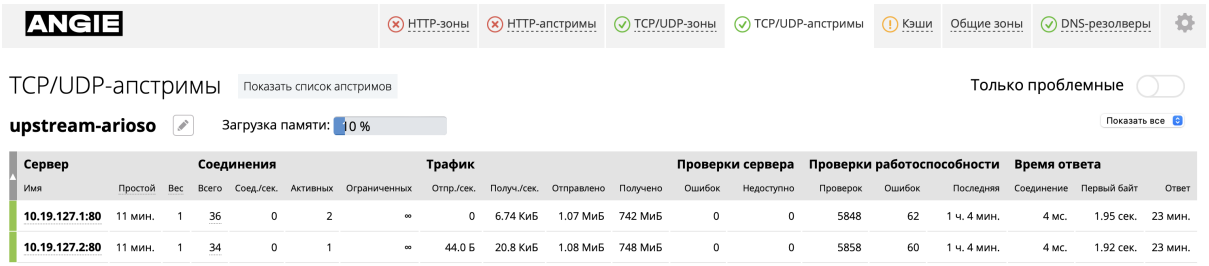
Зоны ограничения соединений (Limit Conn)

	Зона	Передано	Отклонено	Сброшено	Пропущено
	limit-conn-stream	403	0	0	0

Здесь приведена статистика зон `limit_conn` в контексте `stream`, формируемая на основе раздела API `/status/stream/limit_conns/`. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны **Совет** Щелкните значок рядом с пунктом `Зона`, чтобы открыть или закрыть график со следующими показателями.
`Передано`	Общее количество проксированных соединений
`Отклонено`	Общее количество сброшенных соединений
`Сброшено`	Общее количество соединений, сброшенных из-за переполнения хранилища зоны
`Пропущено`	Общее количество соединений, переданных с нулевым или превосходящим 255 байт ключом

5.1.4.7 Вкладка "TCP/UDP-апстримы"



Предупреждение

Требует задать директиву adc__s_u_zone в блоке adc__s_u_upstream в контексте `stream`.

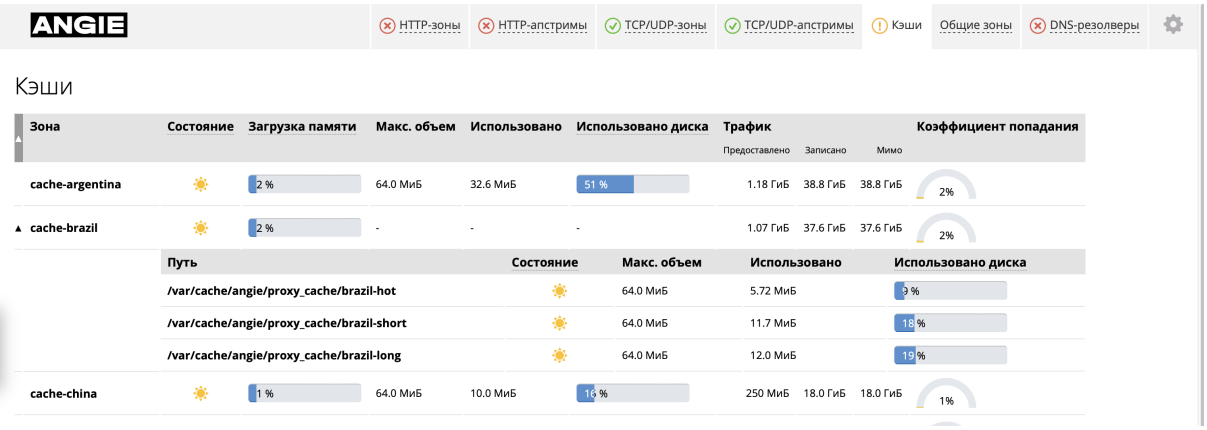
На этой вкладке в сводном виде отображается статистика мониторинга апстримов контекста `stream`, формируемая на основе раздела API `/status/stream/upstreams/`. В режиме отладки также отображается процент загрузки памяти.

- Кнопка `Показать список апстримов` переключает отображение краткого списка апстримов с указанием числа проблемных апстримов и пиров.
- Переключатель `Только проблемные` включает и отключает режим вывода статистики по проблемным апстримам.
- Раскрывающийся список с правой стороны таблицы каждого апстрима позволяет отфильтровать серверы в определенном состоянии (`Активные`, `Проблемные`, `На проверке`, `Выключенные`, `Занятые`, `Режим ожидания`, `Восстанавливается`, `Разгружаемые`).

Для каждого апстрима представлены следующие данные:

`Сервер`	Имена, общее время простоя и веса серверов апстрима **Совет** Щелкните стрелку рядом с пунктом `Сервер`, чтобы отсортировать серверы по их состоянию или порядку в конфигурации.
`Соединения`	Количество активных соединений и их максимальный предел, если он задан
`Трафик`	Скорость исходящего и входящего трафика в байтах в секунду, а также общие объемы исходящего и входящего трафика в байтах
`Проверки сервера`	Количество неуспешных обращений к серверу и число раз, когда сервер считался недоступным (объект `health` в API)
`Проверки работоспособности`	Общее количество проверок сервера, количество неуспешных проверок, а также время последней проверки
`Время ответа`	Время, затраченное на установку соединения с бэкендом; время от начала запроса до получения первого байта ответа; общее время, прошедшее от начала запроса до получения последнего байта ответа (объект `health` в API)

5.1.4.8 Вкладка "Кэши"



Предупреждение

Требует задать зону кэша директивой adc__proxy_cache_path, adc__fastcgi_cache_path, adc__scgi_cache_path или adc__uwsgi_cache_path.

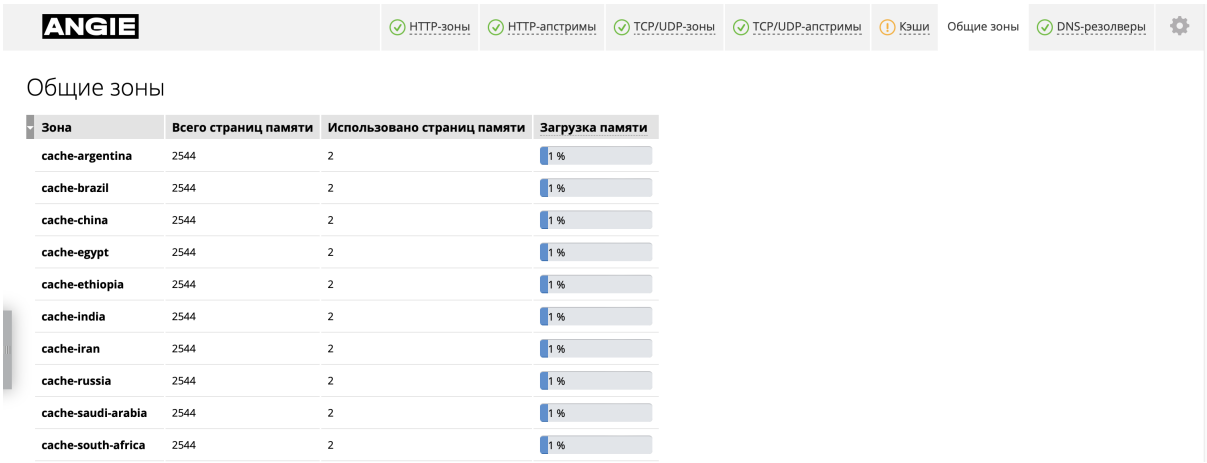
На этой вкладке в сводном виде отображается статистика мониторинга зон кэша контекста `http`, формируемая на основе раздела API `/status/http/caches/`. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны **Совет** Щелкните значок рядом с пунктом `Зона`, чтобы открыть или закрыть списки шардов для всех зон, где они есть.
`Состояние`	Состояние кэша: холодный (метаданные загружаются в память) или горячий (метаданные загружены)
`Загрузка памяти`	Коэффициент использования памяти
`Макс. объем`	Максимальный объем кэша на диске в байтах; знак бесконечности, если объем кэша не ограничен
`Использовано`	Текущий объем кэша на диске в байтах
`Использовано диска`	Коэффициент использования диска
`Трафик`	Объем трафика (в байтах), переданного из кэша, записанного в кэш и возвращенного в обход кэша
`Коэффициент попадания`	Доля ответов, переданных из кэша (`hit`, `stale`, `updating`, `revalidated`), среди всех ответов зоны за временное окно из виджета "Настройки", в процентах; 0, если ответов не было

Для зоны с включенным шардингом значения `Макс. объем`, `Использовано` и `Использовано диска` отслеживаются отдельно для каждого шарда; в строке самой зоны выводятся прочерки, а зона обозначена как раскрывающийся список, в котором перечислены отдельные шарды:

`Путь`	Путь шарда на диске
`Состояние`	Состояние шарда: холодный (метаданные загружаются в память) или горячий (метаданные загружены)
`Макс. объем`	Максимальный объем шарда на диске в байтах; знак бесконечности, если объем шарда не ограничен
`Использовано`	Текущий объем шарда на диске в байтах
`Использовано диска`	Коэффициент использования диска

5.1.4.9 Вкладка "Общие зоны"



На этой вкладке в сводном виде отображается статистика мониторинга **всех** зон разделяемой памяти для всех контекстов. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны **Совет** Щелкните стрелку рядом с пунктом `Зона`, чтобы отсортировать зоны по размеру или порядку в конфигурации.
`Всего страниц памяти`	Общее количество страниц памяти
`Использовано страниц памяти`	Количество используемых страниц памяти
`Загрузка памяти`	Коэффициент использования памяти для зоны

5.1.4.10 Вкладка "DNS-резолверы"



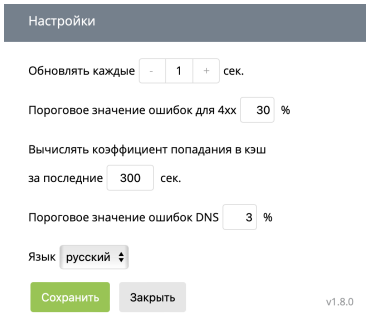
Предупреждение

Требует задать параметр `status_zone` в директиве `resolver` (HTTP, Stream или Mail).

На этой вкладке в сводном виде отображается статистика запросов в зонах разделяемой памяти DNS, формируемая на основе раздела API `/status/resolvers/`. Для каждой зоны представлены следующие данные:

`Зона`	Имя зоны **Совет** Щелкните стрелку рядом с пунктом `Зона`, чтобы отсортировать зоны по состоянию или порядку в конфигурации.
`Запросы`	Количество запросов типа A и AAAA, SRV, PTR
`Ответы`	Количество ответов с разделением по соответствующим кодам (`Успешные`, `Ошибок формата`, `Сервер не завершил запрос`, `Ошибок имени`, `Запрос не поддерживается`, `Запрос отклонен`, `Неизвестных ошибок`, `Истекло время ожидания`)

5.1.4.11 Виджет "Настройки"



Позволяет настроить общие параметры консоли:

- Частоту обновления данных. Значение по умолчанию — 1 сек.
- Порог доли ответов `4xx` среди всех запросов HTTP-зоны или сервера HTTP-апстрима. При его превышении зона или сервер учитывается как предупреждение в виджете "HTTP-зоны" или "HTTP-апстримы", а значок соответствующей вкладки становится "желтым", если там нет проблем; на вкладке "HTTP-зоны" строка такой зоны тоже помечается "желтым". Значение по умолчанию — 30%.
- Временное окно для вычисления соотношения успешных попаданий в кэш. Значение по умолчанию — 300 сек.
- Порог ошибок DNS. При его превышении зона резолвера становится "красной". Значение по умолчанию — 3%.
- Язык интерфейса консоли. Доступные варианты: английский и русский. По умолчанию язык консоли выбирается на основе локали, установленной в браузере.

5.1.4.12 Панель управления консолью

На всех вкладках в середине левой части страницы есть выдвигающаяся панель с двумя кнопками . Верхняя приостанавливает и вновь запускает обновление данных из API, а нижняя позволяет обновить данные вручную, когда обновление приостановлено.

5.1.5 Экспорт метрик

Экспорт метрик из Angie ADC во внешний Prometheus выполняется с помощью механизма `federation`. Для экспорта доступны:

- системные метрики Node Exporter;
- метрики Angie ADC.

5.1.5.1 Экспорт метрик Node Exporter

Чтобы настроить сбор метрик от Node Exporter, необходимо добавить в конфигурационный файл внешнего Prometheus (блок `scrape_configs`) следующую конфигурацию:

```
scrape_configs:
  - job_name: adc_node
    honor_labels: false
    metrics_path: /federate
    params:
      match[]:
        - '{job="node"}'
    static_configs:
      - targets:
        - <адрес_ADC-инстанса1>:8080
        - <адрес_ADC-инстанса2>:8080
```

После обновления конфигурации необходимо перезапустить сервис Prometheus.

Для визуализации собранных данных можно использовать готовый дашборд Grafana: https://grafana.com/grafana/dashboards/1860-node-exporter-full/.

5.1.5.2 Экспорт метрик балансировщика нагрузки

Чтобы настроить сбор метрик от балансировщика нагрузки, необходимо добавить в конфигурационный файл Prometheus (блок `scrape_configs`) следующую конфигурацию:

```
scrape_configs:
  - job_name: adc_angie
    honor_labels: false
    metrics_path: /federate
    params:
      match[]:
        - '{job="local-lb"}'
    static_configs:
      - targets:
        - <адрес_ADC-инстанса1>:8080
        - <адрес_ADC-инстанса2>:8080
```

После обновления конфигурации необходимо перезапустить сервис Prometheus.

Для визуализации собранных данных можно использовать готовый дашборд Grafana: https://grafana.com/grafana/dashboards/20719-angie-dashboard/.

5.1.5.3 Экспорт системных метрик Angie ADC

```
scrape_configs:
  - job_name: hardware
    honor_labels: false
    metrics_path: /federate
    params:
      match[]:
        - '{job="node"}'
        - '{job="smartctl"}'
        - '{job="ipmi"}'
    static_configs:
      - targets:
        - <адрес_ADC-инстанса1>:8080
        - <адрес_ADC-инстанса2>:8080
```

Подробнее о системных метриках см. *Мониторинг состояния системы*.

5.1.6 SNMP

Angie ADC может встраиваться в инфраструктуру мониторинга корпоративного уровня (например, Zabbix, Nagios). Доступно получение стандартных метрик операционной системы и собственных метрик Angie ADC (см. ниже).

Поддерживаемые протоколы:

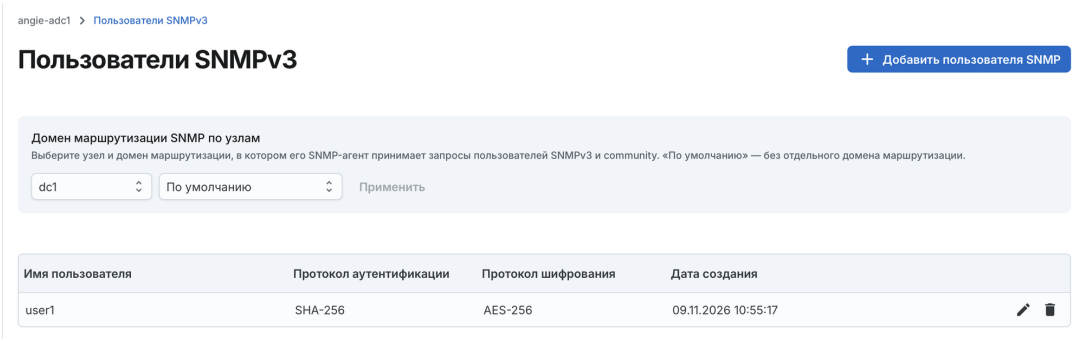
- **SNMPv2c**. При использовании протокола SNMPv2c доступ к метрикам определяется *community*. Данные передаются в незашифрованном виде.
- **SNMPv3**. При использовании протокола SNMPv3 необходимо предварительно добавить *пользователя SNMP*, чтобы предоставить безопасный доступ для системы мониторинга к SNMP-метрикам. Данные передаются в зашифрованном виде.

Протоколы SNMPv2c и SNMPv3 могут работать одновременно. Доступ предоставляется только на чтение. Настройки пользователей и строки community распространяются на все узлы *кластера*. При опросе конкретного узла возвращаются SNMP-метрики этого узла.

> **Примечание**
>
> Для интеграции с системами мониторинга предоставляется MIB-файл, который можно скачать в веб-интерфейсе Angie ADC (`Мониторинг` → `Система` → `Скачать SNMP MIB-файл` в верхней правой части экрана).

5.1.6.1 Настройка для SNMPv3

При использовании протокола SNMPv3 необходимо создать пользователей SNMP (т. е. те системы мониторинга, которые будут иметь доступ к данным).



Примечание

Изменение списка пользователей SNMPv3 вызывает кратковременный перезапуск службы snmpd (1–2 секунды) на узлах кластера.

Добавление пользователя SNMP:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Управление SNMP` → `Пользователи`.
2. Нажмите `Добавить пользователя SNMP`.
3. В открывшемся окне заполните поля формы для добавления нового пользователя:
   - `Имя пользователя` — уникальный идентификатор пользователя SNMPv3, например `zabbix-user`.
   - `Секрет аутентификации` — зашифрованный секрет аутентификации (AES-256-GCM, Base64).
   - `Протокол шифрования` — поддерживаются AES-128 и AES-256.
   - `Секрет шифрования` — зашифрованный секрет шифрования (AES-256-GCM, Base64).
4. Нажмите `Добавить`.

Просмотр пользователей SNMP:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Управление SNMP` → `Пользователи`.
2. В открывшемся окне отображаются добавленные пользователи SNMP.

   Для каждого пользователя отображается следующая информация:
   - Имя пользователя — уникальный идентификатор пользователя SNMPv3.
   - Протокол аутентификации — всегда SHA-256.
   - Протокол шифрования — поддерживаются AES-128 и AES-256.
   - Дата создания — дата и время создания записи.

Редактирование и удаление пользователей SNMP:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Управление SNMP` → `Пользователи`.
2. В открывшемся окне отображаются добавленные пользователи SNMP.

3. Нажмите значок редактирования или удаления напротив нужного пользователя.

5.1.6.2 Настройка для SNMPv2c

При опросе по протоколу SNMPv2c система мониторинга передает в каждом запросе строку community. Angie ADC отвечает на запрос, только если выполнены оба условия:

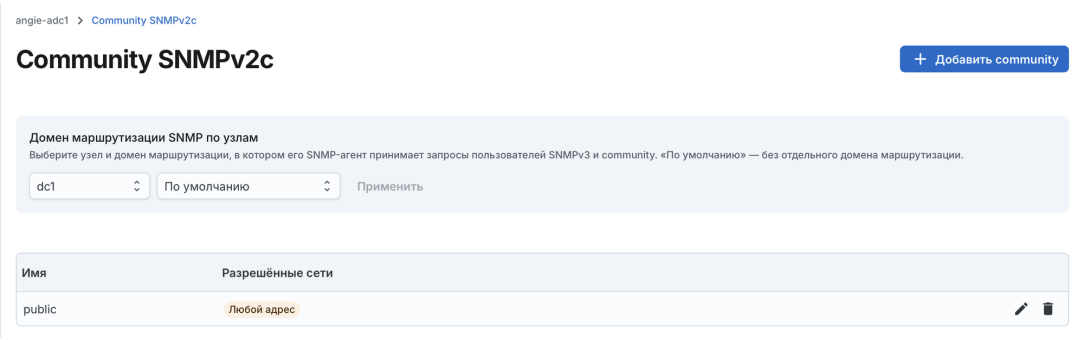
- строка совпадает с одной из заданных в Angie ADC строк community;
- IP-адрес источника запроса входит хотя бы в одну из сетей, разрешенных для этой строки community.

Остальные запросы, в том числе запросы с неизвестной строкой community, отклоняются.

Строка community `public` предустановлена по умолчанию и доступна с любого адреса.

Примечание

Если строка community `public` не используется, удалите ее или ограничьте доверенными сетями.



Добавление новой строки community:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Управление SNMP` → `Community`.
2. Нажмите `Добавить community`.
3. В открывшемся окне заполните поля формы:
   - `Имя` — текстовое значение строки community, например `monitoring`. Допускается от 1 до 64 символов: латинские буквы, цифры и символы `_ . : @ -`. Строка должна быть уникальной.
   - `Разрешенные сети` — IPv4-сети в формате CIDR, по одной сети в строке, например `10.0.2.0/24`. Нужно указать хотя бы одну сеть; сети не должны повторяться.

     Совет

     Чтобы разрешить запросы с любого адреса, укажите `0.0.0.0/0`.
4. Нажмите `Добавить`.

Пример запроса к узлу с community `monitoring` с адреса из разрешенной сети:

```
snmpget -v2c -c monitoring <IP-адрес узла> 1.3.6.1.4.1.2021.4.6.0
```

Просмотр строк community:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Управление SNMP` → `Community`.

2. В открывшемся окне отображаются настроенные строки community.

   Для каждой строки community отображается следующая информация:

   - `Имя` — текстовое значение строки community.
   - `Разрешенные сети` — список IPv4-сетей, из которых разрешены запросы с этой строкой community.

Редактирование строки community:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Управление SNMP` → `Community`.
2. Нажмите значок редактирования напротив нужной строки community.
3. Внесите изменения и нажмите `Сохранить`.

Удаление строки community:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Управление SNMP` → `Community`.
2. Нажмите значок удаления напротив строки community.
3. Подтвердите удаление.

Если удалить все строки community, опрос Angie ADC по протоколу SNMPv2c будет недоступен.

5.1.6.3 Настройка домена маршрутизации

Вы можете задать *домен маршрутизации*, в котором SNMP-агент узла будет принимать запросы пользователей SNMPv3 и community SNMPv2c. По умолчанию на всех узлах используется общая сеть.

Чтобы задать домен маршрутизации:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Управление SNMP` → `Community` или `Пользователи`.
2. В верхней части окна выберите узел, на котором вы хотите задать домен маршрутизации.
3. Выберите нужный домен маршрутизации. Значение `По умолчанию` означает работу в общей сети.
4. Нажмите `Применить`.

Выбранный домен маршрутизации будет применен для SNMPv3 и SNMPv2c.

5.1.6.4 Метрики операционной системы

Поддерживаются все системные метрики `Net-SNMP`.

Пример запроса объема доступной физической памяти:

```
snmpget -v2c -c public 127.0.0.1 1.3.6.1.4.1.2021.4.6.0
```

Пример ответа:

```
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 743028 kB
```

Ниже приведены примеры самых распространенных метрик, которые можно отслеживать:

Метрика	OID	Тип	Описание
diskIOLoad.1	.1.3.6.1.4.1.2021.13.1	Inte	Процент времени, когда диск был занят выполнением операций ввода-вывода.
diskIOReads.1	.1.3.6.1.4.1.2021.13.1	Cou	Количество операций чтения с диска.
diskIOWrites.1	.1.3.6.1.4.1.2021.13.1	Cou	Количество операций записи на диск.
dskErrorFlag.1	.1.3.6.1.4.1.2021.9.1.	Inte	Ошибка диска: становится 1, если место на диске заканчивается.
dskPercent.1	.1.3.6.1.4.1.2021.9.1.	Inte	Процент занятого места на основном разделе.
ifInDiscards.X	.1.3.6.1.2.1.2.2.1.13.X	Cou	Количество входящих пакетов, отброшенных из-за переполнения буферов.
ifInErrors.X	.1.3.6.1.2.1.2.2.1.14.X	Cou	Ошибки сети. Указывает на входящие пакеты с ошибками или проблемы на физическом уровне.
ifInOctets.X	.1.3.6.1.2.1.2.2.1.10.X	Cou	Входящий трафик. Объем полученных данных на сетевом интерфейсе.
ifOutOctets.X	.1.3.6.1.2.1.2.2.1.16.X	Cou	Исходящий трафик. Объем переданных данных через сетевой интерфейс.
hrSystemProcesses.0	.1.3.6.1.2.1.25.1.6.0	Gau	Общее количество запущенных процессов. Резкий рост может указывать на зависшие скрипты.
hrSystemUptime.0	.1.3.6.1.2.1.25.1.1.0	Tick	Время непрерывной работы сервера. Используется для обнаружения перезагрузки сервера.
laLoad.1	.1.3.6.1.4.1.2021.10.1	Stri	Средняя нагрузка (load average) на CPU за одну минуту.
memAvailReal.0	.1.3.6.1.4.1.2021.4.6.	Inte	Объем доступной физической памяти.
memCached.0	.1.3.6.1.4.1.2021.4.15	Inte	Память, используемая файловым кэшем для ускорения операций чтения.
memTotalFreeSwap.	.1.3.6.1.4.1.2021.4.4.	Inte	Свободный Swap. При снижении до 0 возможен запуск OOM Killer.
ssCpuIdle.0	.1.3.6.1.4.1.2021.11.1	Inte	Процент свободного ресурса. Близкое к 0 значение указывает на перегрузку CPU.
ssCpuRawWait.0	.1.3.6.1.4.1.2021.11.5	Cou	Время ожидания ввода-вывода. Рост значения указывает на проблемы с дисковой подсистемой или БД.

5.1.6.5 Собственные метрики Angie ADC

Angie ADC позволяет получать по SNMP собственные метрики из Prometheus. У собственных метрик будет базовый OID `.1.3.6.1.4.1.2021.50`.

Пример запроса метрики базовой доступности сервиса `up`:

```
snmpget -v2c -c public 127.0.0.1 1.3.6.1.4.1.2021.50.2.1
```

Ответ:

```
UCD-SNMP-MIB::ucdavis.50.2.1 = Gauge32: 1
```

Ответ `1` означает, что сервис доступен.

Пример запроса всего дерева собственных метрик:

```
snmpwalk -v2c -c public 127.0.0.1 1.3.6.1.4.1.2021.50
```

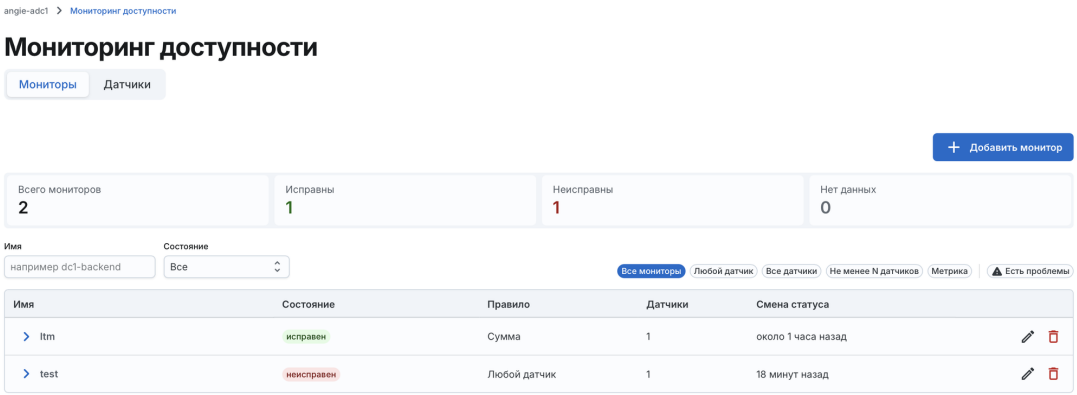
Если Prometheus недоступен или метрик нет, в ответе может быть `NONE` или ошибка.

Ниже приведены метрики Prometheus, поддерживаемые по SNMP на данный момент. Список поддерживаемых метрик будет пополняться.

Метрика из Prometheus	OID	Тип	Описание
angie_connections_	.1.3.6.1.4.1.2021.50.1	Cou	Принятые соединения — мониторинг общего потока входящих подключений.
angie_connections_	.1.3.6.1.4.1.2021.50.1	Gau	Активные сессии — мониторинг количества пользователей на сайте в данную секунду.
angie_connections_	.1.3.6.1.4.1.2021.50.1	Cou	Сброшенные соединения — рост этого показателя указывает на достижение лимитов сервера.
angie_http_request	.1.3.6.1.4.1.2021.50.1	Cou	Всего HTTP-запросов — позволяет рассчитать RPS (количество запросов в секунду).
go_goroutines	.1.3.6.1.4.1.2021.50.2	Gau	Потоки — мониторинг здоровья Go-приложения (защита от утечек памяти).
go_memstats_alloc	.1.3.6.1.4.1.2021.50.2	Gau	Память процесса — позволяет отслеживать, сколько оперативной памяти выделено и используется Go-процессом сейчас.
scrape_duration_se	.1.3.6.1.4.1.2021.50.2	Gau	Время сбора данных в секундах — позволяет оценить производительность.
scrape_samples_scr	.1.3.6.1.4.1.2021.50.2	Gau	Количество полученных строк метрик. Резкое падение показателя может означать, что часть метрик потеряна.
up	.1.3.6.1.4.1.2021.50.2	Gau	Доступность — базовая health-метрика, `1` — сервис доступен, `0` — недоступен.

5.2 Доступность

Мониторинг доступности позволяет отслеживать доступность узлов и бэкендов в кластере Angie ADC.



Для отслеживания состояния бэкендов на узлах кластера настраиваются датчики, выполняющие проверки работоспособности бэкендов. Далее можно создать мониторы, которые будут объединять несколько датчиков и по правилу агрегации определять общий статус доступности объектов.

5.2.1 Датчики

Датчики поддерживают следующие типы проверок бэкендов:

`HTTP`	Активная проверка по протоколу HTTP.
`HTTPS`	Активная проверка по протоколу HTTPS.
`TCP`	Активная проверка по протоколу TCP.
`ICMP`	Проверка доступности с помощью ICMP Echo Request (ping).
`Angie`	Проверка на основе данных о состоянии бэкендов, полученных через Status API Angie. Подходит для случаев, когда бэкенды не имеют собственного URL для проверки.
`Соединения LTM`	Получение числа соединений или запросов из API балансировщика нагрузки (LTM) на узле датчика: для всего балансировщика, группы upstream или зоны `status_zone`. Используется для глобальной балансировки *least connection*.

5.2.2 Мониторы

Поддерживаются мониторы двух типов:

- `Здоровье`: отслеживают работоспособность бэкенда по датчикам с проверками `HTTP`, `HTTPS`, `TCP`, `ICMP`, `Angie`;
- `Метрика`: отслеживают загрузку бэкенда по датчикам с проверкой `Соединения LTM` и отдают число — нагрузку бэкенда для балансировки *least connection*.

Состав датчиков в мониторе зависит от того, доступность чего необходимо отслеживать. В один монитор можно объединять как датчики одного узла, так и датчики с разных узлов кластера.

Мониторы типа `Здоровье` поддерживают следующие типы правил агрегации датчиков:

`Любой датчик`	Монитор исправен, если работает хотя бы один датчик.
`Все датчики`	Монитор исправен, если работают все датчики.
`Не менее N датчиков`	Монитор исправен, если работают N и более датчиков.

Мониторы типа `Метрика` поддерживают следующие типы правил агрегации датчиков:

`Сумма`	Сумма чисел датчиков.
`Среднее`	Среднее число по датчикам.
`Максимум`	Наибольшее число среди датчиков.

5.2.3 Применение

Примеры:

- **Определение доступности дата-центра для глобальной балансировки**: создайте монитор дата-центра и включите в него все датчики всех узлов этого дата-центра по правилу `Любой датчик`. Исправность монитора будет означать, что дата-центр в целом доступен для глобальной балансировки. Простой пример см. *Глобальная балансировка с проверкой доступности приложений*.
- **Определение доступности сервиса на нескольких узлах**: создайте монитор сервиса и включите в него все датчики этого сервиса со всех узлов, где он запущен, по правилу `Любой датчик`. Исправность монитора будет означать доступность сервиса в целом, не на конкретном узле.
- **Углубленная проверка одного бэкенда**: создайте монитор бэкенда и включите в него несколько датчиков этого бэкенда с разными типами проверок по правилу `Все датчики`. Исправность монитора будет означать работоспособность бэкенда сразу на нескольких уровнях.

В этом разделе:

- *Настройка датчиков и мониторов*
- *Мониторинг доступности*

5.2.3.1 Настройка датчиков и мониторов

Датчики и мониторы настраиваются в веб-интерфейсе Angie ADC (`Система` → `Доступность`).

В этой статье:

- *Добавление датчика*;
- *Добавление монитора*;
- *Редактирование датчика*;
- *Редактирование монитора*;
- *Удаление датчика*;
- *Удаление монитора*.

Добавление датчика

Чтобы добавить датчик:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Доступность`.
2. На вкладке `Датчики` нажмите `Добавить датчик`.
3. Задайте параметры датчика:

`Имя ресурса`	Имя проверяемого ресурса в произвольной форме. Допускаются строчные латинские буквы, цифры и дефис, не более 63 символов. Имя ресурса после создания датчика изменить нельзя. **Примечание** Имя датчика формируется автоматически из имени узла и имени ресурса; итоговое имя датчика *`узел-ресурс`* не должно превышать 63 символа. Имя датчика уникально в пределах кластера.
`Узлы`	Узлы кластера, на которых выполняется проверка. **Совет** Можно выбрать несколько узлов, чтобы создать сразу несколько аналогичных датчиков. Для каждого выбранного узла будет создан отдельный датчик.
`Включен`	Переключатель, включающий и выключающий датчик. По умолчанию датчик включен.
`Проверка`	Протокол проверки ресурса. Поддерживаются следующие типы проверок: • `HTTP` — активная проверка по протоколу HTTP. • `HTTPS` — активная проверка по протоколу HTTPS. • `TCP` — активная проверка по протоколу TCP. • `ICMP` — проверка доступности с помощью ICMP Echo Request (ping). • `Angie` — проверка на основе данных о состоянии бэкендов, полученных через Status API Angie. Подходит для случаев, когда бэкенды не имеют собственного URL для проверки. • `Соединения LTM` — получение числа соединений или запросов из API балансировщика нагрузки (LTM) на узле датчика. Используется в мониторах метрики для глобальной балансировки *least connection*. Набор параметров зависит от типа проверки: **Параметры проверки HTTP** `Домен маршрутизаг` — *Домен маршрутизации*, через интерфейсы которого выполняется проверка. Значение `По умолчанию` означает, что используется общая сеть. В списке отображаются только домены маршрутизации, заданные на всех выбранных узлах. `URL` — URL, по которому выполняется запрос проверки, например `https://10.20.0.14/health`. `Метод` — HTTP-метод запроса. Значение по умолчанию `GET`. `Ожидаемые коды` — Коды ответа, при которых проверка считается успешной, например `200`. `Заголовки запроса` — Заголовки, добавляемые к запросу проверки. Необязательный параметр. `Ожидаемое содержимое ответа` — Подстрока, которую должно содержать тело ответа для успешного прохождения проверки. Необязательный параметр. `Интервал проверки` — Как часто выполняется проверка. Значение по умолчанию `1s`. `Таймаут` — Время ожидания ответа. Если за это время ответ не получен, проверка считается неуспешной. Значение по умолчанию `500ms`. `Порог сбоя (проверок)` — Число подряд неуспешных проверок, после которого датчик переходит в состояние `не работает`. Значение по умолчанию 2. `Порог успеха (проверок)` — Число подряд успешных проверок, после которого датчик возвращается в состояние `работает`. Значение по умолчанию 2.

4. Нажмите `Создать`.

   Для каждого выбранного узла будет создан датчик. В таблице датчиков для каждого датчика будет отображаться результат проверки в столбце `Состояние` (`работает`, `не работает` или `нет данных`).

Добавление монитора

Чтобы добавить монитор:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Доступность`.
2. На вкладке `Мониторы` нажмите `Добавить монитор`.
3. Задайте параметры монитора:

`Имя`	Имя монитора. Допускаются строчные латинские буквы, цифры и дефис, не более 63 символов. Должно быть уникальным. Имя монитора после создания изменить нельзя.
`Тип монитора`	Определяет, что отслеживает монитор: • `Здоровье` — отслеживает работоспособность бэкендов по датчикам проверки доступности. • `Метрика` — отслеживает загрузку бэкендов по датчикам с проверкой `Соединения LTM`. Используется для режима балансировки *least connection*. Значение по умолчанию `Здоровье`. Тип монитора после создания изменить нельзя.
`Правило агрегации`	Для монитора типа `Здоровье` определяет, при каком состоянии датчиков монитор имеет статус `исправен`: • `Любой датчик` — монитор исправен, если работает хотя бы один датчик. • `Все датчики` — монитор исправен, если работают все датчики. • `Не менее N датчиков` — монитор исправен, если работают N и более датчиков. Значение N не может превышать число датчиков монитора. Для монитора типа `Метрика` определяет, как числа датчиков сводятся в одно: • `Сумма` — сумма чисел датчиков. Подходит, когда нагрузку одного VIP несут несколько узлов, например в паре высокой доступности. Значение по умолчанию. • `Среднее` — среднее число по датчикам. Подходит, когда бэкенд — площадка с несколькими LTM, а площадки разного размера. • `Максимум` — наибольшее число среди датчиков. Подходит, когда важна загрузка самого нагруженного LTM площадки. В расчет входят только датчики с актуальным числом. Если таких датчиков нет, монитор получает статус `нет данных`.
`Датчики`	Имена датчиков, входящих в монитор. Нужно указать хотя бы один датчик. Для монитора типа `Метрика` доступны только датчики с проверкой `Соединения LTM`, и все они должны считать одну величину: иметь одинаковый `Объект` (а для объекта `Зона (status_zone)` — одинаковый `Протокол`). Не объединяйте в одном мониторе датчики разных VIP: такое число не относится ни к одному бэкенду.

4. Нажмите `Добавить`.

В таблице мониторов отобразится добавленный монитор. Для каждого монитора отображается его статус (`исправен`, `неисправен` или `нет данных`). Статус `исправен` у монитора метрики означает, что число получено.

Редактирование датчика

Чтобы изменить датчик, на вкладке `Датчики` нажмите значок редактирования в строке датчика. В окне `Редактировать датчик` можно изменить тип и параметры проверки, периодичность и пороги. Имя датчика изменить нельзя.

Редактирование монитора

Чтобы изменить монитор, на вкладке `Мониторы` нажмите значок редактирования в строке монитора. В окне `Редактировать монитор` можно изменить правило агрегации и список датчиков. Имя и тип монитора изменить нельзя.

Удаление датчика

Чтобы удалить датчик, на вкладке `Датчики` нажмите значок удаления в строке датчика и подтвердите операцию.

Примечание

Если удаляемый датчик используется в мониторе, его состояние в мониторе начнет отображаться как `нет данных`.

Удаление монитора

Чтобы удалить монитор, на вкладке `Мониторы` нажмите значок удаления в строке монитора и подтвердите операцию. Монитор будет удален из кластера.

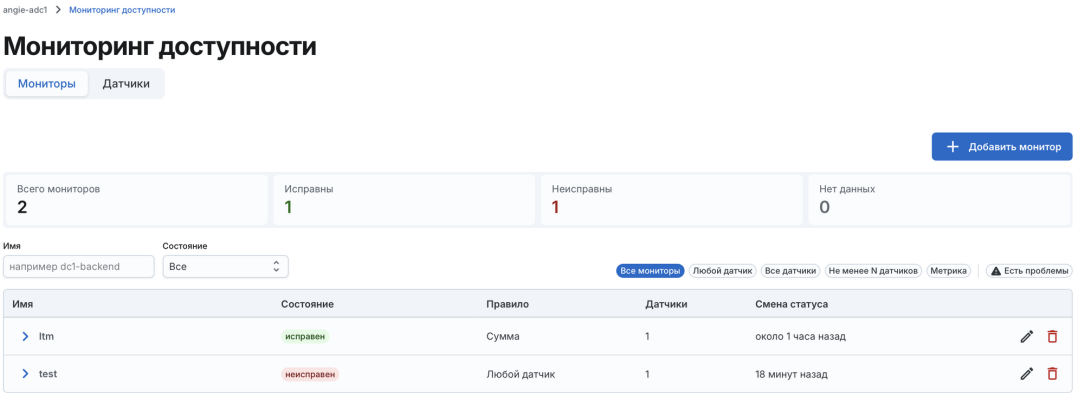
Примечание

Монитор, используемый в конфигурации GSLB, нельзя удалить. Сначала монитор необходимо удалить из настроек бэкенда.

5.2.3.2 Мониторинг доступности

Состояние датчиков и мониторов отображается в веб-интерфейсе Angie ADC (`Система` → `Доступность`) на вкладках `Мониторы` и `Датчики`. Мониторинг можно проводить с любого узла кластера Angie ADC.

Мониторы



В верхней части экрана отображается сводная статистика по мониторам:

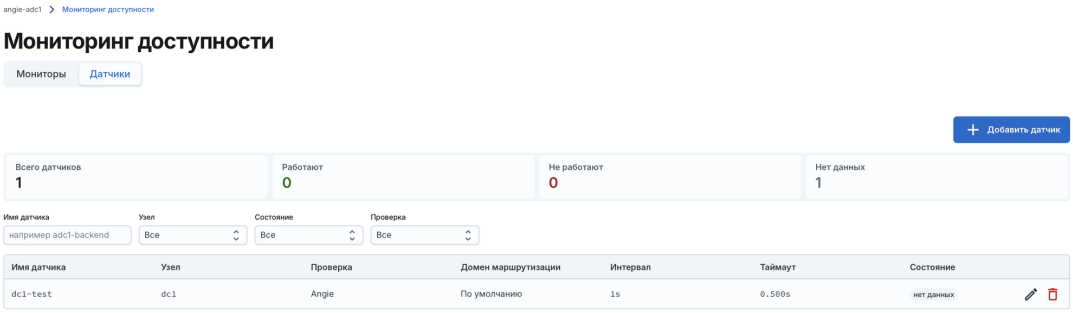
- `Всего мониторов`
- `исправны`
- `неисправны`
- `нет данных`

Ниже отображается таблица с данными по каждому монитору. Таблицу можно отфильтровать по имени монитора, состоянию и правилу агрегации; фильтр `Метрика` оставляет только мониторы метрики.

Для каждого монитора в таблице отображаются:

`Имя`	Имя монитора.
`Состояние`	Текущий статус монитора: `исправен`, `неисправен` или `нет данных`. **Примечание** Индикация `есть проблемы` выводится для монитора, когда правило агрегации позволяет вывести статус `исправен`, но при этом часть датчиков не работает или по ним нет данных.
`Правило`	Правило агрегации статусов датчиков в мониторе. Для монитора метрики — правило, по которому сводятся числа датчиков: `Сумма`, `Среднее` или `Максимум`.
`Датчики`	Число датчиков в мониторе. **Совет** Чтобы увидеть входящие датчики и их статусы, разверните строку монитора. Для монитора метрики в развернутой строке также отображаются его число, измеряемая величина, время замера и число каждого датчика.
`Смена статуса`	Время последнего изменения статуса монитора.

Датчики



В верхней части экрана отображается сводная статистика по датчикам:

- `Всего датчиков`
- `работают`
- `не работают`
- `нет данных`

Ниже отображается таблица с данными по каждому датчику. Таблицу можно отфильтровать по имени, узлу, состоянию и типу проверки.

Для каждого датчика в таблице отображаются:

`Имя датчика`	Имя датчика.
`Узел`	Узел кластера, на котором выполняется проверка.
`Проверка`	Тип проверки: `HTTP`, `HTTPS`, `TCP`, `ICMP`, `Angie` или `Соединения LTM`.
`Домен маршрутизации`	*Домен маршрутизации*, через интерфейсы которого выполняется проверка. Для датчиков без выбранного домена маршрутизации отображается `По умолчанию`.
`Интервал`	Периодичность выполнения проверки.
`Таймаут`	Время ожидания ответа.
`Состояние`	Текущий статус датчика: `работает`, `не работает` или `нет данных`.

5.3 Диагностика и логирование

В Angie ADC доступны следующие средства диагностики:

Веб-интерфейс:

- *Базовая диагностика сети*.
- *Журнал ошибок балансировщика*.

CLI:

- *Журналы событий Angie ADC*.
- *Сбор диагностической информации* (команда `diag`).
- *Расширенная диагностика* (контекст `diagnostics`).

Мастер настройки:

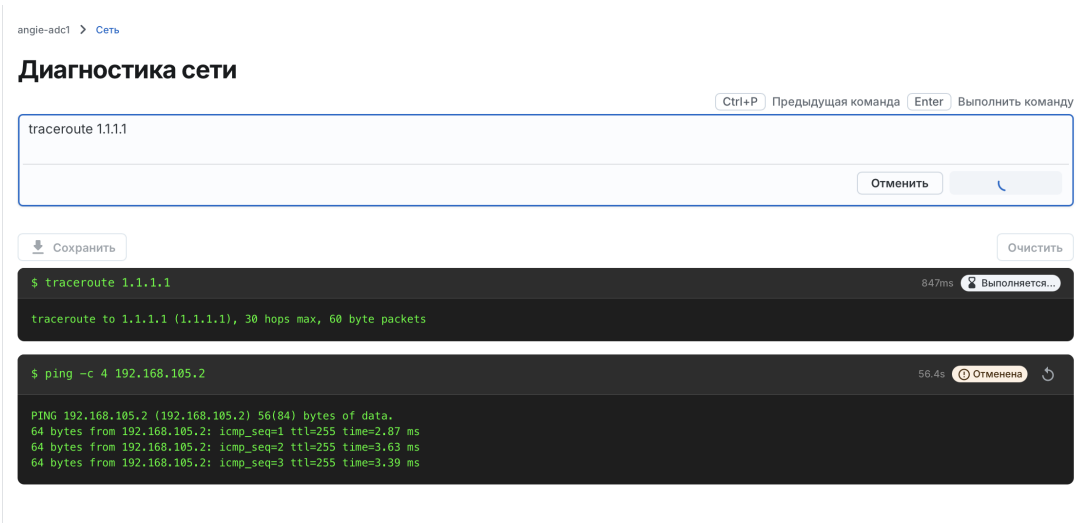
- *Аварийный сбор диагностической информации*.

Техническая поддержка для клиентов:

- https://support.angie.software
- support@angie.software

5.3.1 Диагностика сети

Вы можете проводить базовую диагностику сети через веб-интерфейс (`Диагностика` → `Сеть`).



Поддерживаются команды `ping`, `curl` и `traceroute`. На вкладке отображается окно для ввода команды и окно вывода, в котором в режиме реального времени отображается процесс выполнения команды. При необходимости можно выгрузить отчет в HTML-формате (кнопка `Сохранить`).

Команды `ping` и `traceroute` поддерживают все стандартные аргументы (см. документацию ping, traceroute на man7.org).

Команда `curl` имеет ограничения:

- Разрешены все поддерживаемые протоколы, кроме *file* (см. документацию curl на man7.org).
- Разрешены только следующие аргументы:
  - `--v` (`--verbose`)
  - `--s` (`--silent`)
  - `--S` (`--show-error`)
  - `--i` (`--include`)
  - `--I` (`--head`)
  - `--L` (`--location`)
  - `--k` (`--insecure`)
  - `--m` (`--max-time`)
  - `--x` (`--proxy`)
  - `--u` (`--user`)
  - `--H` (`--header`)
  - `--A` (`--user-agent`)
  - `--e` (`--referer`)
  - `--d` (`--data`)
  - `--b` (`--cookie`)
  - `--G` (`--get`)
  - `--X` (`--request`)
  - `--w` (`--write-out`)

Примеры:

```
curl https://example.com      # проверка доступности веб-сервиса по HTTP/HTTPS
ping 192.0.2.10              # проверка сетевой доступности узла и времени отклика
traceroute 192.0.2.10        # определение маршрута до удаленного узла
```

Примечание

Также доступна расширенная диагностика через CLI (контекст *diagnostics*, поддерживаемые команды: `arping`, `diag`, `nslookup`, `ping`, `pingc`, `ss`, `ssldump`, `tcpdump`, `traceroute`).

5.3.2 Диагностика через CLI

Диагностические данные о работе системы можно получить через CLI.

Для этого:

1. Подключитесь к *CLI Angie ADC*.

2. Перейдите в контекст `diagnostics` и выполните команду `diag`.

Команда собирает системные метрики, конфигурацию системы и системный журнал за последние 24 часа и сохраняет их в файл `diag_<timestamp>.log` в каталоге `/var/transfer`.

Подробнее о расширенной диагностике см. справочник *diagnostics*.

> **Примечание**
>
> Если веб-интерфейс и CLI недоступны, используйте *аварийный сбор данных*.

5.3.3 Аварийная диагностика

Если веб-интерфейс и CLI Angie ADC недоступны, вы можете скачать архив с диагностической информацией через мастер настройки. Аварийную выгрузку необходимо выполнять отдельно на каждом узле Angie ADC.

Предусловия:

- Есть доступ к консоли виртуальной машины Angie ADC через гипервизор.
- Есть сетевая связность с Angie ADC.
- На Angie ADC настроен и доступен по сети хотя бы один IP-адрес.

Чтобы получить архив:

1. Войдите *в мастер настройки*.
2. В основном меню выберите пункт `emergency_diag`.

   Команда соберет системные метрики, конфигурацию системы и системный журнал и сформирует архив.
3. Дождитесь создания архива. После этого в мастере отобразятся имя архива, порт SFTP и срок, в течение которого архив доступен для скачивания (15 минут). Через 15 минут архив будет удален.

   > **Примечание**
   >
   > При повторном запуске команды `emergency_diag` в течение 15 минут текущий архив будет удален и будет создан новый архив.

4. Подключитесь по SFTP под учетной записью `setup`:

   ```
   $ sftp -P 2223 setup@<IP-адрес>
   ```

   > **Примечание**
   >
   > Если был настроен интерфейс управления, используйте его IP-адрес.

5. Проверьте наличие архива (команда `ls`) и скачайте его:

   ```
   sftp> get diag_YYYYMMDD_HHMMSS.tar.gz
   ```

См. также *Диагностика через CLI*.

5.3.4 Журналы событий и экспорт

Angie ADC записывает все события системы и действия пользователей в веб-интерфейсе в журналы событий. Вы можете просмотреть журналы событий через CLI и настроить отправку событий на удаленный syslog-сервер для дальнейшего анализа и аудита.

5.3.4.1 Просмотр журналов событий

Журналы событий Angie ADC можно посмотреть через *CLI*.

Синтаксис: `logs <entity> [{follow|transfer}]`.

Поддерживается *фильтрация*.

Значения для `<entity>`:

`aaa-manager`	События модуля, отвечающего за аутентификацию и авторизацию внешних пользователей Angie ADC
`adc-gslb`	События модуля GSLB (глобальная балансировка)
`adc-server`	События модуля, обеспечивающего выполнение всего предоставляемого функционала Angie ADC (входная точка)
`adc-system`	События модуля, отвечающего за выполнение системных команд Angie ADC
`adc-tracker`	События модуля, отвечающего за RHI-функционал
`auth-dataplane`	События модуля, отвечающего за *аутентификацию клиентов* в балансировщике нагрузки
`certificate-manager`	События сервиса управления сертификатами
`ctrl-access`	События из access_log модуля, отвечающего за кластерное взаимодействие
`ctrl-error`	События из error_log модуля, отвечающего за кластерное взаимодействие
`gslb-component`	События модуля конфигурации GSLB
`kern`	События ядра
`lb-access`	События из access_log балансировщика нагрузки
`lb-error`	События из error_log балансировщика нагрузки

`lb-ls`	Позволяет получить список журналов балансировщика нагрузки (файлы должны иметь расширение `.log`)
	Пример:
	`$$ logs lb-ls`
	`access.log`
	`error.log`
	`healthmonitoring.log`
	`$$`

`mgmt-access`	События из access_log модуля, отвечающего за управление Angie ADC
`mgmt-error`	События из error_log модуля, отвечающего за управление Angie ADC
`session-store`	События модуля, отвечающего за хранение sticky-сессий в паре высокой доступности
`snmp-manager`	События модуля SNMP
`storage`	События из storage_log модуля, отвечающего за управление Angie ADC
`supervisor`	События модуля, отвечающего за управление кластеризацией Angie ADC
`upgrade`	События обновления Angie ADC
`view <filename>`	Позволяет просмотреть произвольный журнал событий, например, добавленный вручную в настройках конфигурации балансировщика. Файл должен находиться в папке `/var/log/angie-lb/` и иметь расширение `.log`. Пример: `$$ logs view error.log`

Дополнительные параметры:

`follow`	Вывод записей в режиме реального времени.
`transfer`	Копирование записей в директорию `transfer`.

5.3.4.2 Экспорт логов

Angie ADC позволяет экспортировать события в работе системы на удаленные серверы по syslog-протоколу. Для работы функциональности необходимо настроить syslog-серверы, на которые будут отправляться события, и указать уровни критичности событий, определяющие, какие события будут отправляться на удаленный сервер.

Поддерживаются следующие уровни критичности событий:

- `EMERGENCY` — только события, приводящие к аварийной ситуации и полному отказу системы.
- `ALERT` — критические ошибки безопасности или выход из строя важных сервисов.
- `CRITICAL` — серьезные проблемы, которые требуют немедленного исправления.
- `ERROR` — ошибки, влияющие на работу системы, но не приводящие к ее остановке.
- `WARNING` — предупреждения о возможных проблемах.
- `NOTICE` — уведомления о событиях.
- `INFO` — информационные сообщения (сообщения аудита дополнительно имеют помету `audit`).
- `DEBUG` — события отладки.

Создание нового syslog-сервера

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Логирование`.

   Откроется окно `Логирование`. В этом окне отображаются настроенные syslog-серверы.

2. Чтобы добавить новый syslog-сервер, нажмите `Добавить сервер`. В открывшемся окне `Новый сервер` заполните следующие поля:

   - Имя сервера (до 255 символов).
   - Доменное имя или IP-адрес (до 255 символов).
   - Порт (по умолчанию используется 514).
   - Протокол: `TCP` или `UDP` (по умолчанию: `UDP`).
   - Уровни критичности: выберите уровни критичности событий, определяющие, какие события будут отправляться на сервер (доступные уровни см. выше).

3. Нажмите `Добавить сервер`.

   Новый сервер отобразится в списке настроенных syslog-серверов.

4. Чтобы протестировать соединение с новым сервером, нажмите на имя этого сервера в таблице. Откроется окно с параметрами выбранного сервера.

5. Нажмите `Проверить соединение`. В случае установки соединения отобразится сообщение `Подключение прошло успешно`.

Просмотр настроенных syslog-серверов

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Логирование`.

   Откроется окно `Логирование`. В этом окне отображаются настроенные syslog-серверы.

2. Нажмите на конкретный сервер, чтобы просмотреть его параметры.

Изменение параметров syslog-сервера

1. В веб-интерфейсе перейдите в раздел `Система` → `Логирование` → `<имя_сервера>`.

   Откроется окно с параметрами выбранного сервера.

2. Чтобы включить или выключить передачу событий на выбранный syslog-сервер, переведите переключатель `Включить` в соответствующее положение.

3. Чтобы изменить параметры сервера, внесите необходимые правки и нажмите `Сохранить`.
4. Чтобы протестировать соединение с сервером, нажмите `Проверить соединение`.
5. Чтобы удалить сервер, нажмите значок удаления напротив этого сервера.

CLI

Можно выполнять следующие операции:

- Создание syslog-сервера.
- Получение списка syslog-серверов.
- Изменение параметров syslog-сервера.
- Удаление syslog-сервера.
- Проверка подключения к syslog-серверу.

Доступные команды CLI см. в описании команды *syslog*.

5.3.5 Техническая поддержка

Если у вас возникла техническая проблема, но нужное решение не удалось найти в других разделах, задайте нам вопрос на форуме сообщества или в Telegram-канале.

Техническая поддержка для клиентов:

- https://support.angie.software
- support@angie.software

Примечание

Документация Angie ADC доступна в машиночитаемом виде для LLM-инструментов (`llms.txt`, `llms-full.txt`, Markdown-версии страниц) — подробности в разделе ИИ-документация. Карточка Angie ADC в реестре Context7: https://context7.com/websites/angie_software_adc.

ГЛАВА 6

Администрирование и безопасность

Здесь описывается администрирование и обеспечение безопасности Angie ADC: системные настройки (включая HTTPS и сертификаты), кластеризация, сеть узлов и домены маршрутизации, управление пользователями и доступами, а также резервное копирование и восстановление узлов.

В этом разделе:

- *Настройка системы*
- *Управление кластером*
- *Сеть и домены маршрутизации*
- *Управление пользователями и доступами*
- *Резервное копирование и восстановление системы*

6.1 Настройка системы

Здесь описываются общие системные настройки Angie ADC: имя устройства и другие параметры конфигурации, включение HTTPS и загрузка сертификатов, синхронизация времени по NTP, управление базами GeoIP.

В этом разделе:

- *Смена имени устройства*
- *Настройка HTTPS*
- *Управление сертификатами*
- *Настройка NTP*
- *Базы GeoIP*

6.1.1 Смена имени устройства

Имя устройства Angie ADC (hostname) задается при развертывании системы. В дальнейшем имя устройства отображается в верхней части экрана веб-интерфейса. Настройки хранятся в *кластерной конфигурации*.

6.1.1.1 Изменение имени устройства

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Конфигурация`.
2. В поле `Hostname (имя устройства)` введите новое имя устройства и нажмите `Сохранить`.

6.1.1.2 CLI

Можно выполнять следующие операции:

- Получение имени устройства.
- Изменение имени устройства.

Доступные команды CLI см. в описании команды *set (CLI)*.

6.1.1.3 Мастер настройки

Можно выполнять следующие операции:

- Просмотр имени устройства.
- Изменение имени устройства.

Подробнее см. *Мастер настройки по SSH*.

6.1.2 Настройка HTTPS

Angie ADC поддерживает загрузку сертификата управления (management) для защищенного подключения к веб-интерфейсу Angie ADC (HTTPS). По умолчанию используются порты 8080/8443, их можно *поменять*. Поддерживается загрузка и использование только одного сертификата управления (management). При загрузке нового сертификата предыдущий автоматически удаляется.

> **Примечание**
>
> Для работы с сертификатами через веб-интерфейс необходимо предварительно создать кластер Angie ADC. Подробнее см. в статье *Создание и масштабирование кластера*.

6.1.2.1 Загрузка сертификата управления и включение защищенного соединения

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Конфигурация`.
2. В блоке `Управление HTTPS` нажмите `Загрузить сертификат и включить HTTPS`.
3. В открывшемся окне введите данные сертификата и ключа в формате PEM вручную или загрузите их из файлов по кнопке `Загрузить из файла`.
4. Нажмите `Загрузить`.

   Сертификат будет загружен. В блоке `Управление HTTPS` будет отображаться статус HTTPS (`выключен`) и данные о сертификате: дата загрузки и срок действия.
5. Нажмите `Включить HTTPS`, чтобы включить использование защищенного соединения. После этого веб-интерфейс автоматически откроется по HTTPS.

Сертификат управления и ключ можно также загружать *через CLI*.

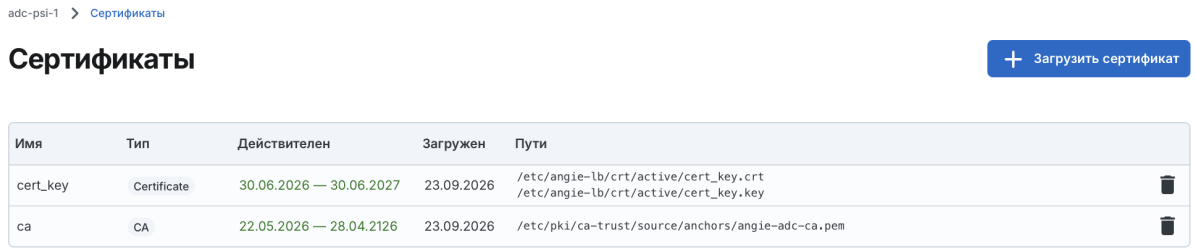
6.1.3 Управление сертификатами

Angie ADC поддерживает загрузку сертификатов через веб-интерфейс (`Система` → `Сертификаты`). Можно загружать:

- сертификаты для обработки TLS-соединений балансируемого трафика; в систему можно загрузить несколько сертификатов такого типа, поддерживается загрузка бандла сертификатов;

- доверенные корневые и промежуточные сертификаты (CA): используются при проверке сертификатов удаленных сервисов при исходящих TLS-подключениях, например при подключении к корпоративному LDAP по LDAPS; каждый доверенный сертификат загружается отдельно, загрузка бандла из нескольких доверенных сертификатов не поддерживается.

Набор загруженных сертификатов распространяется на все узлы кластера.



6.1.3.1 Загрузка сертификата данных

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Сертификаты`.
2. Нажмите `Загрузить сертификат` и заполните следующие поля:
   - `Имя сертификата` — произвольное имя сертификата, которое будет отображаться в системе.
   - `Тип` — `Certificate` для сертификата данных.
   - `Сертификат` — содержимое файла сертификата.
   - `Приватный ключ` — содержимое файла приватного ключа.

   Содержимое сертификата и ключа можно ввести вручную или загрузить из файла по кнопке `Загрузить из файла` под соответствующим полем.
3. Нажмите `Загрузить`.

Сертификат будет загружен. На странице `Сертификаты` будут отображаться данные о сертификате: имя, тип, срок действия, дата загрузки и пути к сертификату и ключу.

> **Примечание**
>
> После загрузки сертификата необходимо вручную настроить его использование в *конфигурации балансировщика нагрузки*.

Например:

```
server {
    listen       80;
    listen       [::]:80;
    listen       443 ssl;
    listen       [::]:443 ssl;
    server_name  localhost;

    ssl_protocols       TLSv1.2 TLSv1.3;
    ssl_ciphers         ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
↪SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384;
    ssl_certificate     /etc/angie-lb/crt/active/example.crt;
    ssl_certificate_key /etc/angie-lb/crt/active/example.key;
    ssl_session_cache   shared:SSL:10m;
    ssl_session_timeout 10m;
```

```
    if ($scheme = http) {
        return 301 https://$host:443$request_uri;
    }

    ## location
}
```

6.1.3.2 Загрузка доверенного сертификата

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Сертификаты`.
2. Нажмите `Загрузить сертификат` и заполните следующие поля:
   - `Имя сертификата` — произвольное имя сертификата, которое будет отображаться в системе.
   - `Тип` — `CA` для доверенного сертификата.
   - `Сертификат` — содержимое файла сертификата (PEM).

   Содержимое сертификата можно ввести вручную или загрузить из файла по кнопке `Загрузить из файла` под полем.
3. Нажмите `Загрузить`.

Сертификат будет загружен. На странице `Сертификаты` будут отображаться данные о сертификате: имя, тип, срок действия, дата загрузки и путь к сертификату.

6.1.3.3 Удаление сертификатов

Чтобы удалить сертификат:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Сертификаты`. Откроется список сертификатов.
2. Нажмите значок удаления рядом с сертификатом, который вы хотите удалить.

Сертификат будет удален из списка.

6.1.3.4 Управление через CLI

Сертификаты можно также загружать и просматривать через CLI:

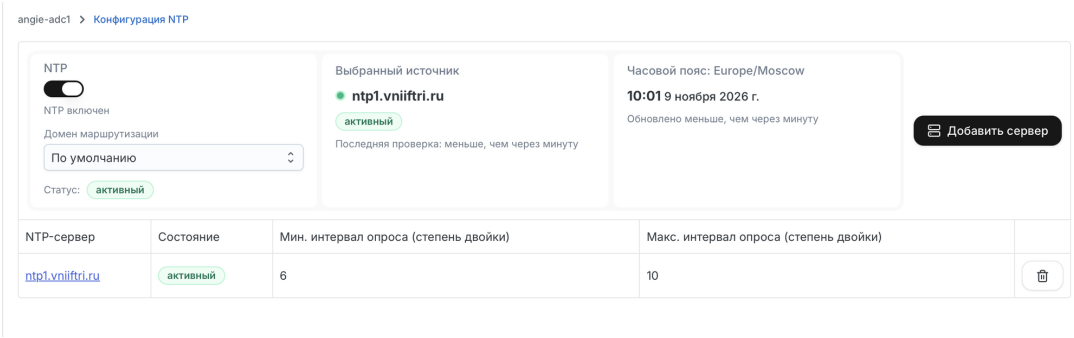
- *Сертификаты данных*
- *Доверенные сертификаты*

6.1.4 Настройка NTP

NTP (Network Time Protocol) позволяет синхронизировать системное время на всех компонентах системы Angie ADC. Вы можете добавить один или несколько NTP-серверов, которые будут использоваться как источники времени. В случае, если ни один из настроенных NTP-серверов не отвечает, система попробует синхронизировать время на текущем узле по одному из других узлов кластера. В качестве выбранного источника будет отображаться IP-адрес этого узла. Настройки хранятся в *кластерной конфигурации*.

Важно

Синхронизация времени на узлах с единым источником критически важна для работы *кластера*.



6.1.4.1 Настройка конфигурации NTP

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `NTP`.

   Откроется окно `Конфигурация NTP`.

2. Включите переключатель `NTP`, чтобы запустить службу синхронизации NTP.

3. Если NTP-серверы должны быть доступны только через домен маршрутизации, выберите его в списке `Домен маршрутизации` под переключателем `NTP`. Домен один для всех NTP-серверов; значение `По умолчанию` означает общую сеть.

4. Чтобы добавить NTP-сервер, нажмите `Добавить сервер` и заполните необходимые поля:

   - Адрес NTP-сервера, например `ntp1.vniiftri.ru`.
   - Минимальный и максимальный интервалы для частоты опроса сервера. Частота опроса может меняться динамически: при нестабильном времени сервер опрашивается чаще, при стабильной синхронизации — реже.

     В качестве значения указывается степень двойки, интервал опроса NTP-сервера рассчитывается как 2 в степени n секунд.

     Например:

     – `6` → 2^6 = 64 секунды;

     – `10` → 2^10 = 1024 секунды (~17 минут).

5. Установите флажок `NTS`, если хотите использовать аутентифицированную синхронизацию времени. Если сервер не поддерживает NTS, синхронизация времени будет невозможна, у сервера отобразится статус `NTS не подтвержден`.

6. Нажмите `Добавить`.

Чтобы изменить параметры сервера, нажмите на имя сервера в таблице. Откроется окно с параметрами сервера. Внесите необходимые правки и сохраните изменения.

Чтобы удалить сервер, нажмите значок удаления в таблице напротив этого сервера.

6.1.4.2 Статусы

В интерфейсе Angie ADC отображаются статус службы NTP и состояние серверов (источников времени).

Статусы службы NTP:

- `активный` — служба NTP включена.
- `выключен` — служба NTP выключена.
- `есть проблемы` — возникли проблемы с синхронизацией времени.
- `не отвечает` — служба недоступна.
- `данные устарели` — не удалось получить свежие данные.

- `применение настроек...` — идет применение изменений.

Статусы NTP-серверов:

- `активный` — сервер доступен.
- `есть проблемы` — возникли проблемы с синхронизацией времени.
- `не отвечает` — сервер недоступен.
- `неизвестно` — статус сервера не определен.
- `применение настроек...` — идет применение изменений.
- `NTS не подтвержден` — сервер не поддерживает NTS, синхронизация времени невозможна.

6.1.4.3 CLI

Конфигурацию NTP можно просмотреть и настроить через CLI. Настройка выполняется в контексте `system`. Можно выполнять следующие операции:

- Просмотр конфигурации и статуса NTP (`ntp`).
- Включение NTP (`ntp enable`).
- Выключение NTP (`ntp disable`).
- Добавление или изменение NTP-сервера (`ntp server <host> [minpoll <value>] [maxpoll <value>] [nts]`). Параметр `nts` включает аутентифицированную синхронизацию времени (NTS).
- Удаление NTP-сервера (`ntp remove server <host>`).

Подробнее см. *ntp*.

6.1.5 Базы GeoIP

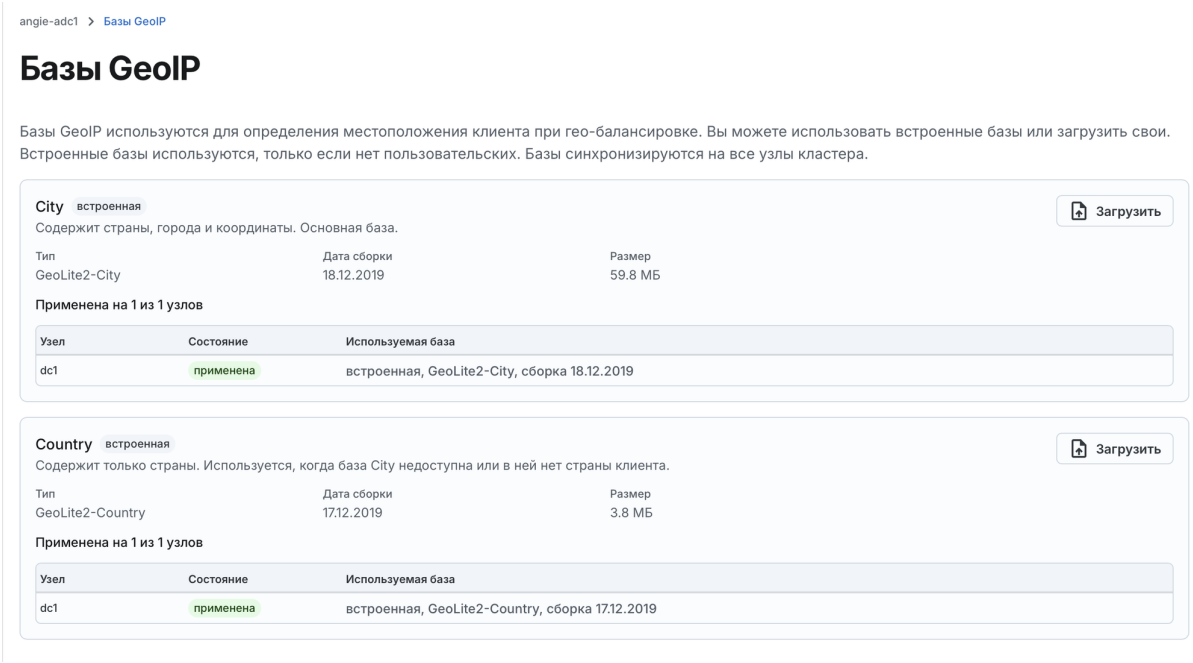
Базы GeoIP используются при глобальной балансировке в режиме *geo-affinity* для определения местоположения клиента.

Angie ADC поставляется со встроенными базами двух типов:

- `City` — основная база, которая позволяет определить страну, город и координаты клиента;
- `Country` — вспомогательная база, которая позволяет определить только страну клиента и используется, если City-база по каким-то причинам недоступна.

> **Совет**
>
> Для более точного определения местоположения клиентов рекомендуется загрузить актуальную пользовательскую базу `City` и обновлять ее самостоятельно, так как базы GeoIP не обновляются автоматически.

Базы синхронизируются на всех узлах кластера.



Для каждой базы отображаются следующие данные:

- источник базы: `пользовательская` или `встроенная`;
- тип базы;
- дата сборки;
- размер базы;
- дата загрузки, если применимо;
- пользователь, выполнивший загрузку, если применимо.

В таблице ниже отображается статистика применения текущей базы на узлах:

- имя узла;
- состояние применения базы;
- имя используемой базы.

6.1.5.1 Загрузка и замена базы

City-базу можно загружать только в блоке `City`. Перед загрузкой убедитесь, что файл и узлы кластера соответствуют требованиям:

- Файл имеет формат MaxMind DB (`.mmdb`).
- Размер файла не превышает 512 МБ.
- На каждом узле кластера достаточно свободного места: необходимо примерно в четыре раза больше места, чем размер самой базы. Система проверяет свободное место только на узле, через который выполняется загрузка.

Примечание

При замене предыдущая загруженная база удаляется.

Чтобы загрузить или заменить базу:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Базы GeoIP`.

2. В блоке `City` нажмите `Загрузить`, если есть только встроенная база, или `Заменить`, если уже есть загруженная пользовательская база.
3. Выберите файл `.mmdb` и подтвердите загрузку.

После загрузки новой базы она начнет использоваться на всех узлах вместо текущей.

Примечание

Синхронизация базы на другие узлы кластера может занять некоторое время, в течение которого узлы могут определять местоположение клиентов по разным базам.

6.1.5.2 Удаление базы

Удалить можно только загруженную базу.

Чтобы удалить загруженную базу:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Базы GeoIP`.
2. Нажмите `Удалить` напротив загруженной базы.
3. Подтвердите удаление.

Загруженная база будет удалена. Для глобальной балансировки на всех узлах начнет использоваться встроенная база.

6.2 Управление кластером

Кластер Angie ADC позволяет настраивать несколько устройств Angie ADC с любого узла через общую кластерную конфигурацию. Данные между узлами кластера синхронизируются и передаются в зашифрованном виде.

В кластерную конфигурацию входят:

- Сетевые настройки каждого узла (сеть, VRRP, маршрутизация, домены маршрутизации);
- конфигурация GSLB;
- сертификаты;
- пользователи SNMP;
- конфигурация мониторинга доступности;
- настройки парольной политики;
- Системные параметры: hostname, timezone, sysctl.

Примечание

Конфигурация локального балансировщика не синхронизируется между узлами кластера.

В этом разделе:

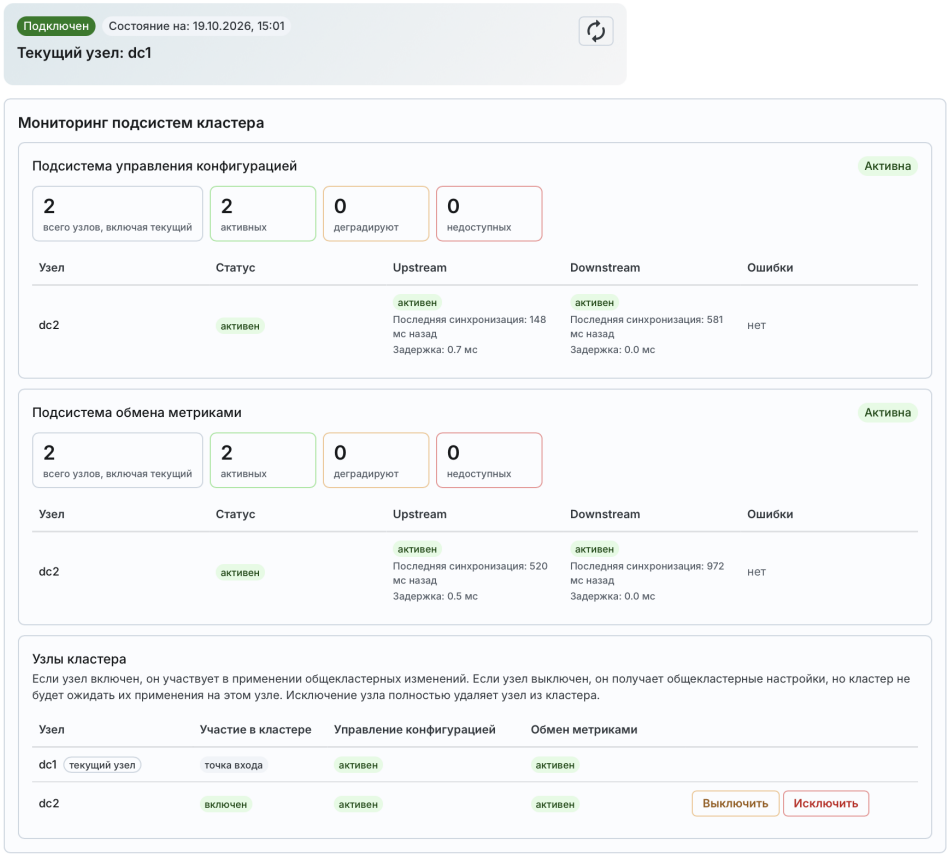
- *Мониторинг состояния кластера*
- *Применение, отмена и откат изменений*
- *Управление составом узлов в кластере*

6.2.1 Мониторинг состояния кластера

Состояние кластера можно просмотреть с любого узла в разделе `Высокая доступность и кластеризация` → `Кластер`.

На странице мониторинга отображается состояние текущего узла и двух подсистем кластера, которые синхронизируются по отдельности:

- В блоке `Подсистема управления конфигурацией` отображается статус синхронизации кластерной конфигурации для пиров текущего узла: подсистема позволяет видеть статус применения изменений в конфигурации по всему кластеру.
- В блоке `Подсистема обмена метриками` отображается статус синхронизации метрик и данных датчиков доступности для пиров текущего узла: подсистема позволяет видеть фактическое состояние кластера: какие узлы работают, а какие нет, независимо от применения конфигурации.



Примечание

На каждом узле будет отображаться состояние кластера по данным этого узла. Если узел потерял связь с кластером, то с этого узла недоступными будут отображаться другие узлы. При этом сами другие узлы будут видеть недоступным только этот узел.

6.2.1.1 Информация о текущем узле кластера

В верхней части экрана отображается информация о текущем узле кластера:

- Имя узла в кластере (может отличаться от `hostname` узла и отображает логическую структуру кластера).
- Статус подключения текущего узла к кластеру:

  - `Ожидает подключения` — узел не входит в кластер.
  - `Подключен` — узел подключен к кластеру.
  - `Подключение...` — выполняется подключение узла к кластеру.

6.2.1.2 Подсистема управления конфигурацией

В блоке `Подсистема управления конфигурацией` отображается состояние подсистемы, синхронизирующей кластерную конфигурацию между узлами, по данным текущего узла:

- Статус подсистемы:
  - `Активна` — подсистема запущена.
  - `Подключение` — выполняется запуск подсистемы.
- Сводная статистика узлов подсистемы:
  - общее число узлов подсистемы;
  - число узлов в рабочем состоянии;
  - число узлов с проблемами синхронизации;
  - число недоступных узлов.
- Таблица с подробной информацией по пирам текущего узла:

`Узел`	Имя узла, входящего в кластер.
`Статус`	– `активен` — узел находится в рабочем состоянии, данные синхронизированы. – `деградирует` — есть проблемы с синхронизацией данных. – `недоступен` — узел недоступен.
`Upstream`	Статус получения данных узлом, время последней синхронизации и задержка: – `активен` — upstream доступен, данные синхронизированы. – `подключение` — выполняется подключение к кластеру. – `синхронизация` — выполняется синхронизация (получение данных узлом). – `недоступен` — upstream недоступен, получение данных невозможно.
`Downstream`	Статус передачи данных узлом, время последней синхронизации и задержка: – `активен` — downstream доступен, данные могут передаваться. – `подключение` — выполняется подключение к кластеру. – `синхронизация` — выполняется синхронизация (передача данных узлом). – `недоступен` — downstream недоступен, передача данных невозможна.
`Последняя синхронизация`	Время, прошедшее с последней синхронизации данных.
`Задержка`	Задержка синхронизации данных на узле.
`Ошибки`	Ошибки синхронизации данных на узле, если есть.

6.2.1.3 Подсистема обмена метриками

В блоке `Подсистема обмена метриками` отображается состояние подсистемы, синхронизирующей между узлами оперативные данные (метрики и результаты проверок доступности), по данным текущего узла:

- Статус подсистемы:
  - `Активна` — подсистема запущена.
  - `Подключение` — выполняется запуск подсистемы.
- Сводная статистика узлов подсистемы:
  - общее число узлов подсистемы;
  - число узлов в рабочем состоянии;
  - число узлов с проблемами синхронизации;
  - число недоступных узлов.
- Таблица с подробной информацией по пирам текущего узла:

`Узел`	Имя узла, входящего в кластер.
`Статус`	– `активен` — узел находится в рабочем состоянии, данные синхронизированы. – `деградирует` — есть проблемы с синхронизацией данных. – `недоступен` — узел недоступен.
`Upstream`	Статус получения данных узлом, время последней синхронизации и задержка: – `активен` — upstream доступен, данные синхронизированы. – `подключение` — выполняется подключение к кластеру. – `синхронизация` — выполняется синхронизация (получение данных узлом). – `недоступен` — upstream недоступен, получение данных невозможно.
`Downstream`	Статус передачи данных узлом, время последней синхронизации и задержка: – `активен` — downstream доступен, данные могут передаваться. – `подключение` — выполняется подключение к кластеру. – `синхронизация` — выполняется синхронизация (передача данных узлом). – `недоступен` — downstream недоступен, передача данных невозможна.
`Последняя синхронизация`	Время, прошедшее с последней синхронизации данных.
`Задержка`	Задержка синхронизации данных на узле.
`Ошибки`	Ошибки синхронизации данных на узле, если есть.

6.2.1.4 Узлы кластера

В блоке `Узлы кластера` отображается список всех узлов кластера и их статусы по данным текущего узла:

`Узел`	Имя узла, входящего в кластер. У текущего узла отображается метка `текущий узел`.
`Участие в кластере`	• `точка входа` — узел, через который происходит управление другими узлами кластера. • `включен` — узел кластера, который участвует в применении общекластерных изменений. • `выключен` — узел кластера, который временно выключен из синхронизации, но получает общекластерные настройки.
`Управление конфигурацией`	Статус узла в подсистеме управления конфигурацией.
`Обмен метриками`	Статус узла в подсистеме обмена метриками.
`Выключить`	Кнопка выключения узла. Выключенный узел будет получать общекластерные настройки, но кластер не будет ожидать их применения на этом узле. Кнопка не отображается для точки входа.
`Включить`	Кнопка включения узла. Включенный узел участвует в применении кластерных изменений. Кнопка не отображается для точки входа.
`Исключить`	Кнопка удаления узла из кластера, например, если узел больше не используется. Кнопка не отображается для точки входа. **Предупреждение** Исключение узла из кластера необратимо. После исключения вы не сможете вернуть узел с тем же именем обратно в кластер.

Подробнее см. *Управление составом узлов в кластере*.

6.2.2 Применение, отмена и откат изменений

В кластерную конфигурацию входят:

- Сетевые настройки каждого узла (сеть, VRRP, маршрутизация, домены маршрутизации);
- конфигурация GSLB;
- сертификаты;
- пользователи SNMP;
- конфигурация мониторинга доступности;
- настройки парольной политики;
- Системные параметры: hostname, timezone, sysctl.

После внесения кластерных изменений на одном из узлов кластера они автоматически применяются на всех остальных узлах кластера.

Важно

Если планируются значительные изменения, рекомендуется предварительно создать или обновить *резервную копию узла*.

6.2.2.1 Применение изменений

Каждое изменение кластерной конфигурации проверяется, затем синхронизируется на все узлы кластера. Одновременно может применяться только одно изменение. Неприменившееся изменение повторяется и блокирует следующие изменения, пока оно не будет отменено или не будет устранена причина, блокирующая его применение.

Изменение в кластерной конфигурации может примениться, только когда все включенные узлы кластера доступны. Рекомендуется ввести в строй или выключить недоступные узлы перед внесением изменений в кластерную конфигурацию.

> **Совет**
>
> Если кластерное изменение было заблокировано в процессе применения новой конфигурации, так как один из узлов перестал отвечать, можно *выключить этот узел*. После этого обновление конфигурации завершится успешно. Выключенный узел получит новую конфигурацию, когда станет доступен. Затем его снова можно включить.

6.2.2.2 Отмена изменений

В случае, если применение изменений в кластере по каким-то причинам занимает долгое время, вы можете отменить применение новой конфигурации, нажав кнопку `Отменить изменения` в окне, информирующем о внесении изменений.

6.2.2.3 Откат изменений

Если перед внесением изменений была создана или обновлена *резервная копия узла*, то уже примененную конфигурацию можно откатить, восстановив узел из резервной копии.

6.2.3 Управление составом узлов в кластере

Состав кластера Angie ADC можно менять — подключать новые узлы, включать или выключать имеющиеся узлы, а также исключать узлы, которые больше не используются.

> **Важно**
>
> Включение, выключение и исключение узла не поддерживаются для узла, который является точкой входа в кластер.

6.2.3.1 Добавление узлов

Чтобы добавить новый узел в кластер, выполните его первоначальную настройку и затем подключите его к кластеру. Подробнее см. *Добавление узлов в кластер*.

6.2.3.2 Включение и выключение узлов

Вы можете применять новую конфигурацию в кластере, даже если часть узлов недоступна, неисправна или находится на обслуживании. Для этого необходимо выключить недоступные узлы, не исключая их из кластера. Выключенные узлы получают общекластерные настройки, но кластер не ожидает их применения на выключенных узлах. При этом настройки, относящиеся только к самим узлам, остаются доступными для изменения.

Чтобы выключить узел:

1. Откройте веб-интерфейс Angie ADC на любом другом узле кластера и перейдите в раздел `Высокая доступность и кластеризация` → `Кластер`.
2. В блоке `Узлы кластера` выберите нужный узел и нажмите `Выключить` напротив него.

3. Подтвердите операцию.

   Узел будет выключен.

Чтобы включить узел:

1. Откройте веб-интерфейс Angie ADC на любом другом узле кластера и перейдите в раздел `Высокая доступность и кластеризация` → `Кластер`.
2. В блоке `Узлы кластера` выберите нужный узел и нажмите `Включить` напротив него.
3. Подтвердите операцию.

   Узел будет включен.

Примечание

Выключенный узел можно также включить в веб-интерфейсе этого узла по кнопке `Включить этот узел` в верхней части экрана.

6.2.3.3 Исключение узлов

Предупреждение

Исключение узла из кластера необратимо. После исключения вы не сможете вернуть узел с тем же именем обратно в кластер. Если необходимо временно отключить узел от кластера, сохранив его, выключите его (см. *Включение и выключение узлов*).

Чтобы исключить узел из кластера:

1. Откройте веб-интерфейс Angie ADC на любом другом узле и перейдите в раздел `Высокая доступность и кластеризация` → `Кластер`.
2. В блоке `Узлы кластера` выберите узел, который вы хотите исключить, и нажмите `Исключить` напротив этого узла.
3. Подтвердите операцию.

   Узел будет исключен из кластера. В веб-интерфейсе исключенного узла будет отображаться информация о недоступности кластера.

6.3 Сеть и домены маршрутизации

Сеть узла можно настроить в веб-интерфейсе Angie ADC (`Система` → `Сетевые настройки`), через *мастер* или через *CLI*. Сетевые настройки каждого узла применяются и хранятся в *кластерной конфигурации*. Настройку можно проводить с любого узла кластера. Поддерживается выделение доменов маршрутизации для управления, передачи данных, служебных обращений Angie ADC и глобальной балансировки.

Примечание

VRRP, BGP и OSPF настраиваются только через команды *CLI*. В CLI также задается часть сетевых настроек: IPv4-адреса, шлюз и DNS интерфейсов, VLAN, MTU, бонды, статические маршруты и правила маршрутизации (см. *set*). Домены маршрутизации создаются в веб-интерфейсе или мастере, утечки маршрутов и IPv6-адреса задаются только в веб-интерфейсе.

Возможности сетевой настройки в веб-интерфейсе:

- *Настройка интерфейсов, VLAN и бондов*;

- *Просмотр настроенных групп VRRP*;
- *Настройка доменов маршрутизации*;
- *Настройка маршрутов и правил маршрутизации*;
- *Настройка утечек маршрутов*;
- *Настройка DNS-резолверов*.

Важно

Не рекомендуется задавать сетевые настройки в обход Angie ADC, так как при следующем применении кластерной конфигурации они будут перезаписаны.

6.3.1 Примеры сетевых схем

Ниже приведены примеры схем сетевой настройки узла:

- **Минимальный вариант: отдельная сеть только для управления**

  Один интерфейс помещен в домен `mgmt`. Веб-интерфейс, CLI и SSH будут доступны только через этот домен. Все остальные интерфейсы находятся в общей сети.

  Порядок настройки см. *Настройка сети управления*.

- **Отдельные сети для управления и служебных обращений**

  Один интерфейс помещен в домен `mgmt` для управления. Обращения узла к инфраструктуре вынесены в отдельный домен маршрутизации. Поддерживается для NTP, DNS, серверов аутентификации клиентов, SNMP, датчиков доступности, резервной копии балансировщика в S3. Домен маршрутизации выбирается в каждом сервисе отдельно, поэтому служебных доменов маршрутизации может быть несколько.

  Порядок настройки см. *Привязка сервисов Angie ADC к домену маршрутизации*.

- **Отдельные сети для управления и изоляции внешнего и внутреннего клиентского трафика**

  Один интерфейс помещен в домен `mgmt` для управления. Внешний клиентский трафик идет в отдельный домен маршрутизации, затем балансировщик нагрузки проксирует его во внутренний домен с бэкендами.

  Пример настройки см. *Изоляция внешнего трафика и проксирование во внутреннюю сеть*.

- **Глобальная балансировка в нескольких доменах маршрутизации**

  Узел принимает DNS-запросы клиентов из разных сетей на разных адресах в разных доменах маршрутизации. Запрос из одной сети к адресу в другом домене маршрутизации не проходит. В блоке `IP-адреса ADNS` для такого узла задается несколько строк, по одной на каждый домен маршрутизации, например `По умолчанию`, `blue` и `red`.

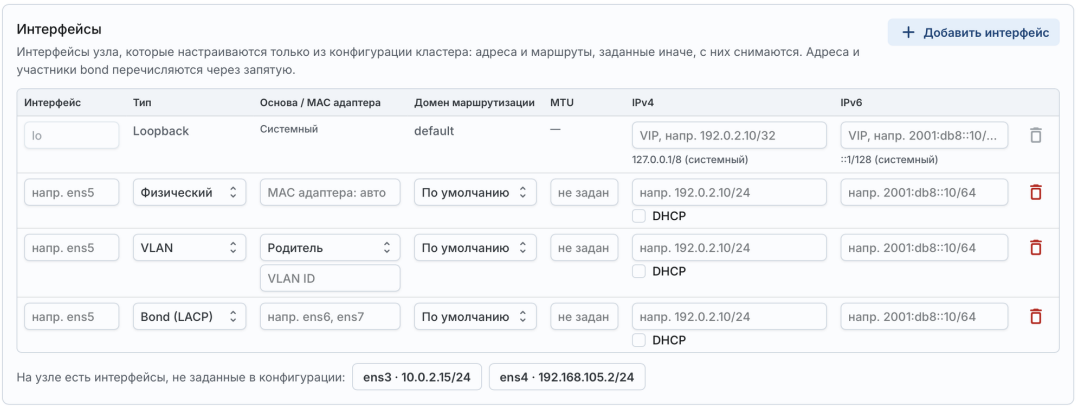
  Порядок настройки см. *Настройка IP-адресов ADNS*.

6.3.1.1 Настройка сетевых интерфейсов

Сеть узла Angie ADC можно просматривать и настраивать через веб-интерфейс на любом узле кластера (`Система` → `Сетевые настройки`). Настройки каждого узла хранятся и применяются через *кластерную конфигурацию*.

Важно

Не рекомендуется задавать сетевые настройки в обход Angie ADC, так как при следующем применении кластерной конфигурации они будут перезаписаны.



Интерфейсы

В блоке **Интерфейсы** можно настроить интерфейсы узла. Интерфейсы узла, еще не заданные в конфигурации, показаны под таблицей. Они не входят в кластерную конфигурацию и не меняются при применении кластерной конфигурации.

> **Примечание**
>
> После того как интерфейс добавлен в таблицу и новая конфигурация сохранена, этот интерфейс будет полностью управляться через кластерную конфигурацию. Адреса и маршруты, заданные на нем другим способом (не через Angie ADC), будут удалены при следующем применении конфигурации.

Для интерфейса задаются следующие параметры:

- **Интерфейс** — имя интерфейса Linux (до 15 байт), например **ens5**. Имя не должно совпадать с именем домена маршрутизации.
- **Тип** — **Физический**, **VLAN** или **Bond (LACP)**; у интерфейса **lo** — **Loopback**.
- **Основа / MAC адаптера** — зависит от типа интерфейса: для физического интерфейса — MAC-адрес сетевого адаптера (если не задан, определяется автоматически); для VLAN — родительский интерфейс и VLAN ID; для бонда — участники бонда через запятую. Имя физического интерфейса закрепляется за адаптером по MAC-адресу и не меняется при перестановке адаптеров.
- **Домен маршрутизации** — домен маршрутизации интерфейса. По умолчанию используется общая сеть.

  > **Важно**
  >
  > Интерфейс с адресом, по которому узел подключен к кластеру, должен оставаться в общей сети.

- **MTU** — максимальный размер пакета, от 68 до 65536. Значение «не задан» означает, что используется системное значение (обычно 1500).
- **IPv4** и **IPv6** — адреса в формате CIDR через запятую.
- **DHCP** — флажок под полем **IPv4** для получения IPv4-адреса от DHCP-сервера. IPv6-адреса задаются только вручную.

Настройка сетевого интерфейса

Чтобы настроить сетевой интерфейс:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо настроить интерфейс.
3. В блоке `Интерфейсы` нажмите `Добавить интерфейс`.
4. В поле `Интерфейс` укажите имя интерфейса узла, например `ens5`. Имена интерфейсов, еще не заданных в конфигурации, но имеющихся на узле, предлагаются в подсказках.
5. В поле `Тип` выберите `Физический`.
6. При необходимости в поле `Основа / MAC адаптера` укажите MAC-адрес сетевого адаптера. Если адрес не указан, адаптер определяется автоматически.
7. В поле `IPv4` задайте адреса вручную или установите флажок `DHCP`, в поле `IPv6` задайте адреса вручную.
8. При необходимости задайте `MTU` и выберите домен маршрутизации в раскрывающемся списке `Домен маршрутизации`.
9. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения в сетевой конфигурации узла.

Создание бонда

При создании бондов используется протокол LACP (802.3ad) и режим active (интерфейс инициирует создание агрегированного канала).

Чтобы объединить несколько физических интерфейсов в один логический интерфейс (бонд):

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо создать бонд.
3. В блоке `Интерфейсы` нажмите `Добавить интерфейс`.
4. В поле `Интерфейс` укажите имя бонда, например `bond0`.
5. В поле `Тип` выберите `Bond (LACP)`.
6. В поле `Основа / MAC адаптера` перечислите через запятую интерфейсы, которые необходимо объединить (максимум 8 интерфейсов). Участниками бонда могут быть только физические интерфейсы без своего домена маршрутизации и адресов; каждый интерфейс может входить только в один бонд.
7. Задайте адреса бонда в полях `IPv4` и `IPv6` и при необходимости — `MTU` и `Домен маршрутизации`.
8. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения в сетевой конфигурации узла.

Создание VLAN-интерфейса

Чтобы создать VLAN-интерфейс:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо создать VLAN-интерфейс.
3. В блоке `Интерфейсы` нажмите `Добавить интерфейс`.
4. В поле `Интерфейс` укажите имя VLAN-интерфейса, например `vl500`.
5. В поле `Тип` выберите `VLAN`.
6. В поле `Основа / MAC адаптера` выберите родительский интерфейс (физический интерфейс или бонд) и укажите VLAN ID (от 1 до 4094).

7. Задайте адреса VLAN-интерфейса в полях `IPv4` и `IPv6` и при необходимости — `MTU` и `Домен маршрутизации`.
8. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения в сетевой конфигурации узла.

Просмотр настроенных сетевых интерфейсов

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, интерфейсы которого вы хотите просмотреть.

   В блоке `Интерфейсы` отображается таблица интерфейсов, заданных в конфигурации узла.

   Под таблицей перечислены интерфейсы узла, не заданные в конфигурации, с их текущими адресами.

Просмотр групп VRRP

Группы VRRP настраиваются в CLI командами `vrrp` (подробнее см. *VRRP*). В веб-интерфейсе их можно только просматривать.

Чтобы просмотреть группы VRRP:

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, группы VRRP которого вы хотите просмотреть.

   В блоке `Группы VRRP` отображается таблица групп со следующими столбцами:

   - `Интерфейс` — интерфейс, на котором настроена группа VRRP;
   - `VRID` — идентификатор группы VRRP;
   - `Адрес` — виртуальный IPv4-адрес группы с длиной префикса, например `198.18.5.100/24`.

Изменение параметров сетевого интерфейса

Предупреждение

Не рекомендуется изменять настройки интерфейсов узлов, объединенных в пару высокой доступности, иначе пара может потерять связность и работоспособность. Интерфейс, на котором настроена группа VRRP, нельзя удалить или переименовать.

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо изменить интерфейс.
3. В блоке `Интерфейсы` измените нужные параметры в строке интерфейса.
4. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения в сетевой конфигурации узла.

Удаление сетевого интерфейса

Предупреждение

Не рекомендуется изменять настройки интерфейсов узлов, объединенных в пару высокой доступности, иначе пара может потерять связность и работоспособность. Интерфейс, на котором настроена группа VRRP, нельзя удалить или переименовать.

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо удалить интерфейс.
3. В блоке `Интерфейсы` нажмите значок удаления напротив строки нужного интерфейса.
4. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения в сетевой конфигурации узла.

Адреса сервисов на интерфейсе lo

Интерфейс `lo` всегда есть в таблице с типом `Loopback`. Его системные адреса `127.0.0.1/8` и `::1/128` не меняются; дополнительно на нем можно задать адреса сервисов (VIP), которые не принадлежат ни одной подсети интерфейсов. IPv4-адреса сервисов можно анонсировать по *BGP* или *OSPF*; на любой адрес сервиса, в том числе IPv6, маршрутизатор может направлять статический маршрут.

Для `lo` доступны только дополнительные статические адреса:

- IPv4 — только с префиксом `/32`, IPv6 — только с префиксом `/128`;
- допускается любой одноадресный адрес, в том числе частный; нельзя задать адреса `0.0.0.0` и `::`, loopback, multicast, link-local и широковещательный адрес;
- MAC-адрес, MTU, домен маршрутизации, DHCP и шлюз не задаются;
- `lo` нельзя удалить, сделать родителем VLAN или участником бонда, использовать для группы VRRP.

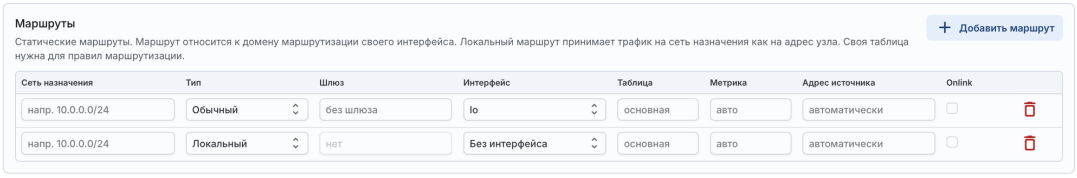
Чтобы задать адрес, в строке `lo` укажите его в поле `IPv4` или `IPv6`, например `192.0.2.10/32`, и нажмите `Применить`.

6.3.1.2 Настройка маршрутизации

Маршрутизацию узлов можно просматривать и настраивать через веб-интерфейс на любом узле кластера (`Система` → `Сетевые настройки`). Настройки каждого узла хранятся и применяются через *кластерную конфигурацию*.

Маршруты

В блоке `Маршруты` задаются статические маршруты.



Чтобы добавить маршрут:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо добавить маршрут.
3. В блоке `Маршруты` нажмите `Добавить маршрут`.
4. В поле `Сеть назначения` укажите адрес сети в формате CIDR (например, `10.0.0.0/24`) и выберите тип маршрута в поле `Тип`: `Обычный` — для маршрута через шлюз или интерфейс, `Локальный` — чтобы узел принимал трафик к этой сети как к своему адресу.
5. В поле `Интерфейс` выберите интерфейс, через который идет маршрут. Для локального маршрута используйте значение `Без интерфейса`.
6. При необходимости в поле `Шлюз` укажите адрес шлюза.

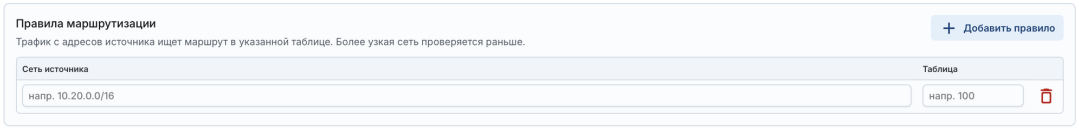
7. При необходимости заполните поля `Таблица`, `Метрика`, `Адрес источника` и установите признак `Onlink`.

   Номер таблицы можно указать только для маршрута через интерфейс без домена маршрутизации: маршрут через интерфейс домена маршрутизации попадает в таблицу этого домена. Номера таблиц 0, 253–255 и 10000–10999 зарезервированы: диапазон 10000–10999 занят таблицами доменов маршрутизации.

8. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

Правила маршрутизации

В блоке `Правила маршрутизации` можно настроить перенаправление трафика с указанных адресов источника в заданную таблицу маршрутизации. Более узкая сеть источника проверяется раньше. Маршруты в эту таблицу добавляются в блоке `Маршруты` с номером таблицы в поле `Таблица` (см. *Маршруты*).

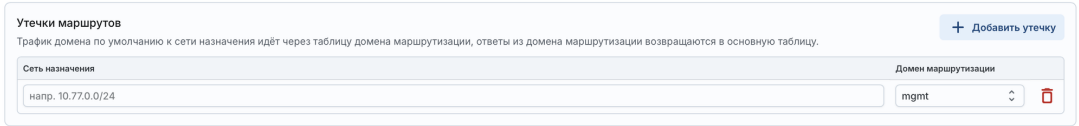


Чтобы добавить правило маршрутизации:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо добавить правило.
3. В блоке `Правила маршрутизации` нажмите `Добавить правило`.
4. В поле `Сеть источника` укажите сеть в формате CIDR.
5. В поле `Таблица` укажите номер таблицы маршрутизации (кроме 0, 253–255 и 10000–10999), в которой будет искаться маршрут для трафика из этой сети.
6. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

Настройка утечек маршрутов

В блоке `Утечки маршрутов` настраивается доступ из общей сети в заданный домен маршрутизации: трафик к указанной сети назначения идет через таблицу домена, а ответы из домена возвращаются в основную таблицу.



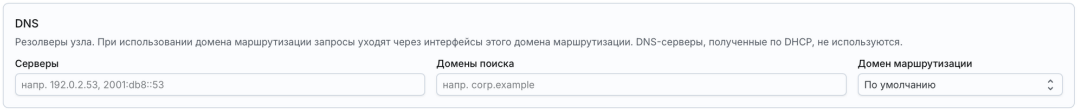
Чтобы добавить утечку маршрута:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо настроить утечку маршрута.
3. В блоке `Утечки маршрутов` нажмите `Добавить утечку`.
4. В поле `Сеть назначения` укажите сеть в формате CIDR, к которой нужен доступ из общей сети.
5. В раскрывающемся списке `Домен маршрутизации` выберите домен маршрутизации, через таблицу которого должен идти трафик к этой сети.
6. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

6.3.1.3 Настройка DNS-резолверов

DNS-резолверы для каждого узла можно просматривать и настраивать через веб-интерфейс на любом узле кластера (`Система` → `Сетевые настройки`). Настройки каждого узла хранятся и применяются через *кластерную конфигурацию*.

В блоке `DNS` задаются резолверы узла: серверы, домены поиска и домен маршрутизации, через интерфейсы которого уходят DNS-запросы. DNS-серверы, полученные по DHCP, не используются. На узле нет рекурсивного резолвера, поэтому в качестве DNS-серверов не принимаются loopback-адреса (например, `127.0.0.1`, `::1`), адреса `0.0.0.0` и `::`, а также multicast-адреса.

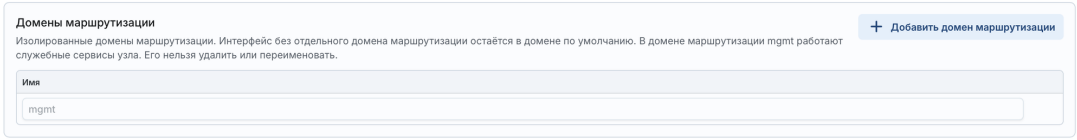


Чтобы настроить DNS-резолверы:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо настроить DNS-резолверы.
3. В блоке `DNS` в поле `Серверы` укажите адреса DNS-серверов через запятую.
4. При необходимости в поле `Домены поиска` укажите домены поиска через запятую.
5. В раскрывающемся списке `Домен маршрутизации` выберите домен маршрутизации, через который уходят DNS-запросы, или оставьте `По умолчанию`, чтобы использовать общую сеть.
6. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

6.3.1.4 Настройка доменов маршрутизации

Домены маршрутизации задаются в веб-интерфейсе Angie ADC на странице `Система` → `Сетевые настройки`. Изменения применяются через *кластерную конфигурацию*.



Трафик в доменах маршрутизации изолирован; доступ из общей сети в домен можно открыть с помощью *утечек маршрутов*.

Домен маршрутизации можно задать для *интерфейсов узла* и для *отдельных сервисов Angie ADC*.

Настройка сети управления

По умолчанию на каждом узле предустановлен домен маршрутизации `mgmt` для управления системой. Если в домене `mgmt` задан хотя бы один интерфейс, то веб-интерфейс Angie ADC, CLI и SSH будут доступны только через этот домен. Если в домене `mgmt` нет интерфейсов, для управления используется общая сеть. Домен `mgmt` нельзя удалить или переименовать.

Важно

Интерфейс с адресом, по которому узел подключен к кластеру, должен оставаться в общей сети и сохранять этот адрес. Для сети управления используйте отдельный интерфейс.

Чтобы вынести управление узлом в `mgmt`:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо выделить сеть управления.
3. В блоке `Интерфейсы` выберите интерфейс, который вы хотите использовать для управления, и в раскрывающемся списке `Домен маршрутизации` укажите для него домен `mgmt`.
4. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

Веб-интерфейс, CLI и SSH будут доступны только через домен `mgmt`.

Добавление домена маршрутизации

Чтобы добавить домен маршрутизации:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо добавить домен маршрутизации.
3. В блоке `Домены маршрутизации` этого узла нажмите `Добавить домен маршрутизации` и укажите имя домена маршрутизации. Имя должно быть корректным именем интерфейса Linux (до 15 байт) и не может совпадать с именем другого домена или интерфейса; имя `default` зарезервировано.
4. В блоке `Интерфейсы` выберите интерфейс, который вы хотите использовать для этого домена, и в раскрывающемся списке `Домен маршрутизации` укажите для него созданный домен.
5. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

Привязка сервисов Angie ADC к домену маршрутизации

Отдельные домены маршрутизации можно задать для следующих сервисов Angie ADC:

- *GSLB*;
- *NTP*;
- *DNS*;
- *аутентификация и авторизация внешних пользователей*;
- *порталы аутентификации клиентов в балансировщике*;
- *SNMP*;
- *датчики доступности*;
- *резервное копирование конфигурации балансировщика нагрузки (S3)*.

Чтобы привязать сервис к домену маршрутизации:

1. *Добавьте домен маршрутизации* и назначьте ему интерфейс, через который сервис будет обращаться к сети. Если нужные сети доступны только через шлюз, *добавьте маршрут* через этот интерфейс.
2. Откройте настройки нужного сервиса Angie ADC.
3. Выберите домен маршрутизации в раскрывающемся списке `Домен маршрутизации`.
4. Сохраните изменения.

Домены маршрутизации задаются для каждого узла отдельно: добавьте домен с тем же именем и интерфейсом на каждом узле, на котором работает сервис.

Удаление домена маршрутизации

Перед удалением домена маршрутизации проверьте, что ни один сервис или интерфейс не использует этот домен, иначе домен не будет удален.

Чтобы удалить домен маршрутизации:

1. Перейдите в раздел `Система` → `Сетевые настройки`.
2. Выберите узел, на котором необходимо удалить домен маршрутизации.
3. В блоке `Домены маршрутизации` нажмите значок удаления в строке домена маршрутизации.
4. Нажмите `Применить` в нижней части экрана, чтобы сохранить изменения.

6.4 Управление пользователями и доступами

В этом разделе описывается управление пользователями Angie ADC: добавление локальных пользователей и подключение внешних через LDAP, RADIUS или TACACS, назначение ролей, требования к паролям, управление сессиями и настройка безопасности учетной записи.

В этом разделе:

- *Пользователи и роли*
- *Управление локальными пользователями*
- *Подключение внешних пользователей*
- *Управление пользовательскими сессиями*
- *Парольная политика*
- *Настройка учетной записи*
- *Аудит действий пользователей*

6.4.1 Пользователи и роли

В Angie ADC могут работать локальные пользователи системы и внешние пользователи. Администратор Angie ADC может просматривать действующие сессии пользователей на узлах и завершать их (см. *Управление пользовательскими сессиями*).

6.4.1.1 Локальные пользователи

Локальные пользователи создаются и хранятся в системе. Их список отображается в веб-интерфейсе в разделе `Система` → `Пользователи` (см. *Управление локальными пользователями*). Роли для локальных пользователей назначаются при их создании и хранятся также в системе. По умолчанию на каждом узле предустановлен локальный пользователь `admin` с правами администратора.

6.4.1.2 Внешние пользователи

Angie ADC поддерживает внешние серверы аутентификации и авторизации RADIUS, LDAP и TACACS+. Данные о внешних пользователях хранятся на внешнем сервере. У системы нет доступа к этим данным. Система также не хранит данные о ролях внешних пользователей. Для подключения внешних пользователей необходимо добавить в веб-интерфейс предварительно настроенные серверы внешней аутентификации и авторизации. Подробнее см. *Подключение внешних пользователей*.

Принятые решения по внешней авторизации записываются в журналы событий системы. Записи можно экспортировать на внешний syslog-сервер для дальнейшего аудита.

6.4.1.3 Роли

Пользователям можно назначить одну из следующих **ролей**:

- `Администратор`: обладает полными правами на все действия в системе;
- `Супервизор`: имеет ограниченные права, может только просматривать информацию в системе, например, проводить аудит;

- `Оператор`: имеет ограниченные права, может редактировать файлы конфигурации балансировщика, к которым ему предоставлен доступ, и просматривать статистику зон, к которым ему предоставлен доступ. Доступы предоставляет администратор. Остальные настройки Angie ADC оператору недоступны и не отображаются в веб-интерфейсе.

Роль локального пользователя задается при его создании (см. *Управление локальными пользователями*). Роль внешнего пользователя задается правилами авторизации (см. *Подключение внешних пользователей*).

Примечание

При превышении допустимого количества неудачных попыток входа в веб-интерфейс (по умолчанию — двух попыток в течение 60 минут) пользователь будет временно заблокирован (см. *Парольная политика*).

6.4.2 Управление локальными пользователями

Локальные пользователи системы отображаются в веб-интерфейсе в разделе `Система` → `Пользователи`. Для каждого пользователя представлена следующая информация:

`Логин`	Логин пользователя в системе
`Имя`	Собственное имя пользователя
`Фамилия`	Фамилия пользователя
`UUID`	Уникальный идентификатор пользователя
`Статус`	Статус пользователя в системе: • `активный` — пользователь имеет доступ к системе. • `неактивный` — у пользователя временно отключен доступ к системе, например, на время отпуска. • `удален` — пользователь удален, но может отображаться в списке, если включен переключатель `Показывать удаленных пользователей`.
`Роль`	Роль пользователя в системе: `Администратор`, `Супервизор` или `Оператор` (см. *Пользователи и роли*).
`Комментарий`	Примечание

6.4.2.1 Добавление локального пользователя

Чтобы добавить нового локального пользователя:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Пользователи`.

   Откроется список пользователей.

2. В открывшемся окне нажмите кнопку `+ Добавить пользователя`.

3. Укажите логин, пароль, имя и фамилию нового пользователя, а также его роль и нажмите `Добавить`.

   Требования:

   - Логин — допускаются латинские буквы, цифры, а также специальные символы: `_ - . @ ! # $ % ^ & * ( ) = +`.
   - Пароль — допускаются латинские буквы, цифры, а также специальные символы: `_ - . @ ! # $ % ^ & * ( ) = +`. Пароль должен соответствовать текущей *парольной политике*. Пароль можно ввести вручную или сгенерировать. Пароль не может совпадать с логином без учета регистра.

> **Примечание**
>
> Кнопка копирования пароля будет доступна, если используется защищенное подключение к веб-интерфейсу (*HTTPS*).

- Имя — допускаются только буквы латиницы и кириллицы, а также дефис и пробел.
- Фамилия — допускаются только буквы латиницы и кириллицы, а также дефис и пробел.
- Роль:
  - `Администратор` — обладает полными правами на все действия в системе;
  - `Супервизор` — имеет ограниченные права, может только просматривать информацию в системе, например, проводить аудит;
  - `Оператор` — имеет ограниченные права, может редактировать файлы конфигурации балансировщика, к которым ему предоставлен доступ, и просматривать статистику зон, к которым ему предоставлен доступ. Доступы предоставляет администратор. Остальные настройки Angie ADC оператору недоступны и не отображаются в веб-интерфейсе.

Новый пользователь отобразится в таблице.

4. Передайте пользователю логин и пароль безопасным способом.

6.4.2.2 Изменение учетных данных и статуса локального пользователя

Чтобы изменить данные локального пользователя:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Пользователи`.

   Откроется список пользователей.

2. Нажмите значок редактирования рядом с пользователем, данные или статус которого вы хотите изменить.

3. В открывшемся окне укажите новые данные и нажмите `Сохранить`.

Информация о пользователе будет обновлена.

6.4.2.3 Сброс пароля локального пользователя

Администратор может вручную сбросить пароль пользователя и задать для него новый пароль. После сброса пароля пользователю необходимо заново войти в систему.

1. Перейдите в раздел `Система` → `Пользователи`.
2. Нажмите значок "ключ" (`Сбросить пароль`) напротив нужного пользователя.
3. В открывшемся окне введите новый пароль для пользователя и повторите его. Можно ввести пароль вручную или сгенерировать его с учетом текущей парольной политики.

> **Примечание**
>
> Кнопка копирования пароля будет работать, если используется защищенное подключение к веб-интерфейсу (*HTTPS*).

4. Нажмите `Сбросить пароль`.

   Старый пароль будет сброшен, новый пароль будет сохранен.

5. Передайте пользователю новый пароль безопасным способом.

6.4.2.4 Сброс настроек двухфакторной аутентификации локального пользователя

Администратор может вручную сбросить настройки двухфакторной аутентификации для локального пользователя, например, если пользователь больше не имеет доступа к подключенному приложению для аутентификации. После сброса настроек двухфакторной аутентификации пользователю необходимо заново войти в систему. При входе в систему пользователь должен настроить двухфакторную аутентификацию заново, если этого требует *парольная политика*.

1. Перейдите в раздел `Система` → `Пользователи`.
2. Нажмите значок "экран с крестиком" (`Сбросить TOTP`) напротив нужного пользователя.

   Настройки двухфакторной аутентификации будут сброшены.

6.4.2.5 Удаление локального пользователя

Чтобы удалить локального пользователя:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Пользователи`. Откроется список пользователей.
2. Нажмите значок удаления рядом с пользователем, запись о котором вы хотите удалить.

Пользователь будет удален из списка, но будет отображаться в списке пользователей, если включен переключатель `Показывать удаленных пользователей`. В дальнейшем вы можете просмотреть список удаленных пользователей при аудите системы.

Чтобы вернуть удаленного пользователя в систему, *восстановите* его.

6.4.2.6 Восстановление удаленного локального пользователя

Чтобы восстановить удаленного локального пользователя:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Пользователи`. Откроется список пользователей.
2. Включите переключатель `Показывать удаленных пользователей`.

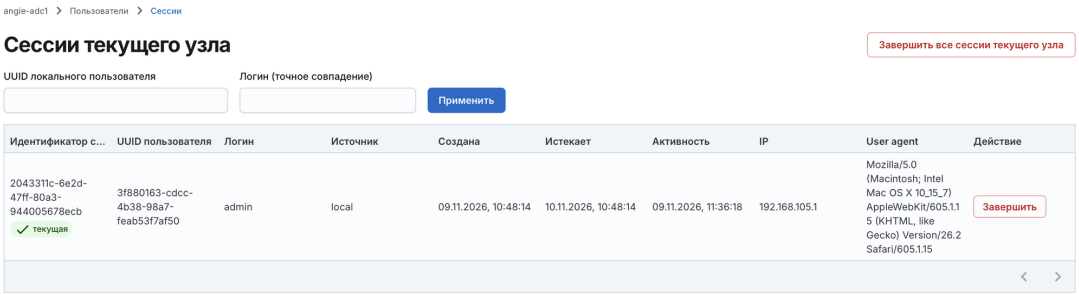
   В списке отобразятся удаленные пользователи со статусом `удален`.
3. Нажмите значок восстановления (`Восстановить пользователя`) напротив нужного пользователя.
4. В открывшемся окне подтвердите действие, нажав `Да`.

Учетная запись пользователя снова станет активной, статус пользователя изменится на `активный`.

6.4.3 Управление пользовательскими сессиями

Администратор Angie ADC может просматривать действующие сессии пользователей на текущем узле и завершать их. После завершения сессии пользователь должен будет заново войти в систему.

Сессии узла отображаются в разделе `Система` → `Пользователи` → `Сессии`. На каждом узле Angie ADC отображаются только сессии этого узла.



Совет

Чтобы полностью запретить доступ к веб-интерфейсу для локального пользователя, завершите все его действующие сессии на каждом узле ADC и переведите его учетную запись в неактивный статус или удалите ее (подробнее см. *Управление локальными пользователями*).

Чтобы полностью запретить доступ для внешнего пользователя, завершите все его действующие сессии на каждом узле ADC и заблокируйте его учетную запись на стороне внешнего провайдера.

6.4.3.1 Просмотр сессий

На странице `Сессии текущего узла` для каждой действующей сессии представлена следующая информация:

`Идентификатор сессии`	Уникальный идентификатор сессии. Текущая сессия отмечена меткой `текущая`.
`UUID пользователя`	Уникальный идентификатор пользователя. UUID отображается только для локальных пользователей.
`Логин`	Логин пользователя в системе.
`Источник`	Способ, которым пользователь вошел в систему (локальный или внешний пользователь).
`Создана`	Время создания сессии.
`Истекает`	Срок действия сессии (24 часа от создания).
`Активность`	Время последней зарегистрированной активности; обновляется не чаще одного раза в пять минут.
`IP`	IP-адрес, с которого выполнен вход.
`User agent`	Клиент, с которого выполнен вход.
`Действие`	Кнопка `Завершить` для отзыва сессии.

Список можно отфильтровать по полям `UUID локального пользователя` и `Логин`. UUID и логин необходимо вводить полностью. Если заполнены оба поля, применяются оба условия одновременно.

6.4.3.2 Завершение сессии

Чтобы завершить отдельную сессию:

1. Перейдите в раздел `Система` → `Пользователи` и нажмите кнопку `Сессии`.
2. Найдите нужную сессию и нажмите кнопку `Завершить` напротив нее.
3. Подтвердите операцию.

Сессия будет отозвана при следующем запросе пользователя к веб-интерфейсу. Пользователь должен будет войти в систему заново.

6.4.3.3 Завершение всех сессий текущего узла

Чтобы завершить все сессии текущего узла:

1. Перейдите в раздел `Система` → `Пользователи` и нажмите кнопку `Сессии`.
2. Нажмите кнопку `Завершить все сессии текущего узла`.
3. Подтвердите операцию.

Будут отозваны все сессии текущего узла независимо от установленных фильтров. Текущая сессия администратора также будет завершена, и ему потребуется войти в систему заново.

Примечание

Сессии разных узлов независимы. Чтобы просмотреть или отозвать сессии другого узла, откройте веб-интерфейс на соответствующем узле.

6.4.4 Подключение внешних пользователей

Angie ADC поддерживает аутентификацию и авторизацию пользователей через внешние серверы RADIUS, LDAP и TACACS+. Политика внешней аутентификации и авторизации относится только к тому узлу, на котором она настраивается. Настройки находятся в разделе `Система` → `Аутентификация и авторизация`. В нижней части страницы можно задать домены маршрутизации, через которые Angie ADC подключается к внешним серверам.

Angie ADC поддерживает два режима подключения:

- *Режим цепочек* (рекомендуется).

  Используются цепочки серверов аутентификации и авторизации: несколько серверов разных типов, в том числе несколько серверов одного типа; задается порядок, в котором они проверяют пользователя (см. *Режим цепочек аутентификации и авторизации*). После первого включения режима цепочек режим с одним провайдером становится недоступен.

- *Режим с одним провайдером* (устарел).

  Для аутентификации и авторизации используется по одному внешнему серверу (см. *Аутентификация (режим без цепочек)* и *Авторизация (режим без цепочек)*). Этот режим действует, если не включены цепочки.

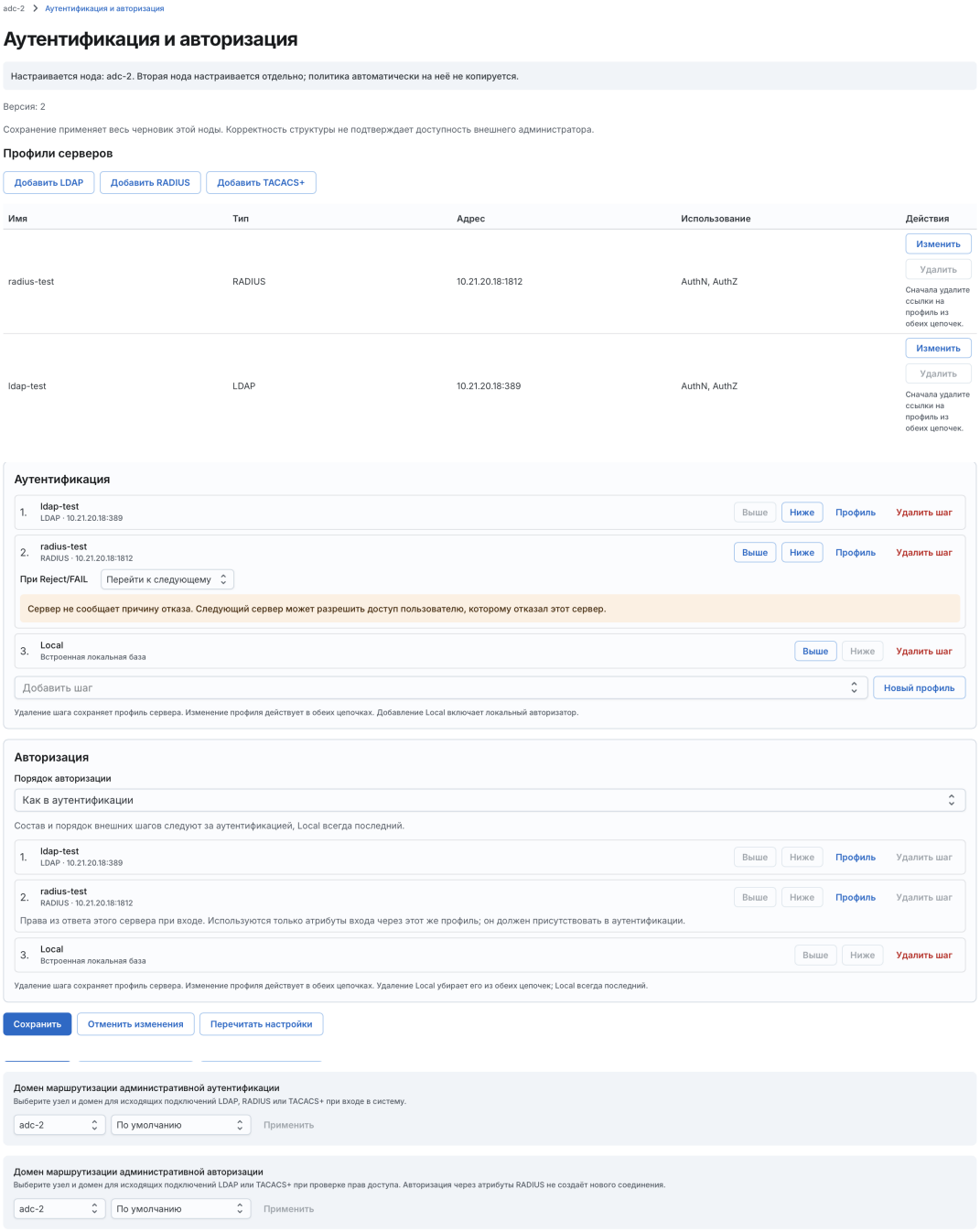
В этом разделе:

- *Режим цепочек аутентификации и авторизации*
- *Профили серверов*
- *Настройка режима цепочек*
- *Аутентификация (режим без цепочек)*
- *Авторизация (режим без цепочек)*

6.4.4.1 Режим цепочек аутентификации и авторизации

Внешние пользователи подключаются к Angie ADC через внешние серверы RADIUS, LDAP и TACACS+ с помощью цепочек аутентификации и авторизации. Цепочки аутентификации и авторизации позволяют проверять внешних пользователей, которые входят в веб-интерфейс, на нескольких внешних серверах по очереди, в том числе на нескольких серверах одного типа, например `LDAP1` → `RADIUS1` → `LDAP2` → `LDAP3` → `TACACS1`.

После сохранения политика применяется к текущему узлу. При первом включении цепочек отзываются все прежние сессии внешних пользователей. Настройки находятся в разделе `Система` → `Аутентификация и авторизация`.



Настройка состоит из двух этапов:

- *Создание профилей серверов*.

  Каждый внешний сервер описывается отдельным профилем: имя, протокол, параметры подключения, секрет, а также параметры аутентификации и авторизации. Один профиль можно использовать в обеих цепочках без повторного ввода адреса и секрета.

- *Создание цепочек аутентификации и авторизации*.

  Цепочка аутентификации определяет, в каком порядке на серверах проверяются введенные логин и пароль.

  Цепочка авторизации определяет, в каком порядке на серверах запрашивается роль пользователя.

Алгоритм проверки

Алгоритм проверки следующий:

1. При входе пользователь вводит логин и пароль.
2. Angie ADC проверяет логин и пароль по шагам цепочки аутентификации сверху вниз:
   - если сервер подтвердил логин и пароль, аутентификация завершается;
   - если пользователь не найден или сервер недоступен, проверяется следующий шаг;
   - если сервер LDAP нашел пользователя, но отклонил пароль, вход запрещается;
   - если отказал сервер RADIUS или TACACS+, результат определяется полем `При Reject/FAIL` этого шага: `Остановить цепочку` (по умолчанию) или `Перейти к следующему`.

   Важно

   Общий таймаут цепочки равен 30 секундам, таймаут для одного шага 10 секунд. Чтобы не потерять доступ к Angie ADC, рекомендуется в начале ставить шаг с локальной аутентификацией *через базу Local*. Тогда локальный администратор сможет войти при недоступности внешних сервисов.

3. Затем Angie ADC запрашивает роль по шагам цепочки авторизации сверху вниз:
   - если шаг разрешил доступ, пользователь получает роль этого шага; роли, полученные на разных шагах, не объединяются;
   - если шаг не применяется к пользователю (например, пользователь не найден в LDAP или вошел через другой профиль RADIUS) или сервер недоступен, проверяется следующий шаг;
   - если шаг запретил доступ (например, пользователь найден в LDAP, но не состоит ни в одной группе из правил), вход запрещается;
   - если отказал сервер TACACS+, результат определяется полем `При Reject/FAIL` этого шага.
4. Если цепочка исчерпана и ни один шаг не завершился успешно, доступ запрещается.

База Local

Предустановленная база `Local` содержит список локальных пользователей Angie ADC. Для обеспечения входа локальных пользователей необходимо добавить эту базу в цепочку аутентификации первым шагом и в цепочку авторизации последним шагом.

Предупреждение

Если база `Local` нигде не добавлена, локальные входы будут запрещены, включая локального администратора `admin`. Все локальные сессии будут отозваны.

Удалять базу `Local` рекомендуется только в том случае, если в организации сознательно запрещен локальный доступ и вход внешнего администратора уже проверен, иначе доступ к Angie ADC может быть полностью потерян.

Перед сохранением цепочки без `Local` сначала войдите в систему через внешнюю цепочку и проверьте, что внешнему администратору доступны необходимые действия. Корректная структура цепочек не подтверждает, что внешний администратор сможет войти.

Применение в доменах маршрутизации

В нижней части страницы `Аутентификация и авторизация` можно задать узел и домен маршрутизации, через которые Angie ADC подключается к внешним серверам:

- `Домен маршрутизации административной аутентификации`: для подключений к серверам LDAP, RADIUS и TACACS+;
- `Домен маршрутизации административной авторизации`: для подключений к серверам LDAP и TACACS+. Авторизация по атрибутам RADIUS новых подключений не создает.

Чтобы задать домен маршрутизации, выберите узел и нужный домен и нажмите `Применить`. Настройки применяются сразу и не входят в черновик политики. По умолчанию для подключений используется общая сеть.

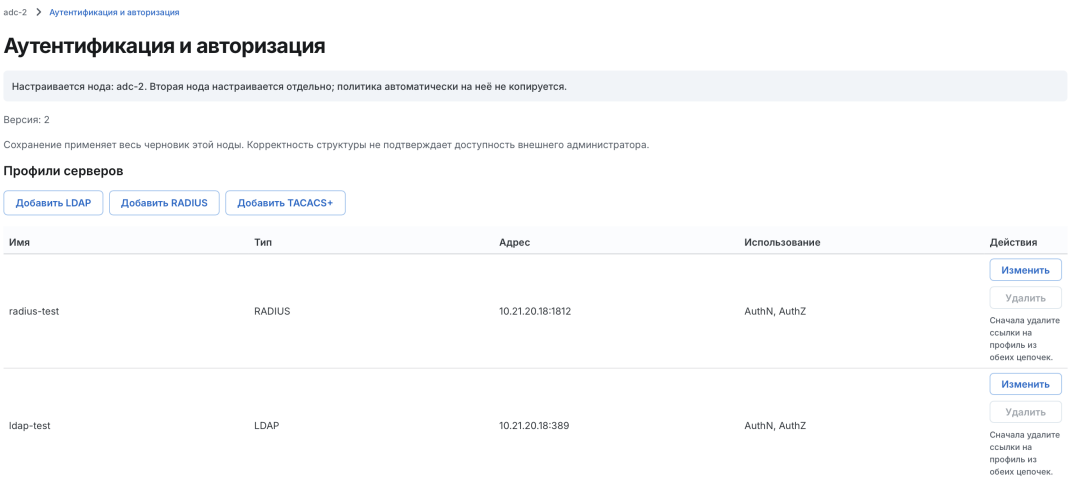
Применение в паре высокой доступности

Политика аутентификации и авторизации хранится на каждом узле отдельно. Имя настраиваемого узла отображается в верхней части страницы.

- Настройте цепочки на каждом узле пары высокой доступности. После переключения на другой узел пользователь проходит цепочки этого узла; если они отличаются, он может потерять доступ.
- Отзыв сессий и удаление `Local` на одном узле не затрагивают другой.
- Существующая пара продолжает работать после удаления `Local` и отзыва пользовательских сессий: узлы используют сохраненный служебный токен пары.
- Чтобы создать новую пару при удаленном `Local`, войдите в мастер как внешний администратор, прошедший обе цепочки на принимающем узле. Для создания пары поддерживается вход только по логину и паролю: если администратору требуется TOTP или смена пароля, создать пару не получится.

6.4.4.2 Профили серверов

Профили серверов отображаются на странице `Система` → `Аутентификация и авторизация`.



Профиль сервера описывает один внешний сервер (LDAP, RADIUS или TACACS+), который используется в *цепочках аутентификации и авторизации*.

Профиль содержит:

- имя и протокол;
- параметры подключения и секрет;

- параметры аутентификации (AuthN);
- параметры авторизации (AuthZ), включая правила назначения ролей.

Один профиль можно использовать в обеих цепочках: адрес, параметры подключения и секрет вводятся один раз. Изменение профиля действует во всех цепочках, где он используется.

Можно создать несколько профилей одного протокола, в том числе для одного адреса, например с разными сервисными учетными записями LDAP. Профили имеют независимые настройки и секреты.

В этой статье:

- *Создание профиля LDAP*
- *Создание профиля RADIUS*
- *Создание профиля TACACS+*
- *Удаление профиля*

Создание профиля LDAP

На стороне LDAP-сервера также должны быть настроены пользователи, группы и сервисная учетная запись для Angie ADC.

Чтобы создать профиль LDAP:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.
2. В блоке `Профили серверов` нажмите `Добавить LDAP`.

   > **Примечание**
   >
   > Профиль также можно создать при добавлении шага в цепочку кнопкой `Новый профиль`. Такой профиль сразу добавляется в соответствующую цепочку.

3. Укажите `Имя профиля`, например `LDAP-main`.
4. В блоке `Подключение` укажите параметры сервера:
   - `Сервер`: IP-адрес или доменное имя LDAP-сервера, например `192.0.2.10` или `ldap.example.com`.
   - `Порт`: порт подключения (по умолчанию `389`).
   - `DN сервисной учетной записи`: DN учетной записи, от имени которой Angie ADC подключается к LDAP-серверу, например `cn=adc-bind,ou=service,dc=example,dc=com`. Пароль этой учетной записи задается как секрет профиля.
   - `LDAPS`: подключение по протоколу LDAPS.
   - `StartTLS`: защита соединения с помощью StartTLS.
   - `Не проверять TLS-сертификат`: отключает проверку сертификата сервера.
5. В поле `Действие с секретом` выберите:
   - `Сохранить прежний`: секрет не меняется. Изменение остальных полей, имени профиля или порядка шагов не влияет на сохраненный секрет.
   - `Заменить`: введите новый секрет в поле `Новый секрет`.
   - `Без секрета (очистить)`: удалить секрет. Вариант доступен, только если профиль используется исключительно для авторизации. Для нового профиля без секрета этот вариант нужно выбрать явно.

Секрет привязан к ID профиля. Новый профиль не наследует секрет другого профиля того же протокола.

6. Установите флажок `Настроить аутентификацию`, если профиль будет использоваться в цепочке аутентификации, и заполните ее параметры.

   - `Base DN`: ветка LDAP, в которой выполняется поиск пользователя, например `ou=users,dc=example,dc=com`.
   - `Фильтр пользователей (%s - логин)`: LDAP-фильтр поиска пользователя, например `(&(objectClass=user)(sAMAccountName=%s))`.
   - `Идентификатор логина`: атрибут LDAP, содержащий логин, например `uid`, `sAMAccountName` или `userPrincipalName`.

   Примечание

   Фильтр определяет, в каком формате пользователь вводит логин:

   - с фильтром `(&(objectClass=user)(sAMAccountName=%s))` логин вводится без доменного имени, например `ivanov`;
   - с фильтром `(&(objectClass=user)(userPrincipalName=%s))` логин вводится полностью, например `ivanov@domain.com`.

7. Установите флажок `Настроить авторизацию`, если профиль будет использоваться в цепочке авторизации, и заполните параметры получения роли.

   Роль определяется по принадлежности пользователя к LDAP-группам.

   - `Базовый DN пользователей`, например `ou=users,dc=example,dc=com`.
   - `Фильтр пользователей AuthZ (%s - логин)`, например `(uid=%s)`.
   - `Базовый DN групп`, например `ou=groups,dc=example,dc=com`.
   - `Фильтр групп (%s - DN пользователя)`, например `(member=%s)`.
   - Правила назначения ролей: нажмите `Добавить правило`, укажите `DN группы`, например `cn=adc-admins,ou=groups,dc=example,dc=com`, и выберите `Роль ADC`: `admin`, `operator` или `supervisor`. Нужно хотя бы одно правило.

8. Проверьте подключение к LDAP:

   Чтобы проверить параметры подключения, нажмите `Проверить подключение LDAP`. Проверяются только подключение к серверу и вход сервисной учетной записи (bind). Вход пользователя и назначение роли не проверяются, настройки не сохраняются.

   - Проверка выполняется через домен маршрутизации той операции, для которой настроен профиль (см. *Применение в доменах маршрутизации*). Если профиль используется и для аутентификации, и для авторизации, проверяются оба домена.
   - Сохраненный пароль сервисной учетной записи можно использовать для проверки, только если не изменены сервер, порт, DN сервисной учетной записи и параметры TLS. Иначе укажите пароль заново.
   - Если выбран вариант `Без секрета (очистить)`, сначала сохраните профиль, затем проверьте подключение.

9. Нажмите `Готово`.

   Примечание

   Все изменения на странице остаются черновиком, пока вы не сохраните их. Кнопка `Готово` в окне профиля только добавляет профиль в черновик.

10. Нажмите `Сохранить` в нижней части окна `Аутентификация и авторизация`, чтобы применить изменения.

Создание профиля RADIUS

Чтобы создать профиль RADIUS:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.
2. В блоке `Профили серверов` нажмите `Добавить RADIUS`.

> **Примечание**
>
> Профиль также можно создать при добавлении шага в цепочку кнопкой `Новый профиль`. Такой профиль сразу добавляется в соответствующую цепочку.

3. Укажите `Имя профиля`, например `RADIUS-main`.
4. В блоке `Подключение` укажите параметры сервера:
   - `Сервер`: IP-адрес или доменное имя RADIUS-сервера, например `192.0.2.11` или `radius.example.com`.
   - `Порт`: порт подключения (по умолчанию `1812`).
   - `Транспорт RADIUS`: `UDP` (по умолчанию) или `TCP`.
   - `NAS-идентификатор`: идентификатор NAS (Network Access Server), передаваемый RADIUS-серверу, например `adc-node1`.
   - `Метод аутентификации`: поддерживается только `PAP`.
5. В поле `Действие с секретом` выберите:
   - `Сохранить прежний`: секрет не меняется. Изменение остальных полей, имени профиля или порядка шагов не влияет на сохраненный секрет.
   - `Заменить`: введите новый секрет в поле `Новый секрет`.

   Секрет привязан к ID профиля. Новый профиль не наследует секрет другого профиля того же протокола.

   Секрет RADIUS обязателен.
6. Установите флажок `Настроить аутентификацию`, если профиль будет использоваться в цепочке аутентификации. Отдельных параметров нет: используются подключение и секрет профиля.
7. Установите флажок `Настроить авторизацию`, если профиль будет использоваться в цепочке авторизации, и заполните параметры получения роли.

   Роль определяется по атрибутам, которые RADIUS-сервер вернул при входе через этот же профиль. Отдельного запроса к RADIUS-серверу не выполняется.
   - `Атрибут роли (filter-id или vsa:vendor:type)`: атрибут, по которому определяется роль, например `filter-id` или `vsa:9:1` (атрибут Vendor-Specific).
   - Правила назначения ролей: нажмите `Добавить правило`, укажите `Значение атрибута`, например `adc-admin` или `shell:priv-lvl=15`, и выберите `Роль ADC`. Нужно хотя бы одно правило.

> **Примечание**
>
> Чтобы использовать RADIUS-профиль в цепочке авторизации, добавьте этот же профиль в цепочку аутентификации. Правила профиля применяются только к пользователям, вошедшим через этот профиль: например, для пользователя, вошедшего через профиль `RADIUS1`, шаг авторизации с профилем `RADIUS2` пропускается.

8. Нажмите `Готово`.

> **Примечание**
>
> Все изменения на странице остаются черновиком, пока вы не сохраните их. Кнопка `Готово` в окне профиля только добавляет профиль в черновик.

9. Нажмите `Сохранить` в нижней части окна `Аутентификация и авторизация`, чтобы применить изменения.

Настройка RADIUS-сервера

На RADIUS-сервере должны быть настроены пользователи и их атрибуты.

Пример:

```
user1 Cleartext-Password := "P@ssword"
    Filter-Id := "adc-admin",
    Cisco-AVPair := "shell:priv-lvl=15"

user2 Cleartext-Password := "P@ssword"
    Filter-Id := "adc-readonly",
    Cisco-AVPair := "shell:priv-lvl=7"
```

В поле `Атрибут роли` профиля можно указать `filter-id`, `class`, `service-type`, `tunnel-private-group-id` или атрибут Vendor-Specific в формате `vsa:<vendorID>:<vendorType>` (например `vsa:9:1` для `Cisco-AVPair`). Для этого примера подойдут правила `filter-id`: `adc-admin` → `admin` или `vsa:9:1`: `shell:priv-lvl=15` → `admin`.

Создание профиля TACACS+

Чтобы создать профиль TACACS+:

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.
2. В блоке `Профили серверов` нажмите `Добавить TACACS+`.

> **Примечание**
>
> Профиль также можно создать при добавлении шага в цепочку кнопкой `Новый профиль`. Такой профиль сразу добавляется в соответствующую цепочку.

3. Укажите `Имя профиля`, например `TACACS-main`.
4. В блоке `Подключение` укажите параметры сервера:
   - `Сервер`: IP-адрес или доменное имя TACACS+-сервера, например `192.0.2.12` или `tacacs.example.com`.
   - `Порт`: порт подключения (по умолчанию 49).

5. В поле `Действие с секретом` выберите:

   - `Сохранить прежний`: секрет не меняется. Изменение остальных полей, имени профиля или порядка шагов не влияет на сохраненный секрет.
   - `Заменить`: введите новый секрет в поле `Новый секрет`.
   - `Без секрета (очистить)`: удалить секрет. Вариант доступен, только если профиль используется исключительно для авторизации. Для нового профиля без секрета этот вариант нужно выбрать явно.

   Секрет привязан к ID профиля. Новый профиль не наследует секрет другого профиля того же протокола.

6. Установите флажок `Настроить аутентификацию`, если профиль будет использоваться в цепочке аутентификации. Отдельных параметров нет: используются подключение и секрет профиля.

7. Установите флажок `Настроить авторизацию`, если профиль будет использоваться в цепочке авторизации, и заполните параметры получения роли.

   Роль определяется по атрибутам пользователя, которые TACACS+-сервер возвращает на запрос авторизации (AUTHOR).

   - `Атрибут роли`: атрибуты, по которым определяется роль, в порядке приоритета, например `priv-lvl`, затем `role`. Чтобы добавить атрибут, нажмите `Добавить атрибут роли`.
   - `Аргумент Authorize`: аргументы запроса авторизации, например `service=shell` и `protocol=ip`. Набор аргументов зависит от сервера. Чтобы добавить аргумент, нажмите `Добавить аргумент Authorize`.
   - Правила назначения ролей: нажмите `Добавить правило`, укажите `Значение атрибута`, например `priv-lvl=15` или `role=adc-admin`, и выберите `Роль ADC`. Нужны хотя бы один атрибут роли и одно правило.

8. Нажмите `Готово`.

> **Примечание**
>
> Все изменения на странице остаются черновиком, пока вы не сохраните их. Кнопка `Готово` в окне профиля только добавляет профиль в черновик.

9. Нажмите `Сохранить` в нижней части окна `Аутентификация и авторизация`, чтобы применить изменения.

Настройка TACACS+-сервера

На TACACS+-сервере должны быть настроены пользователи, группы и их атрибуты. Пример:

```
group = admin {
    service = shell {
        set priv-lvl = 15
    }
}

user = admin {
    password = clear admin
    member = admin
}
```

Для этого примера укажите в профиле атрибут роли `priv-lvl`, аргументы `service=shell` и `protocol=ip` и правило `priv-lvl=15` → `admin`.

Удаление профиля

> **Примечание**
>
> Профиль, который используется в цепочках, удалить нельзя. Сначала удалите его шаги из обеих цепочек.

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.
2. В блоке `Профили серверов` нажмите `Удалить` в строке профиля.
3. Нажмите `Сохранить` в нижней части окна `Аутентификация и авторизация`, чтобы применить изменения.

6.4.4.3 Настройка режима цепочек

В этом примере Angie ADC последовательно проверяет пользователей по встроенной локальной базе `Local` и на серверах LDAP, RADIUS и TACACS+.

```
Local → LDAP → RADIUS → TACACS+
```

Такая цепочка подходит для большинства установок: внешние пользователи входят через свои серверы, а локальные учетные записи, включая администратора `admin`, продолжают работать, в том числе когда внешние серверы недоступны по таймауту.

> **Предупреждение**
>
> Рекомендуется, чтобы логины из разных источников не совпадали, иначе успешный пропуск пользователя зависит от порядка шагов в цепочке. Например, в текущем примере пользователь LDAP с логином, совпадающим с пользователем из базы `Local`, не сможет войти в сиситему, так как при неверном пароле база `Local` выдаст пользователю отказ и остановит цепочку. Если LDAP будет стоять раньше `Local`, то пользователь `Local` не сможет войти, так как его пароль не подойдет для LDAP.

В этой статье:

- *Перед началом*
- *Шаг 1. Откройте настройки*
- *Шаг 2. Создайте профиль LDAP*
- *Шаг 3. Создайте профиль RADIUS*
- *Шаг 4. Создайте профиль TACACS+*
- *Шаг 5. Настройте цепочку аутентификации*
- *Шаг 6. Настройте цепочку авторизации*
- *Шаг 7. Сохраните параметры и включите цепочки*
- *Шаг 8. Проверьте вход*

Перед началом

Подготовьте параметры подключения к серверам. Адреса ниже приведены для примера:

Профиль	Сервер	Порт
LDAP	`192.0.2.10`	389
RADIUS	`192.0.2.11`	1812
TACACS+	`192.0.2.12`	49

Также потребуются:

- DN и пароль сервисной учетной записи LDAP;
- базовые DN и фильтры поиска пользователей и групп LDAP;
- общий секрет RADIUS;
- общий секрет TACACS+;
- правила назначения ролей для каждого сервера: группы LDAP, значения атрибутов RADIUS и TACACS+.

Убедитесь, что:

- хотя бы один внешний пользователь получит роль `admin`;
- логины пользователей не повторяются на разных серверах и не совпадают с логинами локальных пользователей (см. *Шаг 8. Проверьте вход*).

Шаг 1. Откройте настройки

1. Войдите в веб-интерфейс Angie ADC как администратор.
2. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.
3. Нажмите `Настроить цепочки`.

   Откроется страница с профилями серверов и цепочками аутентификации и авторизации. Если ранее был настроен внешний провайдер, его настройки будут перенесены в профиль.

Шаг 2. Создайте профиль LDAP

1. В блоке `Профили серверов` нажмите `Добавить LDAP`.
2. Укажите `Имя профиля`, например `LDAP-main`.
3. В блоке `Подключение` укажите:
   - `Сервер`: `192.0.2.10`;
   - `Порт`: `389`;
   - `DN сервисной учетной записи`, например `cn=adc-bind,ou=service,dc=example,dc=com`.
4. В поле `Действие с секретом` выберите `Заменить` и введите пароль сервисной учетной записи в поле `Новый секрет`.
5. Убедитесь, что установлен флажок `Настроить аутентификацию`, и укажите:
   - `Base DN`: `ou=users,dc=example,dc=com`;
   - `Фильтр пользователей (%s - логин)`: `(uid=%s)`;
   - `Идентификатор логина`: `uid`.
6. Установите флажок `Настроить авторизацию` и укажите:
   - `Базовый DN пользователей`: `ou=users,dc=example,dc=com`;
   - `Фильтр пользователей AuthZ (%s - логин)`: `(uid=%s)`;
   - `Базовый DN групп`: `ou=groups,dc=example,dc=com`;

- `Фильтр групп (%s - DN пользователя)`: `(member=%s)`.

7. Нажмите `Добавить правило` и задайте соответствие групп ролям, например:
   - `cn=adc-admins,ou=groups,dc=example,dc=com` → `admin`;
   - `cn=adc-auditors,ou=groups,dc=example,dc=com` → `supervisor`.
8. Нажмите `Проверить подключение LDAP`.

   Проверяются только подключение и вход сервисной учетной записи; вход пользователей и роли не проверяются.
9. Нажмите `Готово`.

> **Примечание**
>
> Кнопка `Готово` в окне профиля только добавляет профиль в черновик. Все изменения на странице остаются черновиком, пока вы не сохраните их на Шаге 7.

Шаг 3. Создайте профиль RADIUS

1. Нажмите `Добавить RADIUS`.
2. Укажите `Имя профиля`, например `RADIUS-main`.
3. В блоке `Подключение` укажите:
   - `Сервер`: `192.0.2.11`;
   - `Порт`: `1812`;
   - `Транспорт RADIUS`: `UDP`;
   - `NAS-идентификатор`, например `adc-node1`;
   - `Метод аутентификации`: `PAP`.
4. В поле `Действие с секретом` выберите `Заменить` и введите общий секрет RADIUS.
5. Убедитесь, что установлен флажок `Настроить аутентификацию`.
6. Установите флажок `Настроить авторизацию` и укажите `Атрибут роли`, например `filter-id`.
7. Нажмите `Добавить правило` и задайте соответствие значений атрибута ролям, например `adc-admin` → `admin`.
8. Нажмите `Готово`.

> **Примечание**
>
> Кнопка `Готово` в окне профиля только добавляет профиль в черновик. Все изменения на странице остаются черновиком, пока вы не сохраните их на Шаге 7.

Роль пользователя RADIUS определяется по атрибутам, которые сервер вернул при входе через этот профиль. Отдельного запроса авторизации к RADIUS-серверу нет.

Шаг 4. Создайте профиль TACACS+

1. Нажмите `Добавить TACACS+`.
2. Укажите `Имя профиля`, например `TACACS-main`.
3. В блоке `Подключение` укажите:
   - `Сервер`: `192.0.2.12`;

- Порт: 49.

4. В поле Действие с секретом выберите Заменить и введите общий секрет TACACS+.
5. Убедитесь, что установлен флажок Настроить аутентификацию.
6. Установите флажок Настроить авторизацию и укажите:
   - атрибут роли: нажмите Добавить атрибут роли и укажите priv-lvl;
   - аргументы запроса: нажмите Добавить аргумент Authorize и укажите service=shell, затем protocol=ip.
7. Нажмите Добавить правило и задайте соответствие, например priv-lvl=15 → admin.
8. Нажмите Готово.

> **Примечание**
>
> Кнопка Готово в окне профиля только добавляет профиль в черновик. Все изменения на странице остаются черновиком, пока вы не сохраните их на Шаге 7.

В списке Профили серверов появятся три профиля со значением Не используется в столбце Использование.

Шаг 5. Настройте цепочку аутентификации

1. В блоке Аутентификация в списке Добавить шаг по очереди выберите:
   1. Local - встроенная локальная база;

      База Local включает использование локальных учетных записей пользователей Angie ADC. При добавлении Local в аутентификацию она автоматически добавляется и в авторизацию.
   2. LDAP-main;
   3. RADIUS-main;
   4. TACACS-main.

   Если порядок отличается, исправьте его кнопками Выше и Ниже.

> **Важно**
>
> Общий таймаут цепочки равен 30 секундам, таймаут для одного шага 10 секунд. Чтобы не потерять доступ к Angie ADC при недоступности внешних сервисов, рекомендуется ставить шаг с локальной аутентификацией через базу *Local* не дальше третьего шага для попадания в общий таймаут 30 секунд.

2. Для шага RADIUS-main в поле При Reject/FAIL выберите Перейти к следующему.

   RADIUS и TACACS+ отвечают отказом и на неверный пароль, и на неизвестного пользователя. С вариантом Остановить цепочку пользователи TACACS+ не дойдут до своих шагов: их отклонит RADIUS-сервер.

> **Предупреждение**
>
> С вариантом Перейти к следующему следующий сервер может разрешить вход пользователю, которому отказал предыдущий. Если один пользователь есть на нескольких серверах и был заблокирован на RADIUS-сервере, заблокируйте его и на остальных серверах.

Для шага LDAP настройка отказа не нужна: если пользователь не найден в LDAP, проверяется следующий шаг, а если найден, но пароль неверен, вход сразу запрещается.

3. Для шага `TACACS-main` в поле `При Reject/FAIL` выберите `Остановить цепочку`.

Шаг 6. Настройте цепочку авторизации

1. В блоке `Авторизация` в поле `Порядок авторизации` выберите `Как в аутентификации`.

   Цепочка авторизации повторит аутентификацию: `LDAP-main` → `RADIUS-main` → `TACACS-main` → `Local`. Шаг с `Local` всегда последний. Адреса серверов и секреты повторно не вводятся: используются параметры авторизации, заданные в профилях.

2. Для шага `TACACS-main` в авторизации оставьте `При Reject/FAIL` → `Остановить цепочку`.

   После `TACACS-main` в авторизации следует только `Local`, который применяется лишь к локальным пользователям, поэтому переход дальше не даст внешнему пользователю роль.

Каждый шаг авторизации применяется только к подходящим пользователям:

- `LDAP-main` ищет пользователя в каталоге по логину и пропускает пользователей, которых в каталоге нет;
- `RADIUS-main` применяется только к пользователям, вошедшим через `RADIUS-main`.
- `TACACS-main` и `LDAP-main` пропускают локальных пользователей;
- `Local` применяется только к локальным пользователям.

Шаг 7. Сохраните параметры и включите цепочки

1. Проверьте порядок шагов в обеих цепочках и убедитесь, что в них есть `Local`.

   Сводка над цепочками должна сообщать, что новые локальные входы разрешены и локальный авторизатор включен.

2. Нажмите `Сохранить и включить цепочки` и подтвердите действие кнопкой `Включить цепочки`.

   При первом включении отзываются все прежние сессии внешних пользователей.

3. Нажмите `Перечитать настройки` и убедитесь, что профили и порядок шагов сохранились.

   Кнопка `Перечитать настройки` позволяет получить настройки с сервера, если другой администратор уже внес изменения в политику на этом узле.

   В столбце `Использование` для всех трех профилей должно отображаться `AuthN, AuthZ`.

> **Примечание**
>
> Если узлы объединены в пару высокой доступности, повторите настройку на втором узле: политика на него не копируется.

Шаг 8. Проверьте вход

В отдельном окне браузера последовательно войдите:

1. пользователем LDAP;
2. пользователем RADIUS;
3. пользователем TACACS+;
4. локальным пользователем Angie ADC.

На странице входа выбирать тип аутентификации не нужно: пользователь вводит только логин и пароль.

Для чистой проверки используйте разных пользователей, каждый из которых существует только в своем источнике. Проверьте, что каждый пользователь получает ожидаемую роль.

При такой настройке Angie ADC работает так:

- пользователь LDAP входит через `LDAP-main` и получает роль по группам LDAP;
- если пользователь не найден в LDAP, проверяется `RADIUS-main`;
- если RADIUS-сервер отказал, проверяется `TACACS-main`;
- если пользователя нет на внешних серверах (для RADIUS и TACACS+ — также при отказе сервера) или серверы недоступны, проверяется `Local`;
- после первого успешного шага остальные шаги не проверяются.

Предупреждение

Если логин есть сразу в нескольких источниках, результат зависит от порядка шагов:

- пользователь RADIUS или TACACS+, логин которого есть в LDAP без группы из правил, получит отказ в авторизации на шаге `LDAP-main`.

Поэтому логины в разных источниках не должны совпадать.

Если вход не удается, проверьте журнал событий Angie ADC (см. *Аудит действий пользователей*). Для каждого шага цепочки в нем записывается событие аудита с `resource aaa` и `operation authenticate_step` или `authorize_step`: имя профиля, результат шага и переход к следующему.

6.4.4.4 Аутентификация (режим без цепочек)

Примечание

Здесь описан устаревший режим с одним провайдером, который действует, пока не включены цепочки аутентификации и авторизации. Если цепочки включены, см. *Режим цепочек аутентификации и авторизации*.

При использовании внешней аутентификации данные о пользователях хранятся на внешнем сервере аутентификации. У системы нет доступа к данным пользователя. Для включения внешней аутентификации необходимо добавить в веб-интерфейс предварительно настроенный сервер аутентификации. Поддерживаются RADIUS, TACACS+ и LDAP. После этого при входе в веб-интерфейс будет доступен выбор аутентификации через заданный сервер.

Предупреждение

Необходимо также включить и настроить *авторизацию* для внешних пользователей. Если авторизация не настроена, пользователи не смогут получить доступ к системе.

Включение внешней аутентификации

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.

   Откроется страница с настройками аутентификации и авторизации для внешних пользователей.

2. Включите переключатель `Внешняя аутентификация` и выберите провайдера аутентификации.

> **Примечание**
>
> В режиме без цепочек одновременно поддерживается использование только одного провайдера внешней аутентификации. При добавлении нового провайдера аутентификации настройки предыдущего провайдера сбрасываются.

3. Заполните нужные поля.

   Для RADIUS-аутентификации укажите следующие параметры сервера:

   - `Сервер`: IP-адрес или доменное имя RADIUS-сервера.
   - `Порт`: порт подключения к RADIUS-серверу (по умолчанию `1812`).
   - `Протокол`: протокол передачи данных: `UDP` или `TCP` (по умолчанию: `UDP`).
   - `NAS-идентификатор`: идентификатор NAS (Network Access Server), передаваемый серверу RADIUS.
   - `Метод аутентификации`: поддерживается только `PAP`.
   - `Секрет`: общий секрет для шифрования паролей.

   Для TACACS+-аутентификации укажите следующие параметры сервера:

   - `Сервер`: IP-адрес или доменное имя TACACS+-сервера.
   - `Порт`: порт подключения к TACACS+-серверу (по умолчанию `49`).
   - `Секрет`: общий секрет для шифрования паролей.

   Для LDAP-аутентификации укажите параметры LDAP-сервера, сервисной учетной записи и параметры поиска пользователей:

   - `Сервер`: IP-адрес или доменное имя LDAP-сервера.
   - `Порт`: порт подключения к LDAP-серверу (по умолчанию `389`).
   - `Режим защиты соединения` (по умолчанию `Без TLS`, также доступны варианты `LDAPS` и `StartTLS`).
   - `DN сервисной учетной записи`: логин сервисной учетной записи, от имени которой система подключается к LDAP.
   - `Пароль сервисной учетной записи`: пароль сервисной учетной записи для подключения к LDAP-серверу.
   - `Базовый DN пользователя`: задает ветку на LDAP-сервере, в которой система будет искать пользователя, например `ou=users,dc=example,dc=com`.
   - `Идентификатор логина`: поле в LDAP, которое содержит логин, например `uid`, `sAMAccountName` или `userPrincipalName`.
   - `Фильтр поиска`: LDAP-фильтр для поиска пользователя, например `(&(objectClass=user)(sAMAccountName=%s))`.

> **Примечание**
>
> Фильтр LDAP определяет, в каком формате пользователь должен вводить логин при входе в систему:
>
> - если используется фильтр `(&(objectClass=user)(sAMAccountName=%s))`, то логин будет без доменного имени, например `ivanov`;

- если используется фильтр `(&(objectClass=user)(userPrincipalName=%s))`, то логин будет полным: `ivanov@domain.com`.

Чтобы проверить подключение к LDAP-серверу с указанными параметрами, нажмите `Проверить подключение`.

4. Нажмите `Сохранить`.

Внешняя аутентификация с использованием настроенного провайдера будет включена. При входе в веб-интерфейс пользователю будет необходимо выбрать нужный тип аутентификации и ввести свои логин и пароль. Если пользователь с таким логином и паролем будет найден на заданном сервере, то аутентификация пройдет успешно.

Изменение параметров внешней аутентификации

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.

   Откроется страница с настройками аутентификации и авторизации для внешних пользователей.

2. Внесите необходимые изменения и нажмите `Сохранить`.

   Параметры внешней аутентификации будут обновлены.

Отключение внешней аутентификации

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.

   Откроется страница с настройками аутентификации и авторизации для внешних пользователей.

2. Переведите переключатель `Внешняя аутентификация` в положение "выключено".

Внешняя аутентификация будет отключена.

6.4.4.5 Авторизация (режим без цепочек)

Примечание

Здесь описан устаревший режим с одним провайдером, который действует, пока не включены цепочки аутентификации и авторизации. Если цепочки включены, см. *Режим цепочек аутентификации и авторизации*.

Поддерживаются провайдеры *RADIUS*, *TACACS+* и *LDAP*.

Примечание

RADIUS-авторизация доступна только при аутентификации через RADIUS.

Предупреждение

Необходимо также включить и настроить *аутентификацию* для внешних пользователей. Если аутентификация не настроена, пользователи не смогут войти в систему.

Совместимость внешних провайдеров аутентификации и авторизации:

Провайдер аутентификации	Совместимые провайдеры авторизации
RADIUS	RADIUS, LDAP, TACACS+
LDAP	LDAP, TACACS+
TACACS+	LDAP, TACACS+

Примечание

В режиме без цепочек одновременно поддерживается использование только одного провайдера. При добавлении нового провайдера настройки предыдущего провайдера сбрасываются.

В этой статье:

- *LDAP-авторизация*
- *TACACS+-авторизация*
- *RADIUS-авторизация*
- *Выключение внешней авторизации*

LDAP-авторизация

Роли внешних пользователей определяются на основе принадлежности к LDAP-группам.

Чтобы настроить LDAP-авторизацию для внешних пользователей, необходимо:

- включить внешнюю аутентификацию;
- включить внешнюю авторизацию и подключить LDAP-сервер;
- задать настройки сервисной учетной записи для подключения Angie ADC к LDAP-серверу;
- задать базовый DN и фильтры для поиска пользователей и групп на LDAP-сервере;
- настроить соответствие LDAP-групп и ролей пользователей в Angie ADC.

Примечание

На стороне LDAP-сервера также должны быть настроены пользователи, группы и сервисная учетная запись для Angie ADC.

Настройка LDAP-авторизации

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.

   Откроется страница с настройками аутентификации и авторизации для внешних пользователей.

2. В блоке `Внешняя авторизация` переведите переключатель в положение "включено" и выберите провайдера авторизации LDAP.

3. Задайте параметры подключения к серверу:

   - `Сервер`: IP-адрес или доменное имя LDAP-сервера.
   - `Порт`: порт подключения к LDAP-серверу (по умолчанию `389`).

4. Укажите параметры защиты соединения: `Без TLS` (по умолчанию) или `LDAPS`/`StartTLS`, если необходимо использовать безопасное соединение при подключении к серверу.

> **Примечание**
>
> При выборе режима защиты соединения `LDAPS` или `StartTLS` становится доступен флажок `Проверять TLS-сертификат`. По умолчанию флажок установлен.

5. Укажите DN учетной записи, с которой будет выполняться подключение к LDAP-серверу (`DN сервисной учетной записи`).

   Можно использовать учетную запись администратора LDAP-сервера, например `cn=admin,dc=example,dc=com`.

6. Укажите пароль сервисной учетной записи (`Пароль пользователя bind`).

7. В блоке `Поиск пользователя` укажите следующие параметры:

   - `Базовый DN пользователей`, например `ou=users,dc=example,dc=com`;
   - `Фильтр поиска пользователей`, например `(uid=%s)`.

8. В блоке `Поиск групп` укажите следующие параметры:

   - `Базовый DN групп`, например `ou=groups,dc=example,dc=com`;
   - `Фильтр поиска групп`, например `(member=%s)`.

9. В блоке `Маппинг ролей LDAP` нажмите `Добавить правило` и задайте соответствие LDAP-групп пользователей ролям в Angie ADC. Например, если на LDAP-сервере для администраторов создана группа `dn: cn=<group_name>,ou=groups,dc=example,dc=com`, то укажите значение `cn=<group_name>,ou=groups,dc=example,dc=com` в поле `DN группы` и выберите роль `Администратор (admin)`.

10. Нажмите `Сохранить`.

Внешняя авторизация будет настроена и включена. При входе внешнего пользователя в систему на LDAP-сервере будет выполняться поиск групп, в которых он состоит. Если найденные группы совпадают с группами, указанными в маппинге, то пользователю будет назначена соответствующая роль. Если пользователь не найден ни в одной из групп или LDAP-группы недоступны или некорректны, доступ к системе будет запрещен.

TACACS+-авторизация

Роли для внешних пользователей определяются на основе соответствия атрибутам этих пользователей в TACACS+.

Чтобы настроить TACACS+-авторизацию для внешних пользователей, необходимо:

- включить внешнюю аутентификацию;
- включить внешнюю авторизацию и подключить TACACS+-сервер;
- настроить соответствие атрибутов TACACS+ ролям пользователей в Angie ADC.

На стороне TACACS+-сервера также должны быть настроены пользователи и их атрибуты.

Пример настройки:

```
group = admin {
    service = shell {
        set priv-lvl = 15
    }
}

user = admin {
    password = clear admin
    member = admin
}
```

Настройка TACACS+-авторизации

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.

   Откроется страница с настройками аутентификации и авторизации для внешних пользователей.

2. В блоке `Внешняя авторизация` переведите переключатель в положение "включено" и выберите провайдера авторизации TACACS.

3. Задайте параметры подключения к серверу:

   - `Сервер`: IP-адрес или доменное имя TACACS+-сервера.
   - `Порт`: порт подключения к TACACS+-серверу (по умолчанию `49`).
   - `Секрет`: общий секрет для шифрования паролей.

4. Укажите в порядке приоритета атрибуты ролей пользователя в TACACS+, например `priv-lvl`, затем `role`. По этим атрибутам Angie ADC будет определять роль для пользователя.

5. Укажите, какой сервис и протокол будут использоваться в запросе на авторизацию (AUTHOR). Параметры зависят от выбранного сервера. Например, для TACACS+ рекомендуется указать `service=shell` и `protocol=ip`.

6. Задайте соответствие значений атрибутов TACACS+ ролям в Angie ADC, например `priv-lvl=15` → `Администратор` или `role=adc-admin` → `Администратор`.

7. Нажмите `Сохранить`.

Внешняя авторизация будет настроена и включена. При входе внешнего пользователя в систему на TACACS+-сервер будет отправлен запрос на авторизацию. Если атрибуты и значения в ответе TACACS+ совпадают с указанными в маппинге, то пользователю будет назначена соответствующая роль в Angie ADC. Если полученные данные не совпадают с указанными в маппинге или TACACS+-сервер недоступен, доступ к системе будет запрещен.

RADIUS-авторизация

Роли для внешних пользователей определяются на основе соответствия атрибутам этих пользователей в RADIUS.

Чтобы настроить RADIUS-авторизацию для внешних пользователей, необходимо:

- включить внешнюю аутентификацию через RADIUS;
- включить внешнюю авторизацию через RADIUS;
- настроить соответствие атрибутов RADIUS ролям пользователей в Angie ADC.

Допускается использование следующих атрибутов ролей:

- `Filter-Id` — роль пользователя.
- `Class` — группа, к которой относится пользователь.
- `Service-Type` — тип сервиса, по которому определяется роль пользователя (Administrative, Login и др.).
- `Tunnel-Private-Group-ID` — VLAN ID (используется для VLAN-авторизации).
- `VSA` — Vendor-Specific в формате `vsa:<vendorID>:<vendorType>` (например `vsa:9:1`).

На стороне RADIUS-сервера также должны быть настроены пользователи и их атрибуты.

Пример:

```
user1 Cleartext-Password := "P@ssword"
    Filter-Id := "adc-admin",
    Service-Type := Administrative-User,
    Cisco-AVPair := "shell:priv-lvl=15",
    Reply-Message := "Welcome, Admin",
    Class := "AdminGroup",
    Tunnel-Type := VLAN,
    Tunnel-Medium-Type := IEEE-802,
    Tunnel-Private-Group-ID := "100"

user2 Cleartext-Password := "P@ssword"
    Filter-Id := "adc-readonly",
    Service-Type := NAS-Prompt-User,
    Cisco-AVPair := "shell:priv-lvl=7",
    Reply-Message := "Welcome, Supervisor",
    Class := "SupervisorGroup",
    Tunnel-Type := VLAN,
    Tunnel-Medium-Type := IEEE-802,
    Tunnel-Private-Group-ID := "200"
```

Настройка RADIUS-авторизации

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.

   Откроется страница с настройками аутентификации и авторизации для внешних пользователей.

2. В блоке `Внешняя авторизация` переведите переключатель в положение "включено" и выберите провайдера авторизации RADIUS.

3. Укажите атрибут роли пользователя в RADIUS, например `Filter-Id`, `vsa:9:1` или другой используемый атрибут. По этому атрибуту Angie ADC будет определять роль для пользователя.

4. Задайте соответствие значений атрибутов RADIUS ролям в Angie ADC, например, для Filter-Id укажите `adc-admin` → `Администратор`, а при использовании `vsa:9:1` укажите `shell:priv-lvl=15` → `Администратор`.

5. Нажмите `Сохранить`.

Внешняя авторизация будет настроена и включена. При входе внешнего пользователя в систему через RADIUS будут получены атрибуты его роли. Если атрибуты и значения совпадают с указанными в маппинге, то пользователю будет назначена соответствующая роль в Angie ADC. Если данные не совпадают с указанными в маппинге или RADIUS-сервер недоступен, доступ к системе будет запрещен.

Выключение внешней авторизации

1. Откройте веб-интерфейс Angie ADC. В панели навигации перейдите в раздел `Система` → `Аутентификация и авторизация`.

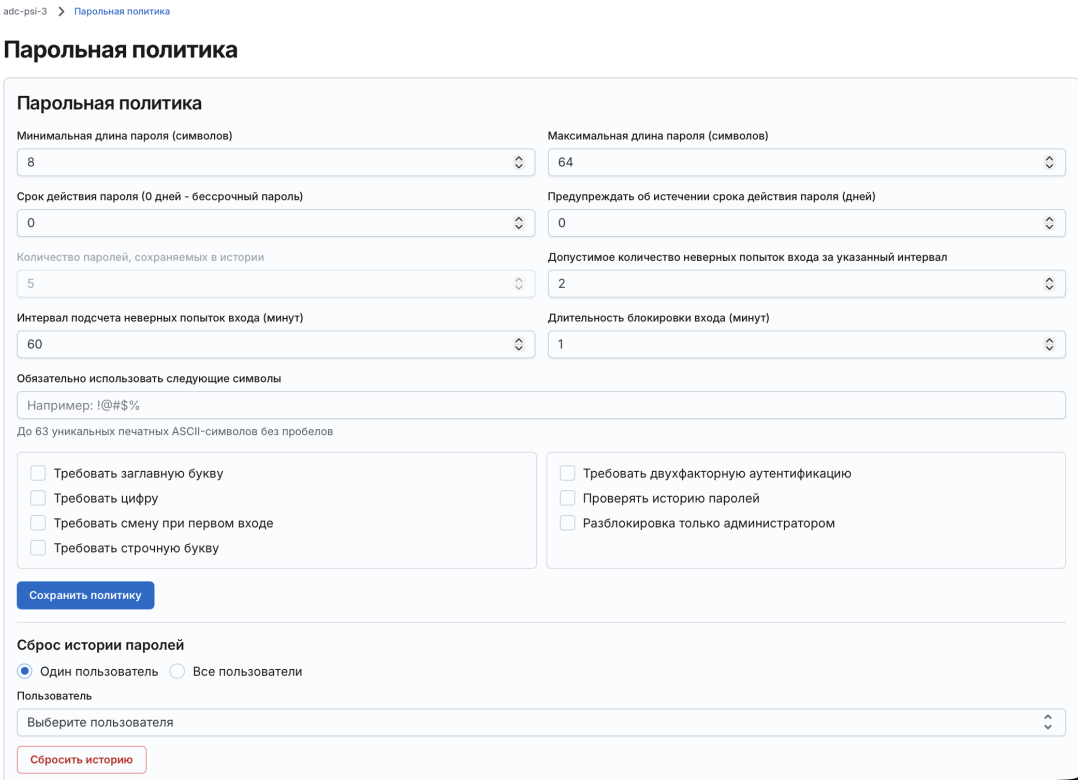
   Откроется страница с настройками аутентификации и авторизации для внешних пользователей.

2. В блоке `Внешняя авторизация` переведите переключатель в положение "выключено".

Внешняя авторизация будет отключена. При входе в систему для внешних пользователей будет отображаться сообщение, что доступ запрещен.

6.4.5 Парольная политика

Angie ADC поддерживает парольную политику для локальных пользователей Angie ADC. Парольная политика начинает действовать сразу при запуске Angie ADC со значениями по умолчанию. Требования к паролям пользователей можно донастроить в соответствии с политикой безопасности в вашей организации в разделе `Система` → `Парольная политика`.



По умолчанию действуют следующие требования: пароль не может совпадать с логином без учета регистра, заданы минимальная длина пароля (8 символов) и максимальная длина пароля (64 символа), а также допустимое количество попыток входа и параметры блокировки пользователя:

- интервал, за который считаются неверные попытки входа пользователя (60 минут);
- допустимое количество попыток входа пользователя (2 попытки);
- длительность блокировки пользователя (1 минута).

> **Примечание**
>
> При таких параметрах пользователь, который в течение 60 минут три раза ввел неправильный пароль, будет заблокирован на одну минуту. При этом после разблокировки пользователя счетчик неправильных попыток **не сбрасывается**, пока не закончится указанный интервал (60 минут). При следующем вводе неправильного пароля в течение этих 60 минут пользователь будет заблокирован сразу.

> **Важно**
>
> Парольная политика распространяется только на *локальных пользователей Angie ADC* текущего тенанта на всех узлах *кластера*.

6.4.5.1 Настройка парольной политики

1. Перейдите в раздел `Система` → `Парольная политика`.
2. Настройте **требования к составу** пароля:
   - Укажите значения в полях `Минимальная длина пароля (символов)` (по умолчанию 8 символов) и `Максимальная длина пароля` (по умолчанию 64 символа).
   - Если необходимо задать более высокий уровень безопасности пароля, установите флажки `Требовать заглавную букву` (A-Z), `Требовать строчную букву` (a-z) и `Требовать цифру` (0-9).
   - Если необходимо, укажите дополнительные требования в поле `Обязательно использовать следующие символы` (можно указать до 63 уникальных печатных ASCII-символов без пробелов).
3. Установите флажок `Требовать смену при первом входе`, чтобы система запрашивала смену предустановленного пароля при первом входе пользователя в веб-интерфейс.
4. Настройте **срок действия пароля** и напоминание о необходимости сменить пароль:
   - Укажите значение в поле `Срок действия пароля`.

     Значение `0` — срок действия пароля не ограничен (бессрочно).

     При указании срока действия пароля система будет напоминать о скором окончании срока за 7 дней до его истечения.
   - Укажите значение в поле `Предупреждать об истечении срока действия пароля`.

     Значение `0` — предупреждение отключено; любое другое значение — количество дней, прошедшее с последней смены пароля, после которого система будет напоминать о необходимости сменить пароль.
5. Настройте **требования к истории паролей** и **защиту от повторения**:
   - Установите флажок `Проверять историю паролей`, чтобы включить хранение истории паролей.
   - Укажите значение в поле `Количество паролей, сохраняемых в истории` (по умолчанию 5).

     Это значение будет определять, сколько паролей подряд не может повторяться. Значение `0` — количество хранимых паролей не ограничено.
6. Настройте допустимое **количество попыток входа** и **параметры блокировки** пользователя:
   - В поле `Интервал подсчета неверных попыток входа` укажите, за какое время система будет подсчитывать попытки входа пользователя (по умолчанию 60 минут).
   - В поле `Допустимое количество неверных попыток входа за указанный интервал` укажите разрешенное количество попыток входа за это время (по умолчанию 2).

     > **Примечание**
     >
     > При сбросе пароля администратором счетчик неправильных попыток ввода пароля тоже сбрасывается.

   - В поле `Длительность блокировки входа` укажите, на какое время блокировать пользователя, превысившего количество разрешенных попыток входа (по умолчанию 1 минута).
   - Установите флажок `Разблокировка только администратором`, если хотите, чтобы заблокированных пользователей можно было разблокировать только вручную. В таком случае поле `Длительность блокировки входа` не будет учитываться.

7. Если необходимо, установите флажок `Требовать двухфакторную аутентификацию`.

   При входе в веб-интерфейс пользователям будут предложены QR-код и секрет для подключения приложения-аутентификатора и дальнейшей аутентификации в системе через одноразовый пароль из этого приложения. Например, можно использовать приложения-аутентификаторы Яндекс.Ключ, Google Authenticator или Multifactor.

   > **Важно**
   >
   > После пяти неудачных попыток ввода одноразового кода в течение пяти минут пользователь будет заблокирован на пять минут.

8. Нажмите `Сохранить политику`.

Политика будет сохранена и применена сразу.

6.4.5.2 Сброс истории паролей для пользователей

Администратор может вручную сбросить историю паролей пользователя.

1. Перейдите в раздел `Система` → `Парольная политика`.
2. В блоке `Сброс истории паролей` укажите, для кого вы хотите сбросить историю:
   - `Один пользователь` (необходимо выбрать пользователя из списка).
   - `Все пользователи` (будет сброшена история паролей для всех локальных пользователей Angie ADC).
3. Нажмите `Сбросить историю`.

6.4.5.3 Сброс пароля локального пользователя

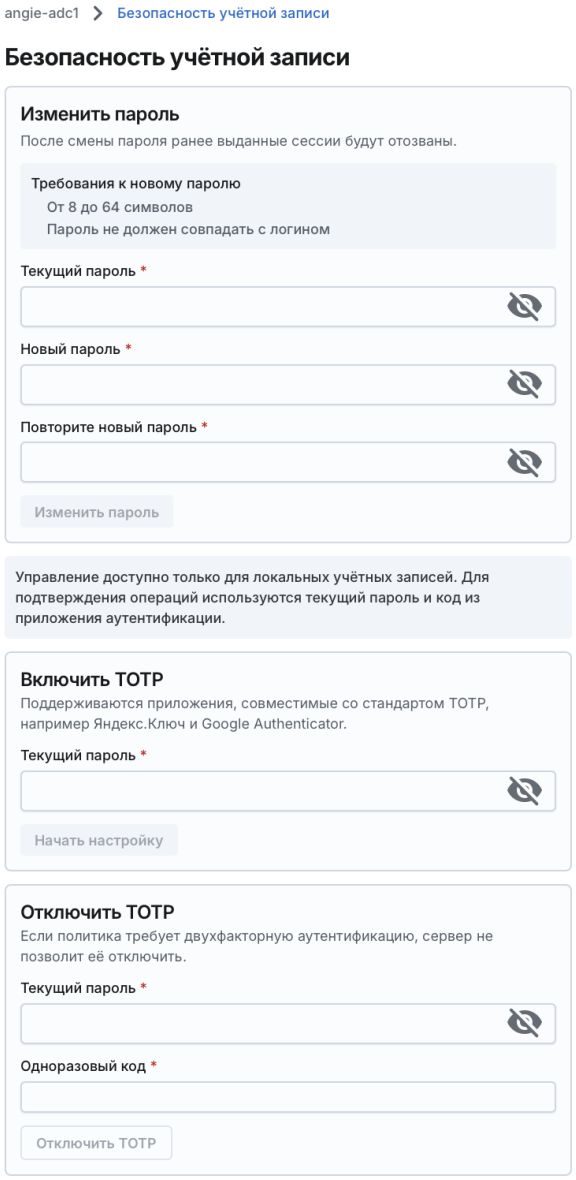
Администратор может *вручную сбросить пароль* для локального пользователя, например, если пользователь забыл пароль. После этого пользователь должен заново войти в систему с новым паролем, назначенным администратором.

6.4.5.4 Сброс настроек двухфакторной аутентификации локального пользователя

Администратор может *вручную сбросить настройки двухфакторной аутентификации* для локального пользователя, например, если пользователь больше не имеет доступа к подключенному приложению для аутентификации. После этого пользователь должен заново войти в систему и настроить двухфакторную аутентификацию, если этого требует *парольная политика*.

6.4.6 Настройка учетной записи

Angie ADC позволяет настраивать безопасность учетной записи. Настройки текущей учетной записи находятся в меню в верхнем правом углу веб-интерфейса (`Безопасность учетной записи`).



Важно

Настройка учетной записи доступна только локальным пользователям Angie ADC.

Поддерживается:

- Смена пароля учетной записи.
- Включение и выключение двухфакторной аутентификации для учетной записи.

Примечание

Выключение двухфакторной аутентификации возможно, если она не требуется *по парольной политике*.

6.4.6.1 Смена пароля учетной записи

1. В верхнем правом углу веб-интерфейса нажмите на значок с символом логина текущей учетной записи и выберите `Безопасность учетной записи`.

   Откроется окно настройки безопасности для текущей учетной записи.

2. Введите текущий пароль, новый пароль, повторите новый пароль и нажмите `Изменить пароль`.

   Новый пароль не должен повторять текущий пароль, не должен повторять логин без учета регистра и должен соответствовать *требованиям парольной политики*. В случае прохождения всех проверок пароль будет изменен и текущая пользовательская сессия будет завершена.

3. Войдите в систему с новым паролем.

Совет

Администратор может *вручную сбросить пароль* для локального пользователя, например, если пользователь забыл пароль. После этого пользователь должен заново войти в систему с новым паролем, назначенным администратором.

6.4.6.2 Включение двухфакторной аутентификации

Для включения двухфакторной аутентификации можно использовать, например, приложения Яндекс.Ключ, Google Authenticator или Multifactor.

Важно

После пяти неудачных попыток ввода одноразового кода в течение пяти минут пользователь будет заблокирован на пять минут. Коды восстановления не поддерживаются.

1. В верхнем правом углу веб-интерфейса нажмите на значок с символом логина текущей учетной записи и выберите `Безопасность учетной записи`.

   Откроется окно настройки безопасности для текущей учетной записи.

2. В блоке `Включить TOTP` введите пароль от текущей учетной записи и нажмите `Начать настройку`.

   Отобразятся QR-код и секрет для подключения приложения-аутентификатора.

3. Отсканируйте QR-код в приложении-аутентификаторе на своем мобильном телефоне. Если вы работаете на компьютере, то вместо QR-кода скопируйте и введите в приложении секрет.

4. Вернитесь в Angie ADC и введите одноразовый код аутентификации из приложения-аутентификатора.

5. Нажмите `Подтвердить и включить`.

   Двухфакторная аутентификация будет включена для текущей учетной записи. Текущая пользовательская сессия будет завершена.

6. Войдите в систему заново, введя свой пароль и одноразовый код.

Совет

Администратор может *вручную сбросить настройки двухфакторной аутентификации* для локального пользователя, например, если пользователь больше не имеет доступа к подключенному приложению для аутентификации. После этого пользователь должен заново войти в систему и настроить двухфакторную аутентификацию, если этого требует *парольная политика*.

6.4.6.3 Отключение двухфакторной аутентификации

1. В верхнем правом углу веб-интерфейса нажмите на значок с символом логина текущей учетной записи и выберите `Безопасность учетной записи`.

   Откроется окно настройки безопасности для текущей учетной записи.

2. В блоке `Отключить TOTP` введите пароль от текущей учетной записи, одноразовый код из подключенного приложения-аутентификатора и нажмите `Отключить TOTP`.

   Двухфакторная аутентификация для текущей учетной записи будет отключена. Текущая пользовательская сессия будет завершена.

3. Войдите в систему заново, введя свой пароль.

6.4.7 Аудит действий пользователей

Действия пользователей, выполняемые в веб-интерфейсе, записываются в журнал событий Angie ADC и имеют помету `"msg":"audit"`.

Примечание

На данный момент логируются только действия, выполняемые через API. В дальнейших релизах будет реализовано логирование действий пользователей, выполняемых через CLI.

Просмотреть журнал событий можно *через CLI*. Для этого необходимо ввести команды `logs` → `adc-server`.

При *отправке на syslog-сервер* события аудита помечаются с помощью пользовательской категории `facility=local4` (в соответствии с RFC 3164). Вы можете настроить фильтрацию по `facility=local4` на своем syslog-сервере для обработки только аудит-логов.

В сообщениях аудита выводятся следующие поля:

- `time` — время фиксации события.
- `level` — уровень критичности события: всегда `INFO` (информационное событие).
- `msg` — тип события: всегда `audit` (аудит действий пользователя).
- `app` — устройство, на котором произошло событие.
- `node_id` — имя устройства, на котором произошло событие.
- `actor_id` — идентификатор пользователя, инициировавшего событие.
- `actor_name` — имя пользователя, инициировавшего событие.
- `actor_auth_source` — тип аутентификации пользователя, например локальная или RADIUS.
- `resource` — категория объекта, к которому относится операция.
- `operation` — выполняемая операция, например `read`, `update`, `delete`.
- `mutating` — изменяет ли выполняемая операция систему (`true`, `false`).
- `resource_id` — идентификатор конкретного экземпляра объекта, если применимо.

- `actor_host` — IP-адрес клиента.
- `client_channel` — канал взаимодействия, например веб-интерфейс, CLI или межсервисный вызов.
- `duration_ms` — время выполнения операции в миллисекундах.
- `result` — результат выполнения (`OK`, `InvalidArgument`).
- `stage` — стадия выполнения операции: `pre` — намерение выполнить действие, `post` — результат выполнения.
- `request_id` — идентификатор запроса, связывающий события одной операции.
- `trace_id` — идентификатор цепочки выполнения запроса.
- `span_id` — идентификатор конкретной операции внутри цепочки выполнения запроса.

6.5 Резервное копирование и восстановление системы

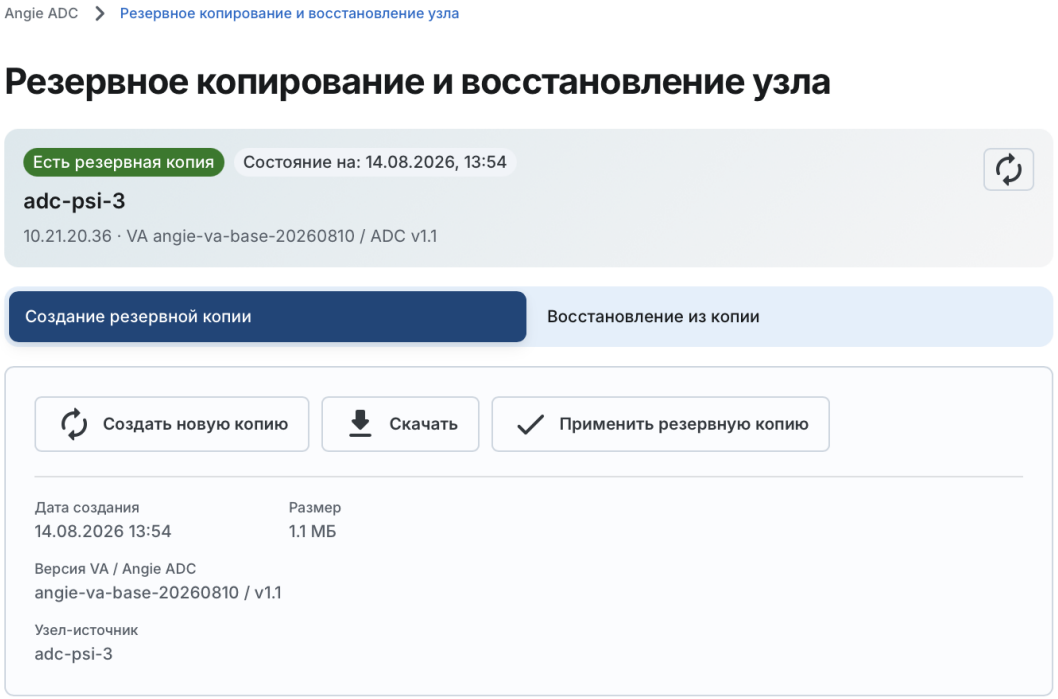
Для защиты от сбоев и возврата к стабильному состоянию в Angie ADC предусмотрены механизмы резервного копирования и восстановления узлов. Они позволяют выполнить следующие задачи:

- Резервное копирование: создание копии текущего узла.
- Откат изменений: восстановление работоспособности текущего узла из сохраненной копии в случае сбоя.
- Миграция узла: перенос резервной копии на новое оборудование.

В этой статье:

- *Создание резервной копии*;
- *Обновление резервной копии*;
- *Скачивание резервной копии*;
- *Восстановление текущего узла из резервной копии*;
- *Перенос резервной копии на новый узел*.

6.5.1 Создание резервной копии



Важно

Рекомендуется создавать или обновлять резервную копию узла перед внесением в систему значительных изменений.

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Резервное копирование и восстановление`.
2. Выберите `Создание резервной копии` и нажмите `Создать копию`.

   Будет запущен процесс создания резервной копии текущего узла.

После завершения процесса отобразится информация о созданной копии:

- дата создания;
- размер;
- версия VA и версия Angie ADC в копии;
- узел-источник копии (hostname).

6.5.2 Обновление резервной копии

Примечание

Поддерживается хранение только одной резервной копии узла, при загрузке новой копии предыдущая удаляется.

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Резервное копирование и восстановление`.

2. Выберите `Создание резервной копии` и нажмите `Создать новую копию`.

   Будет запущен процесс создания новой резервной копии текущего узла. Старая копия будет удалена.

После завершения процесса отобразится информация о новой копии:

- дата создания;
- размер;
- версия VA и версия Angie ADC в копии;
- узел-источник копии (hostname).

6.5.3 Скачивание резервной копии

Вы можете скачать резервную копию текущего узла, чтобы затем применить ее на новом узле.

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Резервное копирование и восстановление`.
2. Выберите `Создание резервной копии`.

   Отобразится информация о текущей резервной копии.
3. Если необходимо, обновите копию, нажав `Создать новую копию`.
4. Нажмите `Скачать`.

   Будет загружен файл `.tar`, содержащий текущую резервную копию узла.

6.5.4 Восстановление текущего узла из резервной копии

1. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Резервное копирование и восстановление`.
2. Выберите `Создание резервной копии` и нажмите `Применить резервную копию`.
3. В открывшемся окне подтвердите операцию, нажав `Начать восстановление`.

После завершения восстановления система перезагрузится. Веб-интерфейс будет доступен по прежнему адресу.

> **Примечание**
>
> Если восстановление завершилось с ошибкой, то по кнопке `Скачать лог` вы можете загрузить файл `restore.log` и получить диагностическую информацию.
>
> Если в процессе восстановления был потерян доступ к веб-интерфейсу, то файл `restore.log` можно просмотреть *через мастер настройки*.

6.5.5 Перенос резервной копии на новый узел

При переносе резервной копии на новый узел он станет полной копией исходного узла:

- сохранятся IP-адреса и сетевая конфигурация исходного узла;
- будут перенесены все данные и настройки;
- если узел был в *паре высокой доступности*, то пара восстановится;
- если узел был в *кластере*, то соседи снова будут видеть этот узел как исходный.

Важно

Не поддерживается перенос резервной копии одного узла кластера на другой, уже существующий узел этого кластера. Для переноса резервной копии необходимо развернуть новый узел. Исходный узел при этом нужно отключить, чтобы избежать конфликта IP-адресов.

Шаги:

1. Разверните Angie ADC на новом узле и назначьте временный IP-адрес для веб-интерфейса. Другие настройки не требуются.

   При восстановлении из резервной копии рекомендуется, чтобы версия VA и версия Angie ADC в копии и на новом узле совпадали.

2. В веб-интерфейсе Angie ADC перейдите в раздел `Система` → `Резервное копирование и восстановление`.

3. Выберите `Восстановление из копии` и загрузите файл `.tar`, содержащий резервную копию узла, который вы хотите восстановить.

   Система проверит файл и отобразит сводную таблицу с основными параметрами текущего узла и загруженной копии.

4. Если были выявлены критические несовпадения и необходимо заменить копию на более подходящую, нажмите `Заменить файл` и загрузите новый архив.

   Не рекомендуется начинать восстановление, если версии VA или Angie ADC не совпадают.

5. Нажмите `Начать восстановление`.

После завершения восстановления система перезагрузится. Веб-интерфейс будет доступен по адресу, который использовался в копии. В статусе узла будет отображаться `Восстановлен из копии`.

Примечание

Если восстановление завершилось с ошибкой, то по кнопке `Скачать лог` вы можете загрузить файл `restore.log` и получить диагностическую информацию.

Если в процессе восстановления был потерян доступ к веб-интерфейсу, то файл `restore.log` можно просмотреть *через мастер настройки*.

Совет

- Чтобы просмотреть данные копии, которая использовалась для восстановления, перейдите в блок `Восстановление из копии`.
- Чтобы заново запустить восстановление из копии, в блоке `Восстановление из копии` нажмите `Заменить файл` и загрузите архив еще раз.

ГЛАВА 7

Мастер настройки по SSH

Мастер настройки позволяет управлять конфигурацией Angie ADC без доступа к веб-интерфейсу.

Для входа в мастер необходимо перейти в консоль виртуальной машины и в окне входа в мастер ввести предустановленные логин `setup` и пароль `setup`. Чтобы выйти из мастера настройки Angie ADC, нажмите `exit` в основном меню.

При первом запуске Angie ADC вам необходимо настроить хотя бы один *сетевой интерфейс* для доступа к веб-интерфейсу Angie ADC.

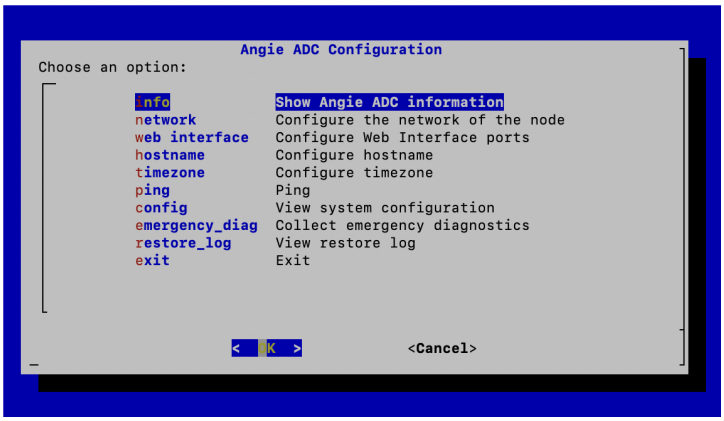
При расширенной настройке вы можете настроить дополнительные параметры:

- *Настройка сети узла* (интерфейсы, бонды, VLAN-интерфейсы, домены маршрутизации и сеть управления, DNS-серверы);
- *Смена портов для веб-интерфейса Angie ADC*;
- *Изменение имени устройства Angie ADC*;
- *Изменение часового пояса*;
- *Проверка доступности узла*;
- *Просмотр конфигурации Angie ADC и сетевых настроек*.

Также доступны **журналы событий**:

- *Аварийная диагностика*;
- *Просмотр журнала восстановления из резервной копии*.

7.1 Меню мастера

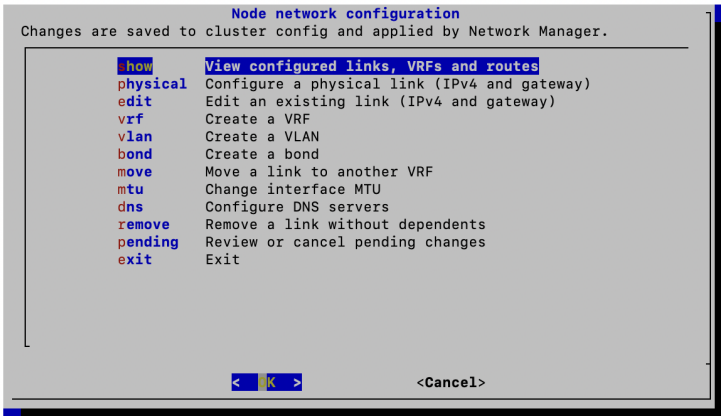


Основное меню мастера настройки Angie ADC содержит следующие команды:

- `info` — просмотр общей информации об Angie ADC.
- `network` — переход к настройке сети узла: интерфейсов, доменов маршрутизации, бондов, VLAN-интерфейсов и DNS.
- `web interface` — изменение порта для веб-интерфейса Angie ADC.
- `hostname` — смена имени устройства.
- `timezone` — смена часового пояса.
- `ping` — проверка доступности узла.
- `config` — просмотр конфигурации Angie ADC и сетевых настроек.
- `emergency_diag` — аварийный сбор логов для передачи в техническую поддержку.
- `restore_log` — просмотр журнала восстановления узла из резервной копии.
- `exit` — выход из мастера.

7.2 Настройка сети узла

Подменю `network` позволяет настраивать сеть узла, а также просматривать текущий статус (`network` → `show`), проверять и отменять изменения, ожидающие применения (`network` → `pending`). Изменения сохраняются в кластерную конфигурацию.



- `show` — просмотр настроенных интерфейсов, доменов маршрутизации и маршрутов.

- `physical` — настройка физического интерфейса (IPv4-адрес или DHCP и шлюз).
- `edit` — изменение настроенного интерфейса (IPv4-адрес или DHCP и шлюз).
- `vrf` — создание домена маршрутизации.
- `vlan` — создание VLAN-интерфейса.
- `bond` — создание бонда.
- `move` — перенос интерфейса в другой домен маршрутизации.
- `mtu` — изменение MTU интерфейса.
- `dns` — настройка DNS-серверов.
- `remove` — удаление интерфейса, от которого не зависят другие интерфейсы.
- `pending` — просмотр и отмена изменений, ожидающих применения.
- `exit` — выход из меню `network`.

7.2.1 Первоначальная настройка

При первом запуске при переходе в подменю `network` система просит задать имя узла в кластере (не влияет на hostname) и запускает узел. Затем можно переходить к *настройке сетевых интерфейсов*.

7.2.2 Настройка сетевых интерфейсов

Чтобы настроить физический сетевой интерфейс Angie ADC:

1. Выберите в основном меню пункт `network`.
2. В меню настройки сети выберите пункт `physical` и затем выберите нужный интерфейс.
3. Укажите адрес интерфейса:
   - IPv4-адрес с длиной префикса, например `192.0.2.10/24`;
   - `dhcp` — получать настройки от DHCP-сервера;
   - `none` — добавить интерфейс без адреса.

   Пустое значение оставляет текущий адрес.
4. Укажите IPv4-адрес шлюза. Значение `none` удаляет шлюз, пустое значение оставляет текущий; при выборе `dhcp` пустое значение удаляет заданный вручную шлюз. Для интерфейса без адреса (`none`) шлюз не задается.
5. Подтвердите изменения.

Чтобы изменить уже настроенный интерфейс:

Выберите `network` → `edit`. Адрес и шлюз задаются так же, как в пункте `physical`, кроме значения `none`: оно доступно только в `physical`.

Чтобы изменить MTU интерфейса:

Выберите `network` → `mtu`.

Чтобы удалить интерфейс:

Выберите `network` → `remove`.

Примечание

Удалить можно только интерфейс, от которого не зависят другие интерфейсы, например VLAN-интерфейсы или бонды.

7.2.3 Выделение сети управления

Чтобы вынести управление узлом в отдельную сеть, необходимо перенести интерфейс управления в предустановленный домен маршрутизации `mgmt`.

Для этого:

1. Выберите в основном меню пункт `network`.
2. Выберите пункт `move`, затем выберите интерфейс и домен маршрутизации `mgmt`.
3. Подтвердите изменения.

   Веб-интерфейс, CLI и аварийный SSH будут доступны только через указанный интерфейс.

> **Предупреждение**
>
> Перед переносом интерфейса в `mgmt` убедитесь, что у вас есть доступ к узлу через эту сеть. Если узел уже входит в кластер, интерфейс, через который он подключен к кластеру, перенести в `mgmt` нельзя: он должен оставаться в общей сети.

7.2.4 Создание домена маршрутизации

Чтобы создать дополнительный *домен маршрутизации*:

1. Выберите в основном меню пункт `network`.
2. Выберите пункт `vrf`, укажите имя домена маршрутизации и подтвердите операцию.

Чтобы перенести интерфейс в созданный домен маршрутизации:

1. Выберите в основном меню пункт `network`.
2. Выберите пункт `move` и укажите интерфейс и домен маршрутизации, а затем подтвердите операцию.

7.2.5 Создание бондов

При создании бондов используется протокол LACP (802.3ad) и режим active (интерфейс инициирует создание агрегированного канала).

Чтобы объединить несколько физических интерфейсов в один логический интерфейс (бонд):

1. Выберите в основном меню пункт `network`.
2. Выберите пункт `bond`.
3. Выберите интерфейсы, которые необходимо объединить (максимум 8 интерфейсов), и подтвердите создание бонда.

> **Примечание**
>
> Рекомендуется объединять в бонд ненастроенные сетевые интерфейсы.

7.2.6 Создание VLAN-интерфейсов

Чтобы создать VLAN-интерфейс:

1. Выберите в основном меню пункт `network`.
2. Выберите пункт `vlan`, укажите родительский интерфейс и VLAN ID и подтвердите операцию.

7.2.7 Настройка DNS-серверов

Чтобы задать DNS-серверы узла:

1. Выберите в основном меню пункт `network`.
2. Выберите пункт `dns` и укажите адреса DNS-серверов.
3. Подтвердите изменения.

7.3 Просмотр конфигурации Angie ADC и сетевых настроек

Чтобы просмотреть текущую конфигурацию Angie ADC или конфигурацию systemd-networkd для заданных сетей, выполните следующие действия:

1. Выберите в основном меню пункт `config`.

   Откроется список доступных действий:

   - `system` — просмотр сетевой конфигурации Angie ADC.
   - `network` — просмотр конфигурации systemd-networkd для заданных сетей.
   - `back` — выход из меню `config`.

2. Выберите `system`, чтобы просмотреть текущую конфигурацию Angie ADC.
3. Выберите `network` → `<имя сети>`, чтобы просмотреть настройки systemd-networkd для этой сети.

7.4 Смена портов для веб-интерфейса Angie ADC

Вы можете назначить для веб-интерфейса Angie ADC любой незанятый порт. Чтобы изменить порты по умолчанию, выполните следующие действия:

1. Выберите в основном меню пункт `web interface`.

   Откроется список доступных действий:

   - `set` — назначение новых портов.
   - `reset` — восстановление настроек по умолчанию.
   - `logs` — просмотр журнала.
   - `back` — выход из меню `web interface`.

2. Выберите `set`, укажите новые значения портов и примените настройки.

7.5 Изменение имени устройства Angie ADC

Чтобы изменить имя устройства Angie ADC, выполните следующие действия:

1. Выберите в основном меню пункт `hostname`.
2. В открывшемся окне введите новое имя устройства и сохраните изменения.

7.6 Изменение часового пояса

Чтобы изменить часовой пояс узла, выполните следующие действия:

1. Выберите в основном меню пункт `timezone`.
2. Выберите нужный часовой пояс и подтвердите изменения.

7.7 Проверка доступности узла

Чтобы проверить доступность узла с помощью ping-запроса, выполните следующие действия:

1. Выберите в основном меню пункт `ping`.
2. В открывшемся окне введите имя или IP-адрес узла, доступность которого нужно проверить.

7.8 Аварийная диагностика

Для случаев, когда нет доступа к CLI и веб-интерфейсу Angie ADC, в мастере предусмотрена возможность получения аварийных логов. Будет собран архив, содержащий системные метрики, конфигурацию системы и системный журнал.

Чтобы получить архив:

1. В основном меню выберите пункт `emergency_diag`.
2. Дождитесь создания архива. После этого в мастере отобразятся имя архива, порт SFTP и срок, в течение которого архив доступен для скачивания (15 минут). Через 15 минут архив будет удален.

   Примечание

   При повторном запуске команды `emergency_diag` в течение 15 минут текущий архив будет удален и будет создан новый архив.

3. Подключитесь по SFTP под учетной записью `setup`:

   ```
   $ sftp -P 2223 setup@<IP-адрес>
   ```

   Примечание

   Если был настроен интерфейс управления, используйте его IP-адрес.

4. Проверьте наличие архива (команда `ls`) и скачайте его:

   ```
   sftp> get diag_YYYYMMDD_HHMMSS.tar.gz
   ```

Для штатного сбора диагностической информации используйте команду *diag*.

7.9 Просмотр журнала восстановления из резервной копии

Для случаев, когда после восстановления узла из резервной копии пропал доступ к веб-интерфейсу Angie ADC, в мастере предусмотрена возможность просмотреть журнал восстановления.

Чтобы просмотреть журнал восстановления, выберите в основном меню пункт `restore_log`.

На экране отобразится содержимое файла `restore.log`.

ГЛАВА 8

Создание и масштабирование кластера

Кластер Angie ADC состоит из нескольких узлов (устройств Angie ADC). Один из узлов кластера является точкой входа в кластер (к нему подключаются остальные узлы кластера). Кластер позволяет настраивать несколько устройств Angie ADC с любого узла через общую кластерную конфигурацию, в которую входят:

- конфигурация GSLB;
- сертификаты;
- пользователи SNMP;
- конфигурация мониторинга доступности;
- настройки парольной политики.

Подробнее о работе с кластером см. *Управление кластером*.

Развертывание кластера состоит из следующих этапов:

1. Первоначальная настройка узла Angie ADC.
2. *Создание точки входа в кластер на одном из узлов*.
3. *Добавление остальных узлов в кластер*.

8.1 Создание точки входа в кластер

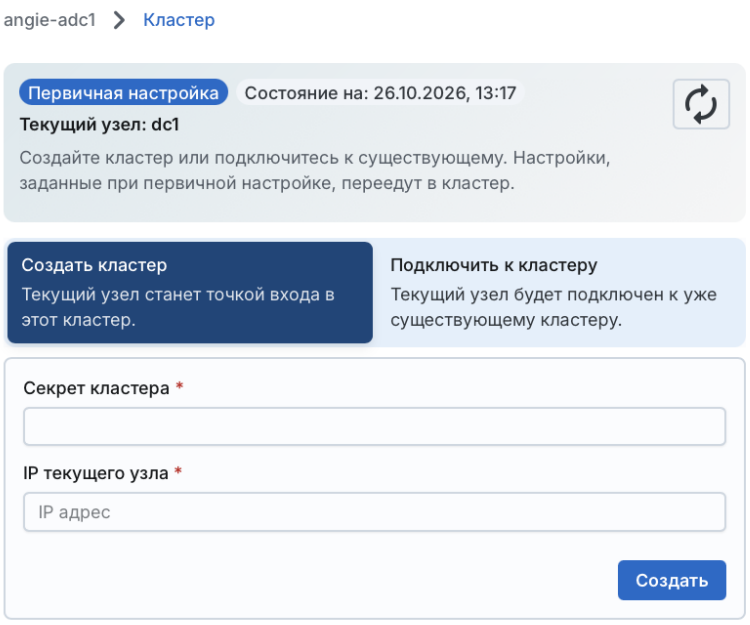
Предупреждение

После создания точки входа ее нельзя изменить, кластер нельзя расформировать. Внимательно проверьте все параметры перед созданием точки входа.

Чтобы создать точку входа в кластер, выполните следующие действия:

1. Откройте веб-интерфейс Angie ADC на узле, который будет точкой входа.

   Откроется экран с информацией о текущем узле и вариантами его интеграции в кластер.



2. Выберите сценарий `Создать кластер` и заполните следующие поля:
   - Секрет для подключения к кластеру.
   - IP-адрес текущего узла (только IPv4).

   Важно

   В качестве IP-адреса текущего узла нельзя использовать *IP-адрес интерфейса управления*, если он был настроен.

3. Нажмите `Создать`.

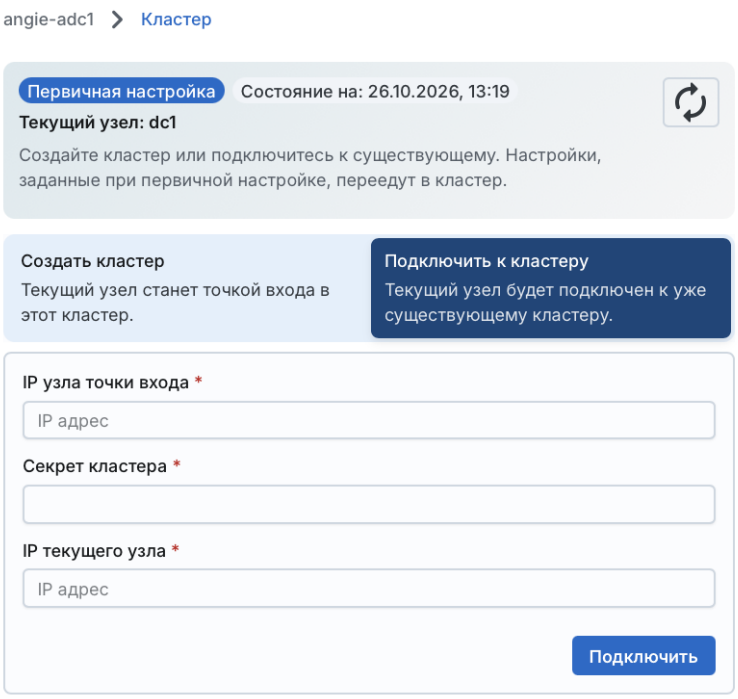
   Будет создан кластер. Текущий узел будет назначен точкой входа в кластер.

8.2 Добавление узлов в кластер

Для каждого последующего узла кластера выполните следующие действия:

1. Перейдите на узел Angie ADC, который вы хотите добавить в кластер.

   Откроется экран с информацией о текущем узле и вариантами его интеграции в кластер.



2. Выберите сценарий `Подключить к кластеру` и заполните следующие поля:
   - IP-адрес узла точки входа (только IPv4).
   - Секрет для подключения к кластеру.
   - IP-адрес текущего узла (только IPv4).

   Важно

   В качестве IP-адреса текущего узла нельзя использовать *IP-адрес интерфейса управления*, если он был настроен.

3. Нажмите `Подключить`.

Узел будет подключен к кластеру.

ГЛАВА 9

Интерфейс командной строки (CLI) Angie ADC

Интерфейс командной строки Angie ADC доступен по SSH на портах 2222 и 22.

Возможности: автодополнение команд по `TAB`; поддержка истории команд; подсказки по синтаксису команд по нажатию `?`; поддержка цветовой схемы; поддержка сокращенных команд.

Запуск CLI

Чтобы запустить интерфейс командной строки (CLI), выполните следующие действия:

1. Подключитесь к SSH-серверу:

   ```
   ssh -p 2222 user@localhost
   ```

2. После подключения сервер запросит пароль для авторизации. Введите пароль:

   ```
   user@localhost's password:
   #
   ```

   Если авторизация прошла успешно, откроется терминал Angie ADC. Справка доступна по `?`.

9.1 Поддерживаемые команды

Ниже приведен список команд в алфавитном порядке.

Основные команды:

1. *certificates*	Управление сертификатами `traffic` в Angie ADC
list	Вывод списка сертификатов
info	Просмотр информации о сертификате
upload	Загрузка сертификата и ключа
remove	Удаление сертификата и ключа
2. *configuration*	Режим настройки узла: сетевые настройки, VRRP и динамическая маршрутизация
end	Выход из режима настройки `configuration`

продолжается на следующей странице

Таблица 1 – продолжение с предыдущей страницы

no ha standby	Снятие ограничений резервного узла, оставшихся после расформирования пары высокой доступности
routing	Динамическая маршрутизация узла: BGP, OSPF, списки префиксов и карты маршрутов
set	Добавление или изменение параметра: интерфейсы, бонды, маршруты, правила маршрутизации
unset	Удаление параметра
vrrp	Группы VRRP узла
3. *diagnostics*	Сетевая диагностика
arping	Отправка ARP-запросов сетевым хостам.
diag	Общая диагностика системы.
nslookup	Выполнение DNS-запросов.
ping	Выполнение команды `ping`.
pingc	Выполнение команды `ping` в стиле Cisco.
ss	Просмотр информации о сетевых соединениях, портах и статистике сетевых сокетов.
ssldump	Анализ SSL/TLS-трафика.
tcpdump	Анализ сетевого трафика.
traceroute	Трассировка маршрута следования пакетов.
4. *firewall*	Управление правилами брандмауэра
list	Вывод списка правил брандмауэра Angie ADC
no open	Закрытие порта в брандмауэре Angie ADC
open	Открытие порта в брандмауэре Angie ADC
save	Сохранение правил брандмауэра Angie ADC
5. *ip*	Стандартное управление сетевыми интерфейсами, маршрутами, адресами и правилами IP-трафика в Linux
6. *logs*	Просмотр журналов
7. *modules*	Просмотр информации о динамических модулях
info	Получение информации о динамическом модуле Angie ADC
list	Получение списка доступных динамических модулей Angie ADC
8. *ps*	Отображение информации о процессах, запущенных в системе
9. *settings*	Просмотр и изменение системных настроек Angie ADC (NTP, отладка, настройка времени и т. д.)
angie debug	Включение режима отладки для локального балансировщика нагрузки
no angie debug	Отключение режима отладки
reload	Перезагрузка элементов Angie ADC
sysctl	Просмотр и настройка параметров ядра Linux
syslog	Управление syslog/Logstash-серверами логирования.
10. *show*	Просмотр состояния динамической маршрутизации и групп VRRP
11. *system*	Управление системой Angie ADC
bond	Просмотр состояния бонда
hostname	Просмотр и установка имени узла
ntp	Просмотр и настройка NTP

продолжается на следующей странице

Таблица 1 – продолжение с предыдущей страницы

reboot	Перезагрузка системы Angie ADC
stat	Просмотр статистики системы Angie ADC
time	Просмотр и установка системного времени
timezone	Просмотр и установка часового пояса узла
upgrade	Обновление Angie ADC
version	Просмотр версии Angie ADC
11. *transfer*	Работа с директорией `transfer`
edit	Редактирование файла в текущей директории.
ls	Получение списка файлов в директории `transfer`
rm	Удаление файла в директории `transfer`
view	Просмотр содержимого файла в директории `transfer`
12. *trusted-ca*	Работа с доверенными сертификатами
upload	Загрузка доверенного сертификата
list	Вывод списка загруженных доверенных сертификатов
info	Вывод информации о загруженном доверенном сертификате
remove	Удаление загруженного доверенного сертификата
13. *web*	Настройка веб-интерфейса Angie ADC
upload	Загрузка сертификата управления и ключа
tls	Включение / выключение HTTPS

Служебные команды:

`exit` или `Ctrl+Z`	Выход из контекста
`quit` или `Ctrl+Q`	Завершение сессии
`?`	Список доступных команд

9.2 Синтаксис

```
command option0 {option1|option2|...|option N} [option3] [{option4|option5|...|option M}] [option6 <user-input1>] [<user-input2>] <user-input3>
```

Параметры:

`command`	команда
`option0`	обязательный параметр
`{option1|option2|...|option N}`	выбор из списка обязательных параметров
`[option3]`	необязательный параметр
`[{option4|option5|...|option M}]`	выбор из списка необязательных параметров
`[option6 <user-input1>]`	необязательный параметр с пользовательским аргументом
`[<user-input2>]`	необязательный пользовательский аргумент
`<user-input3>`	обязательный пользовательский аргумент

9.3 certificates

Контекст `certificates` позволяет управлять сертификатами, используемыми Angie ADC.

Поддерживаемые команды:

`certificates`	Вход в контекст
list	Вывод списка сертификатов `traffic` в Angie ADC
info	Просмотр информации о сертификате
upload	Загрузка сертификата и ключа
remove	Удаление сертификата и ключа

9.3.1 list

Вывод списка сертификатов `traffic` Angie ADC.

Синтаксис: `list`.

Пример:

```
(certificates)$$ list
Name   Validity                  Uploaded    Paths
-----  ------------------------  ----------  ----------------------------------
cert1  18.02.2025 - 18.02.2027  06.08.2026  /etc/angie-lb/crt/active/cert1.crt
                                            /etc/angie-lb/crt/active/cert1.key
```

9.3.2 info

Просмотр информации о сертификате.

Синтаксис: `info <name>`.

Параметры:

- `<name>` — имя сертификата.

Пример:

```
(certificates)$$ info cert1
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C = RU, ST = Moscow, O = Angie, OU = EVO, CN = Root CA
        Validity
            Not Before: Feb 18 12:23:08 2025 GMT
            Not After : Feb 18 12:23:08 2027 GMT
        Subject: CN = Demo Certificate, ST = Moscow, C = RU, O = Angie, OU = EVO
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
...
(certificates)$$
```

9.3.3 upload

Загрузка сертификатов и ключей Angie ADC.

> **Примечание**
>
> Для работы с сертификатами необходимо предварительно создать кластер Angie ADC. Подробнее см. в статье *Создание и масштабирование кластера*.

Синтаксис: `upload <name>`.

Параметры:

- `<name>` — имя, назначаемое сертификату.

Для загрузки сертификата или ключа необходимо вставить текст сертификата или ключа в строку, затем вставить пустую строку или написать `END` в новой строке.

Пример:

```
(certificates)$$ upload cert1
 Certificate (PEM):
 Insert PEM data line by line at the end of the input, add an empty line or enter END
 -----BEGIN CERTIFICATE-----
 MIIF9TCCA92gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJSVTEP
 ...
 Z7SIEeCr84fIlxFMpRxNGZhJQ67xWLwQmjVcphi037Wpx+6dmQRtp8Q=
 -----END CERTIFICATE-----

 Private key (PEM):
 Insert PEM data line by line at the end of the input, add an empty line or enter END
 -----BEGIN PRIVATE KEY-----
 MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQDA9J1JqGANy5uf
 ...
 AgjJ9gmjlDd6t1dNCwLVxc8thGVWSw==
 -----END PRIVATE KEY-----


 Certificate 'cert1' uploaded successfully
 (certificates)$$
```

При загрузке ключа и сертификата проверяется их корректность. В случае некорректного значения сертификат или ключ не будет сохранен.

9.3.4 remove

Удаление сертификатов и ключей Angie ADC.

Синтаксис: `remove <name>`.

Параметры:

- `<name>` — имя сертификата.

Пример:

```
(certificates)$$ remove cert1
Certificate 'cert1' deleted successfully
```

9.4 configuration

Режим настройки узла. Команды режима меняют настройки этого узла, которые хранятся в *кластерной конфигурации*. Каждая команда передает изменение в кластер и ждет, пока узел его применит.

Если узел не применил изменение за 120 секунд, команда завершается с ошибкой, а кластер продолжает повторять попытки. Такое изменение можно отменить в веб-интерфейсе.

Пример:

```
$$ configuration
## set system interface enp0s2 ip address 10.21.20.31/22
## set system interface enp0s2 ip gateway 10.21.20.1
## end
```

Поддерживаемые команды:

`configuration`	Вход в режим настройки
end	Выход из режима настройки `configuration`
no ha standby	Снятие ограничений резервного узла, оставшихся после расформирования пары высокой доступности
routing	Настройка динамической маршрутизации узла
set	Добавление или изменение параметра: интерфейсы, бонды, маршруты, правила маршрутизации
unset	Удаление параметра
vrrp	Настройка групп VRRP узла

9.4.1 end

Выход из режима `configuration`.

9.4.2 no ha standby

После расформирования пары высокой доступности бывший резервный узел держит свои группы VRRP выключенными и ограничивает анонсы динамической маршрутизации (см. *Динамическая маршрутизация в паре высокой доступности*). Команда снимает эти ограничения. Команда недоступна, пока узел входит в пару.

Синтаксис: `no ha standby`.

9.4.3 routing

Динамическая маршрутизация узла: BGP, OSPF, списки префиксов и карты маршрутов. Команда меняет настройки динамической маршрутизации этого узла в кластерной конфигурации. Удаление выполняется командами `no routing` (см. ниже). Порядок настройки и примеры см. в *Настройка динамической маршрутизации* и *Настройка RHI*.

Ограничения:

- BGP запускается командой `routing bgp asn <n>`; остальные команды `routing bgp` до этого отклоняются.
- Сосед BGP создается командой `routing bgp neighbor <ipv4> remote-as <n>`; остальные параметры соседа задаются после нее.
- Процесс OSPF запускается командой `routing ospf <instance>`, номер процесса — от 1 до 10.
- Интерфейсы в `ospf ... interface` и `update-source interface` должны быть заданы в сетевых настройках узла и находиться в домене маршрутизации по умолчанию.
- Префиксы и адреса соседей — только IPv4.
- `recovery` задается только вместе с `upstream`; по умолчанию используется `manual`.

Синтаксис:

- `routing prefix-list <name> seq <seq> {permit|deny} <prefix> [ge <n>] [le <n>] [upstream <upstream>] [recovery {automatic|manual}]` — список префиксов. С параметром `upstream` префикс отзывается, когда указанный upstream недоступен; `recovery` определяет, возвращается ли анонс автоматически или вручную.

- `routing route-map <name> {permit|deny} <seq> [match-prefix-list <name>] [local-preference <n>] [metric <n>]` — карта маршрутов.
- `routing bgp {asn <n> | router-id <ipv4> | network <prefix>}` — параметры BGP.
- `routing bgp redistribute {connected|static|kernel} [metric <n>] [route-map <name>]` — перераспределение маршрутов в BGP.
- `routing bgp neighbor <ipv4> {remote-as <n> | update-source {<ipv4> | interface <link>} | timers <keepalive> <hold> | password <password> | route-map <name> {in|out} | route-reflector-client | next-hop-self [force] | advertise-map <name> exist-map <name>}` — параметры соседа BGP.
- `routing ospf <instance>` — запуск процесса OSPF.
- `routing ospf <instance> {router-id <ipv4> | network <prefix> area <n> | default-information [always]}` — параметры процесса OSPF.
- `routing ospf <instance> redistribute {connected|static|kernel} [metric <n>] [route-map <name>]` — перераспределение маршрутов в OSPF.
- `routing ospf <instance> interface <link> {area <n> | cost <n> | passive | md5-key <key_id> <password>}` — параметры интерфейса OSPF.
- `routing show` — вывод раздела динамической маршрутизации узла.
- `routing show withdrawn` — вывод отозванных префиксов.
- `no routing prefix-list <name> seq <seq> withdrawn` — возврат отозванного префикса в анонс.

Удаление: у параметров со значением в команде `no` указывается только имя параметра, без значения.

- `no routing prefix-list <name> [seq <seq>]` — удаление списка префиксов или его записи; список без записей удаляется целиком.
- `no routing route-map <name> [<seq>]` — удаление карты маршрутов или ее записи; карта без записей удаляется целиком.
- `no routing bgp` — удаление BGP целиком.
- `no routing bgp {router-id | network <prefix> | redistribute {connected|static|kernel}}` — удаление параметра BGP.
- `no routing bgp neighbor <ipv4> [update-source | timers | password | route-reflector-client | next-hop-self | advertise-map]` — удаление параметра соседа; без параметра — удаление соседа.
- `no routing bgp neighbor <ipv4> route-map {in|out}` — удаление карты маршрутов соседа.
- `no routing ospf <instance>` — удаление процесса OSPF.
- `no routing ospf <instance> {router-id | network <prefix> | redistribute {connected|static|kernel} | default-information}` — удаление параметра процесса OSPF.
- `no routing ospf <instance> interface <link> [area | cost | passive | md5-key]` — удаление параметра интерфейса OSPF; без параметра — удаление интерфейса из OSPF.

Например: `no routing bgp neighbor 192.0.2.1 password`, `no routing ospf 1 interface ens5 cost`.

Состояние маршрутизации можно посмотреть командой *show*.

9.4.4 set

Добавление или изменение параметра: интерфейсы, бонды, маршруты, правила маршрутизации. Команда меняет настройки сети этого узла в кластерной конфигурации.

Синтаксис: `set system <system_input> | ip <ip_input>`, где:

- `system <system_input>` — настройка интерфейсов и бондов;
- `ip <ip_input>` — настройка маршрутов и правил маршрутизации.

Возможные варианты `<system_input>`:

- `set system interface <name> {type {static | dhcp} | ip <keyword> <value> | vlan <id> | mtu <value>}` — настройка интерфейса.
  - Возможные значения для `<keyword>`:
    - `address` — IP-адрес интерфейса в формате CIDR;
    - `gateway` — шлюз интерфейса;
    - `dns` — адрес DNS-сервера;
    - `searches` — домены поиска (до 10 доменов).
  - `type static` — используется по умолчанию. Этот параметр можно не указывать явно.
  - `type dhcp` — удаляет все IP-параметры интерфейса и включает режим автоматического получения настроек с DHCP-сервера.
  - `vlan <id>` — VLAN-интерфейс поверх указанного интерфейса, `<id>` от 1 до 4094.
  - `mtu <value>` — MTU интерфейса, от 68 до 65536.
  - `ip address` принимает только IPv4-адреса. Для интерфейса `lo` доступен только этот параметр: дополнительные адреса сервисов с префиксом `/32`. IPv6-адреса, в том числе адреса `/128` на `lo`, задаются в веб-интерфейсе (см. *Адреса сервисов на интерфейсе lo*).
- `set system bond <number> iface <interface> <interface> ...` — бонд из 2–8 интерфейсов.

Примеры:

```
$$ configuration
## set system interface enp0s2 ip address 10.21.20.39/22
## set system interface enp0s2 ip gateway 10.21.20.1
## set system interface enp0s2 ip dns 8.8.8.8
## set system interface enp0s2 ip searches angie.software.ru
## set system interface enp0s2 vlan 100
## set system interface lo ip address 192.0.2.10/32
## set system bond 0 iface ens6 ens7
```

Возможные варианты `<ip_input>`:

- `rule from <address> table <value>` — установка правила.
- `route <address> {nexthop <address> | interface <name>} [table <value>] [type local]` — установка маршрута. Минимально необходимо задать адрес и `nexthop` или `interface`, остальные параметры (таблица маршрутизации и тип маршрута) опциональны.

Пример:

```
$$ configuration
## set ip rule from 0.0.0.0/0 table 100
## set ip route 0.0.0.0/0 nexthop 10.90.90.90
```

9.4.5 unset

Удаление параметра узла.

Синтаксис: `unset system interface <name> [<parameter>] | unset system bond <number> | unset ip <ip_input>`.

Пример:

```
$$ configuration
## unset ip rule from 0.0.0.0/0 table 100
## unset system interface enp0s2 vlan 100
## unset system interface lo ip address 192.0.2.10/32
```

9.4.6 vrrp

Группы VRRP узла. Группа определяется идентификатором VRID и интерфейсом. Подробнее см. *Команды VRRP*.

Синтаксис:

- `vrrp <vrid> interface <link> address <address>` — виртуальный адрес группы;
- `vrrp <vrid> interface <link> {priority | version | advertisement-interval} <value>` — приоритет узла, версия протокола VRRP (2 или 3) и интервал анонсов в миллисекундах;
- `vrrp <vrid> interface <link> {preempt | checksum-with-ipv4-pseudoheader | shutdown}` — флаги группы;
- `vrrp show` — вывод групп VRRP узла;
- `no vrrp <vrid> interface <link> [<parameter>]` — удаление группы или ее параметра: `priority`, `version` и `advertisement-interval` возвращаются к значениям по умолчанию, `preempt` и `checksum-with-ipv4-pseudoheader` выключаются, `no ... shutdown` снова включает группу. Флаги `preempt` и `checksum-with-ipv4-pseudoheader` включены по умолчанию.

Пример:

```
$$ configuration
## vrrp 10 interface ens5 address 198.18.5.100/24
## vrrp 10 interface ens5 priority 150
```

9.5 diagnostics

Контекст `diagnostics` позволяет проводить диагностику сети и анализировать сетевой трафик.

Поддерживаемые команды:

`diagnostics`	Вход в контекст
arping	Отправка ARP-запросов сетевым хостам.
diag	Общая диагностика системы.
nslookup	Выполнение DNS-запросов.
ping	Выполнение команды `ping`.
pingc	Выполнение команды `ping` в стиле Cisco.
ss	Просмотр информации о сетевых соединениях, портах и статистике сетевых сокетов.
ssldump	Анализ SSL/TLS-трафика.
tcpdump	Анализ сетевого трафика.
traceroute	Трассировка маршрута следования пакетов.

9.5.1 arping

Отправка ARP-запросов сетевым хостам.

Синтаксис: `arping [-c <count>] [-w <deadline>] [-t <interval>] [-if <interface>] [-src <source>] [-d] [-u] [-a] [-f] [-b] [-q] <target>`

Параметры:

- `-c <count>` — количество ARP-запросов для отправки перед завершением команды;
- `-w <deadline>` — максимальное время ожидания ответа в секундах;
- `-t <interval>` — интервал между отправкой запросов в секундах;
- `-if <interface>` — сетевой интерфейс, через который отправлять запросы;
- `-src <source>` — исходный IP-адрес для использования в запросах;
- `-d` — режим обнаружения дубликатов адресов;
- `-u` — режим незапрошенного ARP: отправка ARP-пакетов без ожидания ответа (для обновления ARP-кэша);
- `-a` — режим ответа ARP: команда будет отвечать на входящие ARP-запросы;
- `-f` — завершить выполнение при получении первого ответа;
- `-b` — широковещательный режим: отправка запросов на широковещательный адрес;
- `-q` — тихий режим: минимальный вывод информации;
- `<target>` — IP-адрес или имя хоста, к которому отправляются ARP-запросы (обязательный параметр).

Примеры:

- `(diagnostics)$$ arping 192.168.1.1` — проверка доступности хоста.
- `(diagnostics)$$ arping -c 5 -w 10 192.168.1.100` — отправка до 5 ARP-запросов и ожидание ответа не более 10 секунд.
- `(diagnostics)$$ arping -d 192.168.1.50` — проверка на дублирование адреса.
- `(diagnostics)$$ arping -u -if eth0 192.168.1.1` — незапрошенный ARP для обновления кэша.

9.5.2 diag

Выполнение общей диагностики. Собираются системные метрики, конфигурация системы и системный журнал за последние 24 часа. Информация сохраняется в файл `diag_<timestamp>.log`, например в папке `/var/transfer`.

Синтаксис: `diag`

9.5.3 nslookup

Выполнение DNS-запросов.

9.5.3.1 Разовый запрос

Синтаксис: `nslookup <host>`

Примеры:

- `(diagnostics)$$ nslookup example.com` — прямой DNS-запрос.
- `(diagnostics)$$ nslookup 203.0.113.10` — обратный DNS-запрос (PTR).

9.5.3.2 Интерактивный режим

В интерактивном режиме можно выполнять множественные DNS-запросы.

Переход в интерактивный режим: `(diagnostics)$$ nslookup`

Поддерживаемые команды интерактивного режима:

- `host [<server>]` — поиск информации о хосте с использованием текущего сервера по умолчанию или указанного сервера.
- `server <domain>` — изменение сервера по умолчанию. Для поиска информации о домене используется текущий сервер.
- `lserver <domain>` — изменение сервера по умолчанию. Для поиска информации о домене используется начальный сервер (тот, с которым запущен nslookup).
- `set keyword[=value]` — изменение параметров конфигурации, где `keyword` — имя параметра, `value` — значение (если поддерживается).

  Возможные варианты:

  - `set all` — вывод всех текущих настроек.
  - `set class=value` — изменение класса запроса.

    Доступные значения:

    * `IN` — класс Internet (по умолчанию);
    * `CH` — класс Chaos;
    * `HS` — класс Hesiod;
    * `ANY` — подстановочный знак.
  - `set [no]debug` — включение или выключение отображения полного пакета ответа. По умолчанию `nodebug`.
  - `set [no]d2` — включение или выключение режима отладки. По умолчанию `nod2`.
  - `set domain=<name>` — установка списка поиска доменов по умолчанию.
  - `set [no]search` — если запрос содержит хотя бы одну точку, но не заканчивается точкой, добавляет имена доменов из списка поиска доменов к запросу до получения ответа. По умолчанию `search`.
  - `set port=<value>` — изменение порта TCP/UDP-сервера имен (по умолчанию 53).
  - `set querytype=<value>` — изменение типа запроса информации. По умолчанию A, затем AAAA.
  - `set type=<value>` — изменение типа запроса информации. По умолчанию A, затем AAAA.
  - `set [no]recurse` — включение или выключение рекурсивных запросов. По умолчанию `recurse`.
  - `set ndots=<number>` — установка количества точек (разделителей меток) в домене, при котором поиск отключается. Абсолютные имена всегда останавливают поиск.
  - `set retry=<number>` — установка количества повторных попыток.
  - `set timeout=<number>` — изменение начального интервала ожидания ответа (в секундах).
  - `set[no]vc` — указывает, должен ли использоваться виртуальный канал при отправке запросов к серверу. По умолчанию `novc`.
  - `set [no]fail` — использовать ли следующий сервер имен, при ошибке на первом сервере. По умолчанию `nofail`.

9.5.4 ping

Выполнение команды `ping`.

Синтаксис: `ping [-c <count>] [-n] <hostname>`

Параметры:

- `-c <count>` — количество пакетов (по умолчанию бесконечно);
- `-n` — не резолвить имя хоста;
- `<hostname>` — имя хоста или IP-адрес.

9.5.5 pingc

Выполнение команды `ping` в стиле Cisco.

Синтаксис: `pingc {ip|ip6} <hostname> [count <n>]`

Параметры:

- `ip` — выполнение пинга через ipv4;
- `ip6` — выполнение пинга через ipv6;
- `<hostname>` — имя хоста или IP-адрес;
- `count <n>` — количество пакетов (по умолчанию 4).

9.5.6 ss

Позволяет получать детальную информацию о TCP/UDP-соединениях, открытых портах, процессах, использующих сеть, и статистике сетевых интерфейсов.

Синтаксис: `ss [-t] [-u] [-l] [-p] [-a] [-n] [-r] [-s] [-e] [-i] [-4] [-6] [-o] [-m] [-h] [<expression>]`

9.5.6.1 Параметры

- `-t` — отображение только TCP-соединений.
- `-u` — отображение только UDP-соединений.
- `-l` — отображение только прослушивающих сокетов.
- `-p` — отображение процесса (PID и имя программы), использующего сокет.
- `-a` — отображение всех сокетов: как установленных соединений, так и прослушивающих.
- `-n` — выводить только IP-адреса и номера портов.
- `-r` — разрешать IP-адреса и порты в имена (обратное `-n`).
- `-s` — отображение краткой статистики по протоколам (количество соединений, пакетов и т. д.).
- `-e` — расширенный вывод статистики с дополнительной информацией о соединениях.
- `-i` — отображение информации о сетевых интерфейсах.
- `-4` — отображение только IPv4-соединений.
- `-6` — отображение только IPv6-соединений.
- `-o` — отображение таймеров сокетов в выводе.
- `-m` — отображение использования памяти сокетами.
- `-h` — не отображать заголовки таблицы.
- `<expression>` — фильтрация результатов по `state` и по заданным критериям, оформляется кавычками `""`.

9.5.6.2 Примеры

Примеры:

- `(diagnostics)$$ ss -tulpn` — все TCP/UDP-соединения с процессами и портами.
- `(diagnostics)$$ ss -tlnp` — TCP-соединения в состоянии LISTEN.
- `(diagnostics)$$ ss "state listening"` — только прослушивающие соединения.
- `(diagnostics)$$ ss "dport = 80"` — соединения на порт 80.
- `(diagnostics)$$ ss "sport >= 1024"` — соединения с портом источника >= 1024.
- `(diagnostics)$$ ss "dst 192.168.1.1"` — соединения к хосту 192.168.1.1.
- `(diagnostics)$$ ss "src 10.0.0.0/8"` — соединения из сети 10.0.0.0/8.
- `(diagnostics)$$ ss "state established dport = 443"` — соединения, установленные на порт 443.
- `(diagnostics)$$ ss "fwmark = 0x01/0x03"` — соединения с определенной меткой fwmark.
- `(diagnostics)$$ ss -s` — статистика по протоколам.

9.5.6.3 Фильтрация по state

- `state all` — все состояния.
- `state connected` — все соединенные состояния.
- `state synchronized` — синхронизированные состояния.
- `state bucket` — состояния ожидания.
- `state big` — все возможные состояния.
- `state established` — установленное соединение.
- `state syn-sent` — отправлен SYN.
- `state syn-recv` — получен SYN.
- `state fin-wait-1` — ожидание первого FIN.
- `state fin-wait-2` — ожидание второго FIN.
- `state time-wait` — ожидание закрытия.
- `state closed` — закрытое соединение.
- `state close-wait` — ожидание закрытия.
- `state last-ack` — последний ACK.
- `state listening` — прослушивание.
- `state closing` — закрытие соединения.

9.5.6.4 Фильтрация по критериям

Фильтрация сокетов на основе определенных критериев. Выражение состоит из серии предикатов, объединенных логическими операторами.

Логические операторы (в порядке возрастания приоритета):

`or, |, ||`	логическое ИЛИ
`and, &, &&`	логическое И
`not, !`	логическое НЕ

Если между последовательными предикатами нет оператора, предполагается неявный оператор `and`. Подвыражения можно группировать с помощью скобок "(" и ")".

Предикаты:

`dst HOST | src HOST | dst=HOST | src=HOST`	Проверка соответствия адреса назначения или источника хосту HOST. HOST может быть IP-адресом, именем хоста или сетью в формате CIDR.
`dport OP PORT | sport OP PORT`	Сравнение порта назначения или источника с PORT. OP (оператор) может быть следующим: `<`, `<=`, `=`, `==`, `!=`, `>=`, `>` Например: `dport = 80`, `sport >= 1024`, `dport < 8080`.
`dev DEVICE | dev=DEVICE | dev!=DEVICE`	Совпадение по устройству (интерфейсу), которое использует соединение. DEVICE может быть именем устройства или индексом интерфейса.
`fwmark MASK | fwmark=MASK | fwmark!=MASK`	Совпадение по значению fwmark для соединения. MASK может быть конкретным значением метки или значением с маской битов. Например: `fwmark=0x01`, `fwmark=0x01/0x03` (проверка двух младших битов).
`cgroup PATH | cgroup=PATH | cgroup!=PATH`	Совпадение, если соединение является частью `cgroup` по указанному пути.
`cautobound`	Совпадение, если порт или путь исходного адреса был автоматически выделен (а не явно указан).

Операторы сравнения (все эквивалентны):

`=, ==, eq`	равно
`!=, ne, neq`	не равно
`>, gt`	больше
`<, lt`	меньше
`>=, ge, geq`	больше или равно
`<=, le, leq`	меньше или равно
`!, not`	отрицание
`|, ||, or`	логическое ИЛИ
`&, &&, and`	логическое И

Если оператор не указан, предполагается оператор `=`.

9.5.7 ssldump

Анализ SSL/TLS-трафика. Показывает содержимое SSL/TLS-пакетов, включая информацию о рукопожатии (handshake), сертификатах, используемых шифрах и зашифрованные данные. Результаты сохраняются в файлы `ssl_capture_<timestamp>.txt` и `ssl_capture_<timestamp>.pcap`.

Синтаксис: `ssldump [-i <interface>] [-n] [-e] [-h] [<expression>]`

Параметры:

- `-i <interface>` — сетевой интерфейс для захвата SSL/TLS-трафика.
- `-n` — показывать только IP-адреса (не выполнять разрешение доменных имен).
- `-e` — показывать время в читаемом формате вместо Unix timestamp.
- `-h` — показывать полные SSL-заголовки пакетов для детального анализа.
- `<expression>` — фильтр захвата, оформляется кавычками "". Синтаксис выражений фильтров см. документацию pcap-filter.

Примеры:

- `(diagnostics)$$ ssldump -i eth0` — захват всего SSL-трафика на eth0.

- `(diagnostics)$$ ssldump -i eth0 "host example.com"` — SSL-трафик для/от example.com.
- `(diagnostics)$$ ssldump -i eth0 "port 443"` — SSL-трафик на порт 443.
- `(diagnostics)$$ ssldump -h -i eth0 "tcp and port 443"` — полные заголовки SSL-пакетов.

9.5.8 tcpdump

Анализ сетевого трафика в реальном времени.

Синтаксис: `tcpdump [-i <interface>] [-c <count>] [-w <file>] [-v] [-vv] [-vvv] [-n] [-nn] [-x] [-e] [<expression>]`

Параметры:

- `-i <interface>` — указание сетевого интерфейса для захвата трафика (по умолчанию используется первый доступный интерфейс). Если интерфейс не указан, то команда будет использовать все доступные интерфейсы.
- `-c <count>` — количество пакетов для захвата перед автоматическим завершением команды.
- `-w <file>` — запись захваченных пакетов в файл в формате pcap.
- `-v` — подробный вывод: отображение дополнительной информации о пакетах.
- `-vv` — очень подробный вывод: расширенная информация о пакетах.
- `-vvv` — максимально подробный вывод: максимальный уровень детализации.
- `-n` — не выполнять разрешение доменных имен (DNS lookup): отображать только IP-адреса.
- `-nn` — не выполнять разрешение доменных имен и портов: отображать только IP-адреса и номера портов.
- `-x` — вывод пакетов в шестнадцатеричном формате для детального анализа содержимого.
- `-e` — отображение информации о канальном уровне (Ethernet-заголовки): MAC-адреса, тип фрейма и т. д.
- `<expression>` — фильтр захвата для ограничения типа перехватываемых пакетов, оформляется кавычками `""`. Синтаксис выражений фильтров см. документацию pcap-filter.

Примеры:

- `(diagnostics)$$ tcpdump -i eth0` — захват всего трафика на eth0.
- `(diagnostics)$$ tcpdump -i eth0 "host 192.168.1.1"` — трафик только для/от хоста 192.168.1.1.
- `(diagnostics)$$ tcpdump -i eth0 port 80` — трафик на порт 80 (HTTP).
- `(diagnostics)$$ tcpdump -i eth0 "tcp and port 443"` — TCP-трафик на порт 443 (HTTPS).
- `(diagnostics)$$ tcpdump -w capture.pcap -c 100` — записать 100 пакетов в файл.

9.5.9 traceroute

Трассировка маршрута следования пакетов до указанного сетевого узла.

Синтаксис: `traceroute [-i] [-t] [-u] [-4] [-6] [-n] [-d] [-m <max_hops>] [-q <nqueries>] [-p <port>] [-w <waittime>] [-if <interface>] [-s <source>] <target>`

Параметры:

- `-i` — ICMP-режим для трассировки (режим по умолчанию).
- `-t` — TCP-режим: отправка TCP-пакетов вместо ICMP.
- `-u` — UDP-режим: отправка UDP-пакетов.

- `-4` — принудительное использование IPv4.
- `-6` — принудительное использование IPv6.
- `-n` — не выполнять разрешение доменных имен: показывать только IP-адреса.
- `-d` — включение отладочной информации в вывод.
- `-m <max_hops>` — максимальное количество промежуточных узлов (hops) для проверки (по умолчанию 30).
- `-q <nqueries>` — количество запросов, отправляемых на каждый промежуточный узел (по умолчанию 3).
- `-p <port>` — указание порта для использования в TCP/UDP-режимах.
- `-w <waittime>` — время ожидания ответа от каждого узла в секундах (по умолчанию 3).
- `-if <interface>` — указание сетевого интерфейса для отправки пакетов.
- `-s <source>` — указание исходного IP-адреса для отправки пакетов.
- `<target>` — целевой IP-адрес или доменное имя узла, до которого выполняется трассировка (обязательный параметр).

Примеры:

- `(diagnostics)$$ traceroute -n -w 2 192.168.1.1` — трассировка без DNS, время ожидания 2 секунды.
- `(diagnostics)$$ traceroute -t -p 80 example.com` — TCP-трассировка на порт 80.

9.6 firewall

Контекст `firewall` позволяет управлять правилами брандмауэра Angie ADC.

Поддерживаемые команды:

`firewall`	Вход в контекст
list	Вывод списка правил брандмауэра Angie ADC
no open	Закрытие порта в брандмауэре Angie ADC
open	Открытие порта в брандмауэре Angie ADC
save	Сохранение правил брандмауэра Angie ADC

9.6.1 list

Вывод списка правил брандмауэра Angie ADC.

Синтаксис: `list {ip|ip6}`.

Параметры:

- `ip` — вывод списка правил для IPv4;
- `ip6` — вывод списка правил для IPv6.

Пример вывода:

```
(firewall)$$ list ip
tcp 9999 enp0s2
(firewall)$$
```

9.6.2 no open

Закрытие порта в брандмауэре Angie ADC.

Синтаксис: `no open {ip|ip6} {tcp|udp} <port> <interface>`.

Параметры:

- `ip` — порт для IPv4;
- `ip6` — порт для IPv6;
- `tcp` — порт для протокола TCP;
- `udp` — порт для протокола UDP;
- `<port>` — номер порта;
- `<interface>` — интерфейс.

Пример:

```
(firewall)$$ no open ip tcp 9999 enp0s2
Port 9999/tcp successfully closed on interface enp0s2
(firewall)$$ save
rules saved successfully
```

Примечание

Изменения будут применены сразу, но сохранены только после выполнения команды `save`.

9.6.3 open

Открытие порта в брандмауэре Angie ADC.

Синтаксис: `open {ip|ip6} {tcp|udp} <port> <interface>`.

Параметры:

- `ip` — порт для IPv4;
- `ip6` — порт для IPv6;
- `tcp` — порт для протокола TCP;
- `udp` — порт для протокола UDP;
- `<port>` — номер порта;
- `<interface>` — интерфейс.

Пример:

```
(firewall)$$ open ip tcp 9999 enp0s2
Port 9999/tcp successfully opened on interface enp0s2
(firewall)$$ save
rules saved successfully
```

Примечание

Изменения будут применены сразу, но сохранены только после выполнения команды `save`.

Примечание

При настройке конфигурации не занимайте следующие порты (используются внутренними сервисами Angie ADC):

TCP: 22, 199, 2222, 2601, 2602, 2603, 2604, 2605, 2606, 2615, 2616, 2617, 2619, 2623, 3050, 3051, 3053, 3054, 3060, 3111, 3122, 3123, 3301, 3302, 3380, 3391, 4460, 5044, 5355, 5432, 8010, 8080, 8443, 9090, 9100, 9120, 9600, 9633, 9898, 9900, 60080

- Порты 8080 и 8443 можно использовать, если у вас выделен отдельный *интерфейс управления*.

UDP: 53, 123, 161, 323, 546, 3784, 3785, 4784, 5355, 7784

9.6.4 save

Сохранение правил брандмауэра Angie ADC.

Синтаксис: `save`.

9.7 ip

Стандартное управление сетевыми интерфейсами, маршрутами, адресами и правилами IP-трафика в Linux.

Предупреждение

При перезагрузке Angie ADC настройки, выполненные через `ip`, не сохраняются. Для настройки системы рекомендуется использовать режим *configuration*.

9.8 logs

Позволяет просматривать журналы событий Angie ADC. Используйте эту команду для получения диагностической информации при обращении в службу технической поддержки.

Синтаксис: `logs <entity> [{follow|transfer}]`.

Поддерживается *фильтрация*.

Значения для `<entity>`:

`aaa-manager`	События модуля, отвечающего за аутентификацию и авторизацию внешних пользователей Angie ADC
`adc-gslb`	События модуля GSLB (глобальная балансировка)
`adc-server`	События модуля, обеспечивающего выполнение всего предоставляемого функционала Angie ADC (входная точка)
`adc-system`	События модуля, отвечающего за выполнение системных команд Angie ADC
`adc-tracker`	События модуля, отвечающего за RHI-функционал
`auth-dataplane`	События модуля, отвечающего за *аутентификацию клиентов* в балансировщике нагрузки
`certificate-manager`	События сервиса управления сертификатами
`ctrl-access`	События из access_log модуля, отвечающего за кластерное взаимодействие
`ctrl-error`	События из error_log модуля, отвечающего за кластерное взаимодействие
`gslb-component`	События модуля конфигурации GSLB
`kern`	События ядра
`lb-access`	События из access_log балансировщика нагрузки
`lb-error`	События из error_log балансировщика нагрузки

`lb-ls`	Позволяет получить список журналов балансировщика нагрузки (файлы должны иметь расширение `.log`)
	Пример:
	`$$ logs lb-ls`
	`access.log`
	`error.log`
	`healthmonitoring.log`
	`$$`

`mgmt-access`	События из access_log модуля, отвечающего за управление Angie ADC
`mgmt-error`	События из error_log модуля, отвечающего за управление Angie ADC
`session-store`	События модуля, отвечающего за хранение sticky-сессий в паре высокой доступности
`snmp-manager`	События модуля SNMP
`storage`	События из storage_log модуля, отвечающего за управление Angie ADC
`supervisor`	События модуля, отвечающего за управление кластеризацией Angie ADC
`upgrade`	События обновления Angie ADC
`view <filename>`	Позволяет просмотреть произвольный журнал событий, например, добавленный вручную в настройках конфигурации балансировщика. Файл должен находиться в папке `/var/log/angie-lb/` и иметь расширение `.log`. Пример: `$$ logs view error.log`

Дополнительные параметры:

`follow`	Вывод записей в режиме реального времени.
`transfer`	Копирование записей в директорию `transfer`.

9.8.1 Фильтрация вывода

Вывод записей поддерживает фильтрацию через pipe. Допускается использование нескольких фильтров в виде:

```
command | filter1 | filter2 | ... | filterN
```

Поддерживаются следующие фильтры:

- `grep` — фильтрация по подстроке;
- `exclude` — исключение строк, содержащих указанную подстроку;
- `include` — вывод только строк, содержащих указанную подстроку;
- `head` — вывод первых N строк;
- `tail` — вывод последних N строк.

9.8.1.1 grep

Синтаксис: `grep -i -o -v <pattern>`

Параметры:

- `-i` — игнорировать регистр;
- `-o` — показать только совпавшую часть вместо всей строки;
- `-v` — инвертировать результат;
- `<pattern>` — подстрока для поиска.

Пример:

```
$$ logs lb-access | grep GET
127.0.0.1 - - [29/Aug/2025:14:34:03 +0300] "GET /metrics HTTP/1.1" 200 1800 "-"
↪"Prometheus/" "-"
$$ logs lb-access | grep -v GET
2025/08/29 10:19:42 [notice] 976#976: signal 29 (SIGIO) received
$$ logs lb-access | grep -i get
127.0.0.1 - - [29/Aug/2025:14:34:03 +0300] "GET /metrics HTTP/1.1" 200 1800 "-"
↪"Prometheus/" "-"
$$ logs lb-access | grep -o GET
GET
```

9.8.1.2 include

Синоним `grep <pattern>`.

Синтаксис: `include <pattern>`.

Параметры:

- `<pattern>` — подстрока для поиска.

Пример:

```
$$ logs lb-access | include GET
127.0.0.1 - - [29/Aug/2025:14:34:03 +0300] "GET /metrics HTTP/1.1" 200 1800 "-"
↪"Prometheus/" "-"
```

9.8.1.3 exclude

Синоним `grep -v <pattern>`.

Синтаксис: `exclude <pattern>`.

Параметры:

- `<pattern>` — подстрока для поиска.

Пример:

```
$$ logs lb-error | exclude exit
2025/08/29 10:19:42 [notice] 976#976: signal 29 (SIGIO) received
```

9.8.1.4 head

Вывод первых N строк.

Синтаксис: `head <n>`.

Параметры:

- `<n>` — количество строк.

Пример:

```
$$ logs lb-access | head 2
127.0.0.1 - - [28/Aug/2025:14:53:48 +0300] "GET /metrics HTTP/1.1" 200 1798 "-"
↪"Prometheus/" "-"
127.0.0.1 - - [28/Aug/2025:14:53:58 +0300] "GET /metrics HTTP/1.1" 200 1798 "-"
↪"Prometheus/" "-"
```

9.8.1.5 tail

Вывод последних N строк.

Синтаксис: `tail <n>`.

Параметры:

- `<n>` — количество строк.

Пример:

```
$$ logs lb-access | tail 2
127.0.0.1 - - [28/Aug/2025:14:53:48 +0300] "GET /metrics HTTP/1.1" 200 1798 "-"
↪"Prometheus/" "-"
127.0.0.1 - - [28/Aug/2025:14:53:58 +0300] "GET /metrics HTTP/1.1" 200 1798 "-"
↪"Prometheus/" "-"
```

9.9 modules

Контекст `modules` позволяет просматривать информацию о динамических модулях Angie ADC.

info	Получение информации о динамическом модуле Angie ADC
list	Получение списка доступных динамических модулей Angie ADC
`modules`	Вход в контекст

9.9.1 info

Получение информации о динамическом модуле Angie ADC.

Синтаксис: `info <module>`.

Параметры:

- `<module>` — имя модуля.

9.9.2 list

Получение списка доступных динамических модулей Angie ADC.

Синтаксис: `list`.

9.10 ps

Отображение информации о запущенных процессах в системе. Показывает список активных процессов с различной степенью детализации в зависимости от используемых параметров.

Синтаксис: `ps [-f] [-p <pid>] [-o <format>] [-c <command>] [-s <sortspec>] [-t] [-w] [-h]`.

Параметры:

- `-f` — полный формат вывода: отображение расширенной информации о процессах.
- `-p <pid>` — отображение информации только о процессе с указанным PID (Process ID).
- `-o <format>` — пользовательский формат вывода. Формат задается как список полей, разделенных запятыми (например: pid,cmd,mem). Доступные поля описаны ниже.
- `-c <command>` — поиск и отображение процессов по имени команды (фильтрация по имени процесса).
- `-s <sortspec>` — сортировка вывода по указанным полям (например, по использованию CPU, памяти).
- `-t` — отображение процессов в древовидной структуре: показывает родительско-дочерние связи между процессами.
- `-w` — широкий вывод: позволяет отображать полные команды без обрезания.
- `-h` — не показывать заголовки столбцов в выводе.

Примеры:

- `$$ ps` — список процессов текущего пользователя.
- `$$ ps -p 1234` — информация о процессе с PID 1234.
- `$$ ps -c angie` — поиск процессов angie.
- `$$ ps -o pid,ppid,cmd,mem` — пользовательский формат вывода.

Форматы для параметра `-o`:

Ключ	Полное имя	Описание
`c`	cmd	Простое имя исполняемого файла
`C`	pcpu	Использование CPU (в процентах)
`f`	flags	Флаги как в длинном формате (поле F)
`g`	pgrp	Идентификатор группы процессов
`G`	tpgid	Идентификатор группы процессов управляющего терминала
`j`	cutime	Совокупное пользовательское время
`J`	cstime	Совокупное системное время
`k`	utime	Пользовательское время
`m`	min_flt	Количество малых ошибок страниц (minor page faults)
`M`	maj_flt	Количество больших ошибок страниц (major page faults)
`n`	cmin_flt	Совокупные малые ошибки страниц
`N`	cmaj_flt	Совокупные большие ошибки страниц
`o`	session	Идентификатор сессии
`p`	pid	Идентификатор процесса
`P`	ppid	Идентификатор родительского процесса
`r`	rss	Размер резидентного набора (resident set size) в килобайтах
`R`	resident	Резидентные страницы
`s`	size	Размер памяти в килобайтах
`S`	share	Количество разделяемых страниц
`t`	tty	Номер устройства управляющего терминала
`T`	start_time	Время запуска процесса
`U`	uid	Числовой идентификатор пользователя
`u`	user	Имя пользователя
`v`	vsize	Общий размер виртуальной памяти в килобайтах
`y`	priority	Приоритет планировщика ядра

Примеры:

- `$$ ps -o pid,cmd` — отобразить только PID и команду.
- `$$ ps -o user,pid,pcpu,pmem,cmd` — пользователь, PID, CPU, память, команда.
- `$$ ps -o pid,ppid,cmd,start_time` — PID, PPID, команда, время запуска.

9.11 settings

Контекст `settings` позволяет просматривать и изменять настройки Angie ADC.

Поддерживаемые команды:

angie debug	Включение режима отладки для балансировщика нагрузки
no angie debug	Отключение режима отладки
reload	Перезагрузка элементов Angie ADC
`settings`	Вход в контекст
sysctl	Просмотр и настройка параметров ядра Linux
syslog	Управление syslog-серверами

9.11.1 angie debug

Включение *режима отладки* для локального балансировщика нагрузки.

Синтаксис: `angie debug`.

9.11.2 no angie debug

Отключение режима отладки `angie`.

Синтаксис: `no angie debug`.

9.11.3 reload

Перезагрузка элементов Angie ADC.

Синтаксис: `reload {angie|prometheus}`.

Параметры:

- `angie` — перезагрузка `angie-mgmt`.
- `prometheus` — перезагрузка `prometheus`.

9.11.4 sysctl

Параметры ядра Linux узла.

Синтаксис: `sysctl {set <variable> <value> | remove <variable> | show {all | config}}`.

- `sysctl set <variable> <value>` — задание параметра в кластерной конфигурации узла;
- `sysctl remove <variable>` — удаление параметра из кластерной конфигурации;
- `sysctl show all` — вывод всех параметров ядра;
- `sysctl show config` — вывод параметров, заданных в кластерной конфигурации.

Пример:

```
$$ settings
(settings)$$ sysctl set net.core.somaxconn 1024
```

9.11.5 syslog

Настройка и управление удаленными серверами для экспорта событий Angie ADC по syslog-протоколу.

Синтаксис: `syslog {add <input> | del <uuid> | disable <uuid> | enable <uuid> | list | test | update}`.

Параметры:

- `add` — добавление нового syslog-сервера.

  Синтаксис: `syslog add <name> <host> <port> <tcp | udp> [<levels>]`

  Параметры:

  - `name` — имя сервера.
  - `host` — IP-адрес или доменное имя сервера.
  - `port` — номер порта (по умолчанию 514).
  - `tcp | udp` — используемый транспортный протокол (по умолчанию udp).
  - `levels` — уровни критичности событий от 0 до 7 (если не указано, будут включены все уровни):
    - `0` — Emergency: только события, приводящие к аварийной ситуации и полному отказу системы.
    - `1` — Alert: критические ошибки безопасности или выход из строя важных сервисов.
    - `2` — Critical: серьезные проблемы, которые требуют немедленного исправления.

  - `3` — Error: ошибки, влияющие на работу системы, но не приводящие к ее остановке.
  - `4` — Warning: предупреждения о возможных проблемах.
  - `5` — Notice: уведомления о событиях.
  - `6` — Informational: информационные сообщения.
  - `7` — Debug: включение событий отладки.

  Примеры:

  - `syslog add rsyslog1 10.0.2.2 514 udp`
  - `syslog add rsyslog1 10.0.2.2 514 udp 1 2 3`

- `del` — удаление syslog-сервера по UUID.

  Синтаксис: `syslog del <uuid>`

- `disable` — выключение syslog-сервера по UUID.

  Синтаксис: `syslog disable <uuid>`

- `enable` — включение syslog-сервера по UUID.

  Синтаксис: `syslog enable <uuid>`

- `list` — просмотр списка настроенных syslog-серверов.

  Синтаксис: `syslog list`

- `test` — проверка доступности syslog-сервера.

  Синтаксис: `syslog test <host> <port> <tcp|udp>`

  Параметры:

  - `host` — IP-адрес или доменное имя сервера.
  - `port` — номер порта.
  - `tcp | udp` — используемый транспортный протокол.

- `update` — изменение параметров syslog-сервера. Можно менять только одно поле за раз.

  Синтаксис: `syslog update <uuid> {name <name> | host <host> | port <port> | protocol <tcp|udp> | levels: [0..7]}`

  Параметры:

  - `name` — имя syslog-сервера.
  - `host` — IP-адрес или доменное имя syslog-сервера.
  - `port` — номер порта.
  - `tcp | udp` — транспортный протокол.
  - `levels` — уровень критичности событий от 0 до 7 (если не указано, будут включены все уровни):
    - `0` — Emergency: только события, приводящие к аварийной ситуации и полному отказу системы.
    - `1` — Alert: критические ошибки безопасности или выход из строя важных сервисов.
    - `2` — Critical: серьезные проблемы, которые требуют немедленного исправления.
    - `3` — Error: ошибки, влияющие на работу системы, но не приводящие к ее остановке.
    - `4` — Warning: предупреждения о возможных проблемах.
    - `5` — Notice: уведомления о событиях.
    - `6` — Informational: информационные сообщения.

* `7` — Debug: включение событий отладки.

Примеры:

* `syslog update <uuid> levels 1 3` — выставляет только указанные уровни критичности событий.
* `syslog update <uuid> levels` — выставляет все уровни критичности событий.

9.12 show

Просмотр состояния динамической маршрутизации и групп VRRP узла. Команда передает show-команды маршрутизатору FRR; изменить настройки маршрутизации с ее помощью нельзя (для этого используйте команду *routing*).

Синтаксис: `show <command>`. Список доступных команд выводится по `?`.

Пример:

```
$$ show ip bgp summary
$$ show ip ospf neighbor
$$ show vrrp interface ens33 summary
```

9.13 system

Контекст `system` для управления системой Angie ADC.

Поддерживаемые команды:

bond	Просмотр состояния бонда
hostname	Просмотр и установка имени узла
ntp	Просмотр и настройка NTP
reboot	Перезагрузка системы Angie ADC
stat	Просмотр статистики системы Angie ADC
`system`	Вход в контекст
time	Просмотр и установка системного времени
timezone	Просмотр и установка часового пояса узла
upgrade	Обновление Angie ADC
version	Просмотр версии Angie ADC

9.13.1 bond

Просмотр состояния бонда.

Синтаксис: `bond <number>`.

Параметры:

- `<number>` — номер бонда, например `0` для `bond0`.

Бонды настраиваются командой *set system bond*.

9.13.2 hostname

Просмотр и установка имени узла. Имя записывается в кластерную конфигурацию; команда завершается, когда узел применит новое имя.

Синтаксис: `hostname [set <name>]`.

Примеры:

- `(system)$$ hostname` — показать имя узла.

- `(system)$$ hostname set adc-home` — установить имя узла.

9.13.3 ntp

Просмотр и настройка NTP.

Синтаксис: `ntp {enable | disable | server <host> [minpoll <value>] [maxpoll <value>] [nts] | remove server <host>}`

- `ntp` — просмотр конфигурации и текущего состояния NTP.
- `ntp enable` — включение синхронизации времени по NTP.
- `ntp disable` — выключение синхронизации времени по NTP.
- `ntp server <host> [minpoll <value>] [maxpoll <value>] [nts]` — добавление NTP-сервера или изменение параметров уже добавленного.

  Параметры:

  - `<host>` — адрес NTP-сервера, например `pool.ntp.org`.
  - `minpoll <value>` — минимальный интервал опроса как степень двойки (от 4 до 17, по умолчанию: 6), необязательный параметр.
  - `maxpoll <value>` — максимальный интервал опроса как степень двойки (от 4 до 17, по умолчанию: 10), необязательный параметр.
  - `nts` — включение аутентифицированной синхронизации времени (NTS), необязательный параметр.
- `ntp remove server <host>` — удаление NTP-сервера.

  Параметры:

  - `<host>` — адрес NTP-сервера, например `pool.ntp.org`.

Примеры:

```
$$ system
(system)$$ ntp enable
(system)$$ ntp server pool.ntp.org minpoll 4 maxpoll 17
```

Вывод состояния:

```
(system)$$ ntp
enabled: yes
configured servers:
  pool.ntp.org (minpoll 6, maxpoll 10)
status: healthy
source: stratum2-1.ntp.mow01.ru.misaka.io
timezone: Europe/Moscow
system_time: 2026-09-10T13:43:09.273875160Z
last_checked_at: 2026-09-10T13:43:09.273875160Z
last_error:
servers:
  * pool.ntp.org: healthy
```

9.13.4 reboot

Перезагрузка системы Angie ADC.

Синтаксис: `reboot [force]`

Параметры:

- `force` — принудительная перезагрузка.

9.13.5 stat

Просмотр статистики системы Angie ADC.

Синтаксис: `stat [count <n>] [delay <m>]`

Параметры:

- `count <n>` — количество обновлений статистики;
- `delay <m>` — задержка между обновлениями статистики в секундах.

9.13.6 time

Просмотр и установка системного времени.

Синтаксис: `time {set <YYYY-MM-DD HH:MM:SS>}`.

Подкоманды:

- `set <YYYY-MM-DD HH:MM:SS>` — установка системного времени в указанном формате.

Примеры:

- `(system)$$ time` — показать текущее время.
- `(system)$$ time set 2025-01-15 14:30:00` — установить время на 15 января 2025, 14:30:00.

9.13.7 timezone

Просмотр и установка часового пояса узла. Часовой пояс определяет смещение локального времени относительно UTC. Изменение часового пояса не изменяет системное время (Unix timestamp), а только влияет на его отображение.

Синтаксис: `timezone [set <value>]`.

Часовой пояс указывается в формате IANA Time Zone Database, например `Europe/Moscow`; доступные значения подсказываются по `TAB`.

Примеры:

- `(system)$$ timezone` — показать текущий часовой пояс.
- `(system)$$ timezone set Europe/Moscow` — установить часовой пояс.

9.13.8 upgrade

Обновление Angie ADC.

Синтаксис: `upgrade <filename> [check]`

Параметры:

- `<filename>` — имя файла обновления в директории `transfer`;
- `check` — проверка, выполняется ли обновление.

9.13.9 version

Просмотр версии Angie ADC.

Синтаксис: `version [detail]`

Параметры:

- `detail` — подробный вывод версии.

9.14 transfer

Контекст `transfer` для работы с директорией `transfer`.

Поддерживаемые команды:

edit	Редактирование файла в текущей директории.
ls	Получение списка файлов в директории `transfer`
rm	Удаление файла в директории `transfer`
`transfer`	Вход в контекст
view	Просмотр содержимого файла в директории `transfer`

9.14.1 edit

Позволяет редактировать файлы в текущей директории.

Синтаксис: `edit [<filename>]`.

Параметры:

- `<filename>` — имя файла, который необходимо отредактировать (обязательный параметр).

9.14.2 ls

Получение списка файлов в директории `transfer`.

Синтаксис: `ls`.

9.14.3 rm

Удаление файла в директории `transfer`.

Синтаксис: `rm <filename>`.

Параметры:

- `<filename>` — имя файла.

9.14.4 view

Просмотр содержимого файла в директории `transfer`.

Синтаксис: `view <filename> [page]`.

Параметры:

- `<filename>` — имя файла;
- `page` — вывод записей в режиме постраничного просмотра.

9.15 trusted-ca

Контекст `trusted-ca` для загрузки доверенных корневых и промежуточных сертификатов в Angie ADC.

Поддерживаемые команды:

trusted-ca	Вход в контекст
upload	Загрузка доверенного сертификата
list	Вывод списка загруженных доверенных сертификатов
info	Вывод информации о загруженном доверенном сертификате
remove	Удаление загруженного доверенного сертификата

9.15.1 upload

Загрузка доверенного сертификата.

Синтаксис: `upload <name>`.

Параметры:

- `<name>` — имя, назначаемое сертификату.

Для загрузки сертификата необходимо вставить текст сертификата в строку, затем вставить пустую строку или написать `END` в новой строке.

Пример:

```
(trusted-ca)$$ upload ca-test
Certificate (PEM):
Insert PEM data line by line at the end of the input, add an empty line or enter END
-----BEGIN CERTIFICATE-----
MIIFjzCCA3egAwIBAgIUUlhm+3JoG0u0l2cPqJHKxwl++hYwDQYJKoZIhvcNAQEL
...
dZ+p4m4cDvEDrKTUUncN6TLR9UoRAFFOfDWrj/8+p3KK5T4=
-----END CERTIFICATE-----

Trusted CA 'ca-test' uploaded successfully
(trusted-ca)$$
```

При загрузке сертификата проверяется его корректность. В случае некорректного значения сертификат не будет сохранен.

9.15.2 list

Вывод списка доверенных сертификатов в Angie ADC.

Синтаксис: `list`.

Пример:

```
(trusted-ca)$$ list
Name     Validity                 Uploaded    Paths
-------  -----------------------  ----------  ----------------------------------------
↪--------------
ca-test  22.05.2026 - 28.04.2126  27.08.2026  /etc/pki/ca-trust/source/anchors/angie-
↪adc-ca-test.pem
```

9.15.3 info

Просмотр информации о доверенном сертификате.

Синтаксис: `info <name>`.

Параметры:

- `<name>` — имя сертификата.

Пример:

```
(trusted-ca)$$ info ca-test
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            52:58:66:fb:72:68:1b:4b:b4:97:67:0f:a8:91:ca:c7:09:7e:fa:16
        Signature Algorithm: sha256WithRSAEncryption
```

```
        Issuer: C=RU, ST=Test, L=Test, O=ADC-TestCA, CN=ADC Test CA
        Validity
            Not Before: May 22 09:35:12 2026 GMT
            Not After : Apr 28 09:35:12 2126 GMT
        Subject: C=RU, ST=Test, L=Test, O=ADC-TestCA, CN=ADC Test CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
...
                CA:TRUE
...
(trusted-ca)$$
```

9.15.4 remove

Удаление доверенного сертификата Angie ADC.

Синтаксис: `remove <name>`.

Параметры:

- `<name>` — имя сертификата.

Пример:

```
(trusted-ca)$$ remove ca-test
Trusted CA 'ca-test' deleted successfully.
```

9.16 web

Контекст `web` для настройки веб-интерфейса Angie ADC.

Поддерживаемые команды:

web	Вход в контекст
upload	Загрузка сертификата управления и ключа
tls	Включение / выключение HTTPS

9.16.1 upload

Загрузка сертификата и ключа для управления Angie ADC.

> **Примечание**
>
> Для работы с сертификатами необходимо предварительно создать кластер Angie ADC. Подробнее см. в статье *Создание и масштабирование кластера*.

Синтаксис: `upload`.

Для загрузки сертификата или ключа необходимо вставить текст сертификата или ключа в строку, затем вставить пустую строку или написать `END` в новой строке.

При загрузке ключа и сертификата проверяется их корректность. В случае некорректного значения сертификат или ключ не будет сохранен.

9.16.2 tls

Включение / выключение HTTPS и просмотр информации о статусе и используемом сертификате.

Синтаксис: `tls {enable | disable | info | status}`.

Параметры:

- `enable` — включение HTTPS;
- `disable` — выключение HTTPS;
- `info` — вывод информации о загруженном сертификате управления;
- `status` — вывод статуса HTTPS (включен или выключен).

ГЛАВА 10

Права на интеллектуальную собственность

Документация на программный продукт Angie ADC является интеллектуальной собственностью ООО «Веб-Сервер».

Copyright © 2026, ООО «Веб-Сервер». Все права защищены.