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

Руководство по развертыванию

версия 1.2

ООО «Веб-Сервер»

сент. 25, 2026

Оглавление

1 Аннотация **1**

2 Общие сведения **2**

3 Развертывание и первоначальная настройка **3**
3.1 Сценарий развертывания . . . 3
3.1.1 Установка . . . 3
3.1.2 Базовая настройка системы . . . 3
3.1.3 Расширенная настройка . . . 4
3.1.4 Примеры типовых схем развертывания Angie ADC . . . 4
3.2 Установка . . . 5
3.2.1 Аппаратные и программные требования . . . 5
3.2.1.1 Загрузка дистрибутива . . . 5
3.2.1.2 Запуск образа qcow2 . . . 6
3.2.1.3 Запуск образа OVA . . . 7
3.3 Первоначальная настройка . . . 8
3.3.1 Мастер настройки . . . 8
3.3.1.1 Меню мастера . . . 9
3.3.1.2 Настройка сетевых интерфейсов . . . 10
3.3.1.3 Настройка интерфейса управления . . . 10
3.3.1.4 Создание бондов . . . 11
3.3.1.5 Создание VLAN-интерфейсов . . . 11
3.3.1.6 Просмотр конфигурации Angie ADC и сетевых настроек . . . 11
3.3.1.7 Смена портов для веб-интерфейса Angie ADC . . . 12
3.3.1.8 Изменение имени устройства Angie ADC . . . 12
3.3.1.9 Проверка доступности узла . . . 12
3.3.1.10 Аварийная диагностика . . . 12
3.3.1.11 Просмотр журнала восстановления из резервной копии . . . 13
3.3.2 Кластеризация . . . 13
3.3.2.1 Обзор . . . 13
3.3.2.2 Применение и отмена изменений . . . 13
3.3.3 Настройка сетевых интерфейсов . . . 19
3.3.3.1 Изменение параметров сетевого интерфейса . . . 19
3.3.3.2 Просмотр параметров сетевого интерфейса . . . 19
3.3.4 Подключение внешних пользователей . . . 20
3.3.4.1 Подключение внешних пользователей через LDAP . . . 20
3.3.4.2 Подключение внешних пользователей через TACACS . . . 23
3.3.4.3 Подключение внешних пользователей через RADIUS . . . 25
3.4 Обновление системы . . . 27
3.4.1 Обновление Angie ADC . . . 27
3.4.1.1 Предварительные действия . . . 27

3.4.1.2 Откат обновления . . . 28
3.4.1.3 Обновление с версии 1.1.1 до версии 1.2 . . . 28
3.4.2 Приложение: пути обновления Angie ADC . . . 29
3.4.2.1 Обновление с версии 1.0 и выше . . . 29
3.4.2.2 Обновление до версии 1.0-rc2 . . . 30

4 Интерфейс командной строки (CLI) Angie ADC 32
4.1 Поддерживаемые команды . . . 33
4.2 Синтаксис . . . 35
4.3 certificates . . . 35
4.3.1 list . . . 35
4.3.2 info . . . 36
4.3.3 upload . . . 36
4.3.4 remove . . . 37
4.4 configuration . . . 37
4.4.1 commit . . . 38
4.4.2 end . . . 38
4.4.3 rollback . . . 38
4.4.4 set . . . 38
4.4.5 show . . . 39
4.4.6 unset . . . 39
4.5 diagnostics . . . 40
4.5.1 arping . . . 40
4.5.2 diag . . . 41
4.5.3 nslookup . . . 41
4.5.3.1 Разовый запрос . . . 41
4.5.3.2 Интерактивный режим . . . 41
4.5.4 ping . . . 42
4.5.5 pingc . . . 42
4.5.6 ss . . . 43
4.5.6.1 Параметры . . . 43
4.5.6.2 Примеры . . . 43
4.5.6.3 Фильтрация по state . . . 44
4.5.6.4 Фильтрация по критериям . . . 44
4.5.7 ssldump . . . 45
4.5.8 tcpdump . . . 46
4.5.9 traceroute . . . 46
4.6 firewall . . . 47
4.6.1 list . . . 47
4.6.2 no open . . . 47
4.6.3 open . . . 48
4.6.4 save . . . 49
4.7 ip . . . 49
4.8 logs . . . 49
4.8.1 Фильтрация вывода . . . 51
4.8.1.1 grep . . . 51
4.8.1.2 include . . . 51
4.8.1.3 exclude . . . 52
4.8.1.4 head . . . 52
4.8.1.5 tail . . . 52
4.9 modules . . . 52
4.9.1 info . . . 53
4.9.2 list . . . 53
4.10 ps . . . 53
4.11 settings . . . 54
4.11.1 angie debug . . . 54
4.11.2 no angie debug . . . 55
4.11.3 reload . . . 55

4.11.4 sysctl . . . 55
4.11.5 syslog . . . 55
4.12 system . . . 57
4.12.1 ntp . . . 57
4.12.2 reboot . . . 58
4.12.3 stat . . . 58
4.12.4 time . . . 58
4.12.5 timezone . . . 58
4.12.6 upgrade . . . 58
4.12.7 version . . . 59
4.13 transfer . . . 59
4.13.1 edit . . . 59
4.13.2 ls . . . 59
4.13.3 rm . . . 59
4.13.4 view . . . 59
4.14 trusted-ca . . . 60
4.14.1 upload . . . 60
4.14.2 list . . . 60
4.14.3 info . . . 61
4.14.4 remove . . . 61
4.15 vtysh . . . 61
4.16 web . . . 61
4.16.1 upload . . . 62
4.16.2 tls . . . 62

5 Права на интеллектуальную собственность 63

ГЛАВА 1

Аннотация

Настоящий документ содержит пошаговую инструкцию по развертыванию 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

Общие сведения

Angie ADC — комплексное программное обеспечение для балансировки нагрузки и управления сетевым трафиком для создания гибкой, производительной и безопасной инфраструктуры.

Особенности:

- Балансировщик нагрузки на уровнях L4-L7.
- Глобальная DNS-балансировка (GSLB).
- IP-маршрутизация.
- Решения для обеспечения высокой доступности.
- Присутствие в реестре российского ПО.

Angie ADC имеет удобный веб-интерфейс, командную строку (CLI) и API для интеграции с внешними системами, что обеспечивает понятный и надежный мониторинг и управление функциями.

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

ГЛАВА 3

Развертывание и первоначальная настройка

Здесь описывается развертывание виртуального устройства Angie ADC, первоначальная настройка после установки, объединение узлов в кластер управления, а также обновление версии.

В этом разделе:

- *Сценарий развертывания*
- *Установка*
- *Первоначальная настройка*
- *Обновление системы*

3.1 Сценарий развертывания

3.1.1 Установка

Первым шагом развертывания Angie ADC является *установка и запуск* виртуального образа Angie ADC.

3.1.2 Базовая настройка системы

После установки и запуска виртуального образа Angie ADC необходимо выполнить первоначальную настройку узла, создать кластер и выполнить общую настройку системы. Затем можно настроить конфигурацию балансировщика нагрузки.

1. Задайте сетевую конфигурацию Angie ADC через *мастер настройки*. Минимально необходимо настроить хотя бы один сетевой интерфейс (вручную или с помощью DHCP).

   После этого у вас появится доступ к веб-интерфейсу Angie ADC по адресу `http://<IP-адрес веб-интерфейса>:8080`. IP-адрес веб-интерфейса можно посмотреть в консоли ВМ или по команде `sudo virsh net-dhcp-leases default`.

2. Перейдите на страницу веб-интерфейса в браузере и выполните *первоначальную настройку узла*.

   Необходимо задать имя узла для кластера, авторизоваться в системе и настроить синхронизацию времени по NTP. Реквизиты для первого входа предоставляются после покупки решения.

После авторизации необходимо сменить пароль. Если необходимо, в дальнейшем можно настроить парольную политику Angie ADC.

3. Создайте *точку входа в кластер Angie ADC*.

   В дальнейшем, если необходимо, вы сможете подключить другие узлы Angie ADC к этой точке входа.

4. Донастройте сетевые интерфейсы *через веб-интерфейс*, если это необходимо.
5. Настройте HTTPS для защищенного подключения к веб-интерфейсу.
6. Добавьте пользователей системы и настройте для них аутентификацию и авторизацию (поддерживаются локальные и *внешние пользователи*).
7. Настройте конфигурацию балансировщика нагрузки и использование сертификатов.

3.1.3 Расширенная настройка

После выполнения общей настройки системы дополнительно можно настроить:

- высокую доступность для standalone-устройства Angie ADC;
- пару высокой доступности для двух устройств Angie ADC;
- глобальную балансировку.

3.1.4 Примеры типовых схем развертывания Angie ADC

- В рамках одного дата-центра (DC) для локальной балансировки трафика:

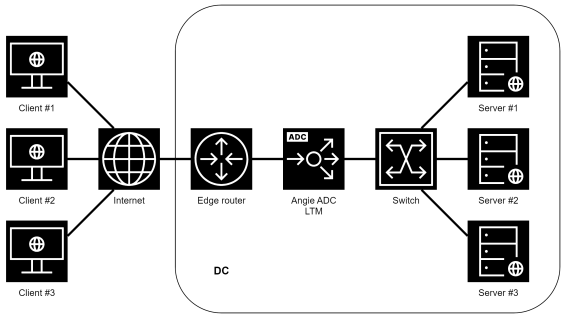


Рис. 1

- В двух и более дата-центрах с поддержкой резервирования и глобального управления трафиком (GSLB):

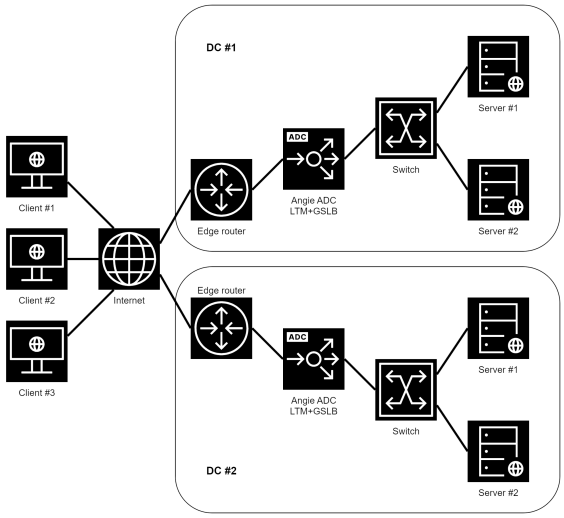


Рис. 2

3.2 Установка

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

При приобретении виртуального устройства Angie ADC вы можете выбрать для установки один из следующих двух образов:

- *OVA* (Open Virtual Appliance VMWare) для VMware ESXi;
- *qcow2* (QEMU Copy-On-Write v2) для Linux-сред.

Образы собраны на базе операционной системы РЕД ОС 8.

3.2.1 Аппаратные и программные требования

Минимальные аппаратные требования для запуска виртуального устройства Angie ADC:

- 2 vCPU
- 2 ГБ RAM
- 50 ГБ HDD

Поддерживаемые платформы виртуализации:

- KVM (QEMU)
- OpenStack
- VMware

В этом разделе:

- *Загрузка дистрибутива*
- *Запуск образа qcow2*
- *Запуск образа OVA*

3.2.1.1 Загрузка дистрибутива

После покупки решения Angie ADC или получения пробной версии на вашу почту придет письмо с архивом, содержащим файл `angie-adc-repo.p12` для скачивания дистрибутива через браузер, а также с отдельными файлами сертификата и ключа, если вы планируете использовать curl.

Вы можете выбрать для установки один из двух образов Angie ADC из нашего репозитория:

- *OVA* (Open Virtual Appliance VMWare) для VMware vSphere, ESXi, VirtualBox;
- *qcow2* (QEMU Copy-On-Write v2) для Linux-сред.

Для загрузки дистрибутива через браузер вам необходимо:

- импортировать файл `angie-adc-repo.p12` в браузер с паролем, указанным в письме;
- открыть репозиторий по ссылке https://download.angie.software/adc/ и загрузить дистрибутив.

Пример команды для curl:

```
$ curl -O https://download.angie.software/adc/angie-adc-1.2-x86_64.cloud-init.qcow2 \
  --cert angie-adc-repo.crt \
  --key angie-adc-repo.key
```

Примечание

Если выход в интернет осуществляется через прокси, то необходимо добавить домен репозитория в white-list, либо загружать дистрибутив напрямую без использования прокси.

3.2.1.2 Запуск образа qcow2

Ниже приведены инструкции по локальному развертыванию виртуальной машины Angie ADC.

Подготовка среды

Для работы необходима система виртуализации, например qemu. Перед ее использованием убедитесь, что у вас установлены следующие утилиты:

- `virsh`;
- `virt-install`;
- `qemu`;
- `libvirt`;
- `libguestfs-tools`;
- `virt-viewer`.

Установка `qemu` на Fedora:

```
$ sudo dnf install qemu libvirt libguestfs-tools libguestfs virt-viewer virt-install
```

Установка `qemu` на Ubuntu и Debian:

```
$ sudo apt update
$ sudo apt install -y \
  qemu-kvm qemu-system-x86 qemu-utils \
  libvirt-daemon-system libvirt-clients virtinst virt-manager \
  ovmf cpu-checker
```

После установки необходимо добавить своего пользователя в соответствующие группы:

```
$ sudo usermod -aG libvirt USER
$ sudo usermod -aG kvm USER
```

Скачивание дистрибутива

Скачайте образ Angie ADC *из репозитория*.

Развертывание

Чтобы развернуть образ qcow2, выполните следующие действия:

1. Проверьте состояние виртуальной сети:

   ```
   $ sudo virsh net-list --all
   ```

2. Запустите дистрибутив Angie ADC.

   Пример команды:

   ```
   $ sudo mv angie-adc-1.2-x86_64.cloud-init.qcow2 /var/lib/libvirt/images/
   $ sudo virt-install  --name angie-adc-1.2 --ram 2048 --disk /var/lib/libvirt/
   ↪images/angie-adc-1.2-x86_64.cloud-init.qcow2 --os-variant generic --import
   ```

3. Перейдите в консоль виртуальной машины. Откроется окно входа в мастер первоначальной настройки Angie ADC.
4. Введите логин `setup` и пароль `setup`. Откроется мастер первоначальной настройки Angie ADC.
5. Выполните необходимые настройки сетевой конфигурации Angie ADC и нажмите `exit`, чтобы выйти из мастера настройки.

   Подробнее см. *Мастер настройки*.

   > **Примечание**
   >
   > Минимально необходимо настроить хотя бы один сетевой интерфейс (вручную или с помощью DHCP).

6. Перейдите в веб-интерфейс Angie ADC по следующему адресу: `http://<IP-адрес веб-интерфейса>:8080`. IP-адрес веб-интерфейса можно посмотреть в консоли ВМ или по команде `sudo virsh net-dhcp-leases default`.

   Откроется страница входа в веб-интерфейс Angie ADC.
7. Авторизуйтесь в Angie ADC. Реквизиты для первого входа предоставляются после покупки решения. Рекомендуется сменить пароль после первого входа.

   В веб-интерфейсе Angie ADC вы можете настраивать функции Angie ADC и просматривать статистику работы балансировщика нагрузки.

3.2.1.3 Запуск образа OVA

> **Примечание**
>
> Образ OVA собран для VMware ESXi 7. При развертывании на более новых версиях ESXi (8, 9) функции Angie ADC будут работать по совместимости.

Подготовка среды

Для развертывания образа OVA необходима система виртуализации, например VMware ESXi.

Скачивание дистрибутива

Скачайте образ Angie ADC *из репозитория*.

Развертывание

Чтобы развернуть образ OVA через веб-интерфейс VMware ESXi, выполните следующие действия:

1. Войдите в веб-интерфейс VMware ESXi через браузер.
2. В контекстном меню сервера выберите `Deploy OVF template`.

   Откроется мастер развертывания.
3. Следуйте указаниям мастера, чтобы начать импорт образа Angie ADC.

   В результате на сервере появится новая виртуальная машина.
4. Запустите виртуальную машину Angie ADC и перейдите в консоль ВМ.

   Откроется окно входа в мастер первоначальной настройки Angie ADC.
5. Введите логин `setup` и пароль `setup`. Откроется мастер первоначальной настройки Angie ADC.

6. Выполните необходимые настройки сетевой конфигурации Angie ADC и нажмите `exit`, чтобы выйти из мастера настройки.

   Подробнее см. *Мастер настройки*.

   > **Примечание**
   >
   > Минимально необходимо настроить хотя бы один сетевой интерфейс (вручную или с помощью DHCP).

7. Перейдите в веб-интерфейс Angie ADC по следующему адресу: `http://<IP-адрес веб-интерфейса>:8080`. IP-адрес веб-интерфейса можно посмотреть в консоли ВМ или по команде `sudo virsh net-dhcp-leases default`.

   Откроется страница входа в веб-интерфейс Angie ADC.

8. Авторизуйтесь в Angie ADC. Реквизиты для первого входа предоставляются после покупки решения. Рекомендуется сменить пароль после первого входа.

   В веб-интерфейсе Angie ADC вы можете настраивать функции Angie ADC и просматривать статистику работы балансировщика нагрузки.

3.3 Первоначальная настройка

После установки и запуска виртуального образа Angie ADC рекомендуется выполнить общую настройку системы:

- настроить сеть;
- получить доступ к веб-интерфейсу;
- настроить точку входа в кластер;
- добавить пользователей и настроить авторизацию;
- настроить синхронизацию времени и конфигурацию балансировщика нагрузки.

Дополнительно можно настроить высокую доступность и глобальную балансировку.

В этом разделе:

- *Мастер настройки*
- *Кластеризация*
- *Настройка сетевых интерфейсов*
- *Подключение внешних пользователей*

3.3.1 Мастер настройки

Мастер настройки позволяет управлять конфигурацией Angie ADC без доступа к веб-интерфейсу. Также в мастере можно просмотреть сетевую конфигурацию и проверить доступность узла, выполнив ping-запрос.

При первом запуске Angie ADC вам необходимо настроить хотя бы один *сетевой интерфейс* для доступа к веб-интерфейсу Angie ADC.

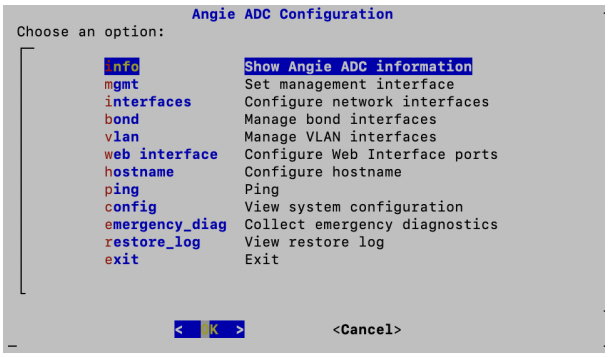
При расширенной настройке вы можете дополнительно настроить другие интерфейсы, бонды и VLAN-интерфейсы, назначить выделенный интерфейс управления, изменить имя устройства и порт для веб-интерфейса.

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.

В этой статье:

- *Меню мастера*;
- *Настройка сетевых интерфейсов*;
- *Настройка интерфейса управления*;
- *Смена портов для веб-интерфейса Angie ADC*;
- *Создание бондов*;
- *Создание VLAN-интерфейсов*;
- *Просмотр конфигурации Angie ADC и сетевых настроек*;
- *Изменение имени устройства Angie ADC*;
- *Проверка доступности узла*;
- *Аварийная диагностика*;
- *Просмотр журнала восстановления из резервной копии*.

3.3.1.1 Меню мастера



Основное меню мастера настройки Angie ADC содержит следующие команды:

- `info` — просмотр общей информации об Angie ADC.
- `mgmt` — настройка интерфейса управления Angie ADC.
- `interfaces` — переход к просмотру и настройке сетевых интерфейсов, бондов и VLAN-интерфейсов.
- `bond` — переход к созданию, просмотру и удалению сетевых бондов.
- `vlan` — переход к созданию, просмотру и удалению VLAN-интерфейсов.
- `web interface` — изменение порта для веб-интерфейса Angie ADC.
- `hostname` — смена имени устройства.
- `config` — просмотр конфигурации Angie ADC и сетевых настроек.
- `ping` — проверка доступности узла.
- `emergency_diag` — аварийный сбор логов для передачи в техническую поддержку.
- `restore_log` — просмотр журнала восстановления узла из резервной копии.
- `exit` — выход из мастера.

3.3.1.2 Настройка сетевых интерфейсов

Чтобы настроить сетевой интерфейс Angie ADC, выполните следующие действия:

1. Выберите в основном меню пункт `interfaces`.

   Откроется список доступных интерфейсов.

2. Выберите интерфейс и перейдите в его меню.

   Откроется список доступных действий:

   - `show` — просмотр информации об интерфейсе.
   - `config` — переход к ручной настройке IP-адреса и шлюза (Gateway).
   - `dhcp` — настройка автоматического получения IP-адреса от DHCP-сервера.
   - `mtu` — переход к настройке MTU.
   - `clear` — сброс всех заданных настроек интерфейса, кроме MTU. Значение MTU, заданное вручную, не сбрасывается.
   - `back` — выход из меню интерфейса.

3. Выберите `config` или `dhcp` в зависимости от ваших целей и задайте необходимые настройки.

3.3.1.3 Настройка интерфейса управления

Рекомендуется использовать для управления отдельную сеть, в которой нет служебных сервисов, иначе эти сервисы перестанут быть доступными для других компонентов Angie ADC. Если вы хотите сохранить доступ к этим сервисам, после выделения интерфейса управления настройте для них маршруты-исключения.

Чтобы выделить отдельный интерфейс для управления Angie ADC, выполните следующие действия:

1. Выберите в основном меню пункт `mgmt`.

   Откроется список доступных действий:

   - `setup` — переход к настройке интерфейса управления.
   - `status` — просмотр текущего статуса интерфейса управления.
   - `leak` — переход к настройке маршрутов-исключений для сервисов внутри сети управления (пункт отображается, если интерфейс управления настроен).
   - `back` — выход из меню `mgmt`.

2. В открывшемся меню выберите `setup`.

   Откроется список доступных интерфейсов.

3. Выберите нужный интерфейс. Этот интерфейс будет использоваться для управления системой через отдельную сеть и будет иметь собственную таблицу маршрутизации.

4. Подтвердите операцию.

   Предупреждение

   Служебные сервисы, расположенные в этой сети, перестанут быть доступными для других компонентов Angie ADC.

5. Если необходимо, настройте маршруты-исключения для служебных сервисов. Для этого перейдите в меню `mgmt` → `leak` → `add` и добавьте сеть назначения, из которой будет производиться доступ к сервисам, находящимся в сети управления.

3.3.1.4 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), выполните следующие действия:

1. Выберите в основном меню пункт `bond`.

   Откроется список доступных действий:

   - `list` — просмотр списка бондов.
   - `create` — переход к созданию нового бонда.
   - `back` — выход из меню `bond`.

2. Выберите `create`, укажите номер бонда (по умолчанию будет предложен первый свободный номер по возрастанию) и нажмите `OK`.

3. Выберите интерфейсы, которые необходимо объединить (максимум 8 интерфейсов), и нажмите `OK`.

   > **Примечание**
   >
   > Рекомендуется объединять в бонд ненастроенные сетевые интерфейсы.

4. В открывшемся окне с конфигурацией подтвердите создание нового бонда.

Просмотр свойств бонда и его удаление доступны через основное меню `bond` → `list` → `<bond_name>`.

Настройка бонда доступна через основное меню настройки интерфейсов: `interfaces` → `<bond_name>`.

3.3.1.5 Создание VLAN-интерфейсов

Чтобы настроить VLAN-интерфейс, выполните следующие действия:

1. Выберите в основном меню пункт `vlan`.

   Откроется список доступных действий:

   - `list` — просмотр списка VLAN-интерфейсов.
   - `create` — переход к созданию нового VLAN-интерфейса.
   - `back` — выход из меню `vlan`.

2. Выберите `create`, укажите родительский интерфейс, VLAN ID для нового VLAN и нажмите `OK`.

   Будет создан новый VLAN-интерфейс.

Просмотр свойств VLAN и его удаление доступны через основное меню `vlan` → `list` → `<vlan_name>`.

Настройка VLAN доступна через основное меню настройки интерфейсов: `interfaces` → `<vlan_name>`.

3.3.1.6 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.

3.3.1.7 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.

3.3.1.8 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.

3.3.1.9 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.

3.3.1.10 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*.

3.3.1.11 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`.

3.3.2 Кластеризация

3.3.2.1 Обзор

Кластер управления Angie ADC позволяет настраивать несколько устройств Angie ADC с любого узла через общую кластерную конфигурацию. В нее входят:

- конфигурация GSLB;
- сертификаты;
- пользователи SNMP;
- конфигурация мониторинга доступности;
- настройки парольной политики.

Данные между узлами кластера синхронизируются и передаются в зашифрованном виде.

> **Важно**
>
> Рекомендуется создавать или обновлять резервную копию узла перед внесением в систему значительных изменений.

> **Примечание**
>
> Конфигурация локального балансировщика не синхронизируется между узлами кластера.

3.3.2.2 Применение и отмена изменений

После применения изменений на одном из узлов кластера они автоматически синхронизируются на все остальные узлы кластера.

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 об внесении изменений.

Предупреждение

Применение изменений, распространяющихся на весь кластер, невозможно, если хотя бы один узел кластера недоступен. Рекомендуется ввести в строй недоступные узлы перед внесением изменений в кластерную конфигурацию.

В этом разделе:

- *Создание и масштабирование кластера управления*
- *Мониторинг состояния кластера управления*

Создание и масштабирование кластера управления

Кластер управления Angie ADC состоит из нескольких узлов (устройств Angie ADC). Один из узлов кластера является точкой входа в кластер (к нему подключаются остальные узлы кластера).

Развертывание кластера состоит из следующих этапов:

1. *Развертывание устройств Angie ADC* в дата-центрах.
2. *Первоначальная настройка узлов*.
3. *Создание точки входа в кластер* на одном из узлов.
4. *Добавление остальных узлов в кластер*.

Предупреждение

В качестве IP-адресов узлов кластера нельзя указывать *IP-адрес интерфейса управления*, если он был настроен.

Важно

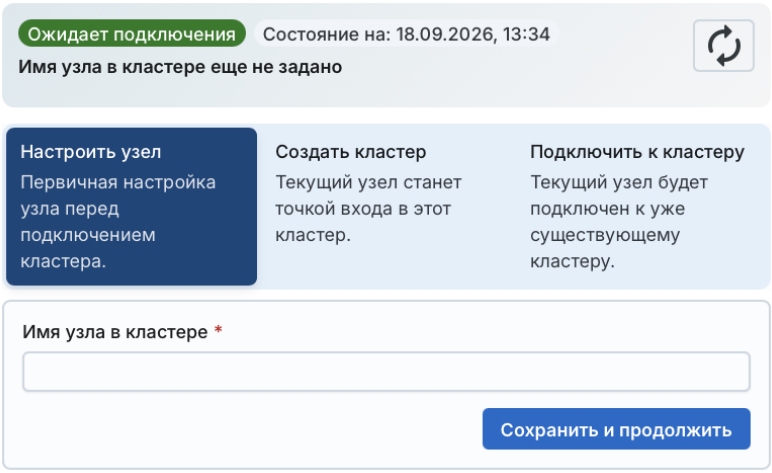
Рекомендуется обязательно выполнять первичную настройку NTP на всех узлах кластера, так как синхронизация времени на узлах с единым внешним источником критически важна для работы кластера.

Первоначальная настройка узла

Чтобы выполнить первоначальную настройку узла Angie ADC после установки:

1. Откройте веб-интерфейс Angie ADC на узле.

   Откроется экран с информацией о текущем узле и вариантами его интеграции в кластер.



2. Выберите сценарий `Настроить узел`.
3. Задайте имя текущего узла в кластере (произвольное). Допускаются строчные латинские буквы, цифры и одиночные дефисы внутри имени. Это имя может отличаться от `hostname` узла и отображает логическую структуру кластера управления.
4. Нажмите `Сохранить и продолжить`.

   В веб-интерфейсе откроется окно авторизации.
5. Авторизуйтесь в системе. При первом входе система также запросит смену пароля.
6. В окне с запросом на настройку NTP включите переключатель `Синхронизация времени (NTP)`.

> **Важно**
>
> Рекомендуется обязательно выполнять настройку NTP, так как синхронизация времени на узлах с единым внешним источником критически важна для работы кластера.

7. 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).
   - Установите флажок `NTS`, если хотите использовать аутентифицированную синхронизацию времени.

> **Примечание**
>
> NTP также можно настроить в веб-интерфейсе в разделе `Система` → `NTP` и через *CLI*.

8. Нажмите `Сохранить`.

Новые настройки узла будут применены.

Далее можно перейти к созданию кластера или подключению узла к уже существующему кластеру.

Создание точки входа в кластер

> **Предупреждение**
>
> После создания точки входа ее нельзя изменить, кластер нельзя расформировать. Внимательно проверьте все параметры перед созданием точки входа.

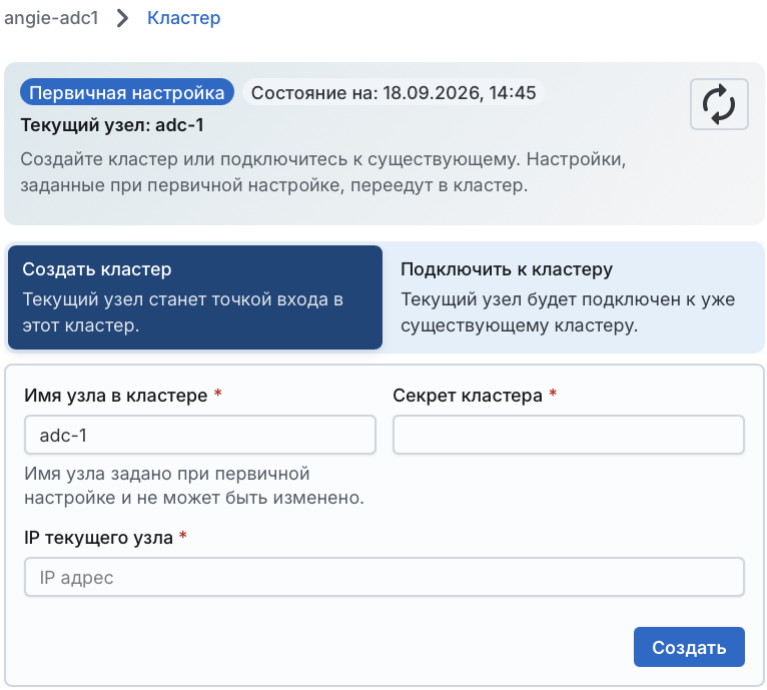
Чтобы создать точку входа в кластер, выполните следующие действия:

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. Выполните *первоначальную настройку узла* (рекомендуется).

   Откроется экран с информацией о текущем узле и вариантами его интеграции в кластер.



3. 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.

4. Нажмите `Создать`.

   Будет создан кластер. Текущий узел будет назначен точкой входа в кластер.

Добавление узлов в кластер

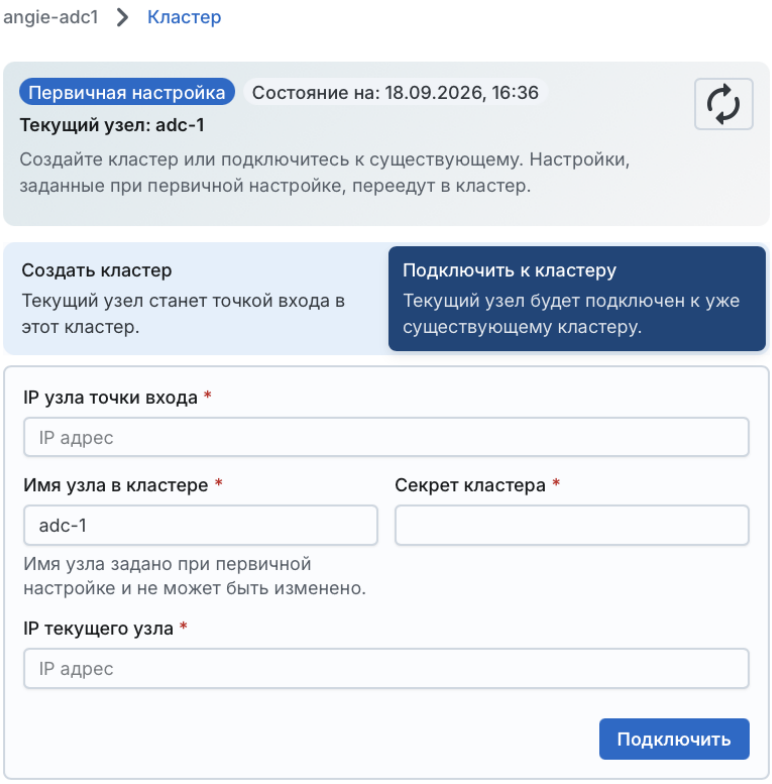
Для каждого последующего узла кластера выполните следующие действия:

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. Выполните *первоначальную настройку узла* (рекомендуется).

   Откроется экран с информацией о текущем узле и вариантами его интеграции в кластер.



3. 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.

4. Нажмите `Подключить`.

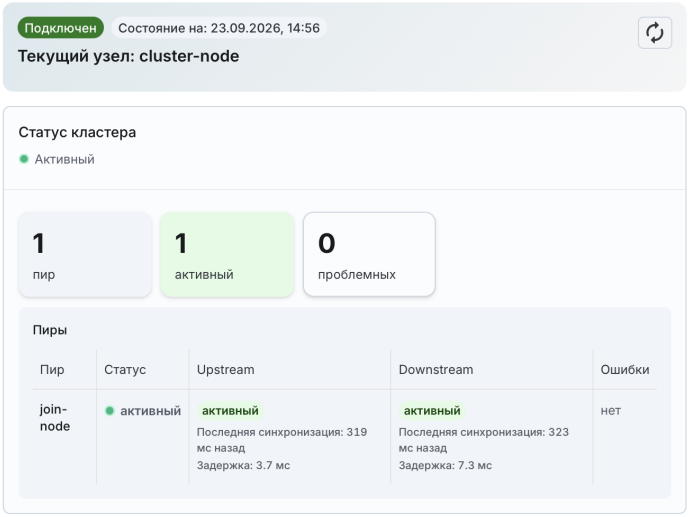
Узел будет подключен к кластеру.

Мониторинг состояния кластера управления

После создания кластера управления на странице `Настройки кластера` отображаются:

- Имя текущего узла в кластере.

  Имя узла в кластере управления может отличаться от `hostname` узла и отображает логическую структуру кластера.



- Статус подключения текущего узла к кластеру управления:
  - `Ожидает подключения` – узел не входит в кластер.
  - `Подключен` – узел подключен к кластеру.
  - `Подключение...` – выполняется подключение узла к кластеру.
- Статус кластера управления:
  - `Активный` – кластер запущен.
  - `Подключение` – выполняется запуск кластера.
- Сводная статистика других узлов кластера (пиров текущего узла).
- Таблица с подробной информацией по каждому пиру:

`Пир`	Имя узла, входящего в кластер.
`Статус`	• `активный` – пир находится в рабочем состоянии, данные синхронизированы. • `сбой` – есть проблемы с синхронизацией данных. • `недоступен` – пир недоступен.
`Upstream`	Статус получения данных пиром: • `активный` – upstream доступен, данные синхронизированы. • `подключение` – выполняется подключение к кластеру. • `синхронизация` – выполняется синхронизация (получение данных пиром). • `недоступен` – upstream недоступен, получение данных невозможно.
`Downstream`	Статус передачи данных пиром: • `активный` – downstream доступен, данные могут передаваться. • `подключение` – выполняется подключение к кластеру. • `недоступен` – downstream недоступен, передача данных невозможна.
`Последняя синхронизация`	Время, прошедшее с последней синхронизации данных.
`Задержка`	Задержка синхронизации данных между текущим узлом и пиром.
`Ошибки`	Ошибки, возникающие при синхронизации данных для каждого пира.

3.3.3 Настройка сетевых интерфейсов

Вы можете просматривать и изменять параметры сетевых интерфейсов в веб-интерфейсе Angie ADC (`Система` → `Конфигурация`).

Предупреждение

Не рекомендуется изменять настройки интерфейсов узлов, объединенных в пару высокой доступности, иначе пара может потерять связность и работоспособность.

3.3.3.1 Изменение параметров сетевого интерфейса

1. В веб-интерфейсе Angie ADC перейдите `Система` → `Конфигурация`.
2. В блоке `Сетевые интерфейсы` нажмите на сетевой интерфейс, параметры которого вы хотите изменить.

   Откроется окно с параметрами выбранного сетевого интерфейса.

   Примечание

   Если для интерфейса был указан способ получения настроек по DHCP, то в окне редактирования будет отображаться подсказка с DHCP-параметрами интерфейса.

3. Внесите необходимые изменения и нажмите `Сохранить`.

Также изменение параметров сетевых интерфейсов доступно через *CLI* и *в мастере*.

3.3.3.2 Просмотр параметров сетевого интерфейса

В блоке `Сетевые интерфейсы` отображается список настроенных сетевых интерфейсов.

Для каждого интерфейса отображаются следующие параметры:

- Имя сетевого интерфейса.
- MAC-адрес (формат: `"XX:XX:XX:XX:XX:XX"`).
- Тип конфигурации: `static`, `DHCP`.
- Массив IPv4-адресов в формате CIDR.
- Массив IPv6-адресов в формате CIDR.
- IP-адрес шлюза по умолчанию (глобальный для всех интерфейсов), если установлен.
- Массив IP-адресов DNS-серверов.
- Массив доменов поиска DNS.

3.3.4 Подключение внешних пользователей

При использовании внешнего провайдера аутентификации и авторизации данные о пользователях хранятся на внешнем сервере. Вы можете настроить аутентификацию и авторизацию внешних пользователей в Angie ADC через провайдеров RADIUS, TACACS и LDAP.

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 не доступны и не отображаются в веб-интерфейсе.

Для включения внешней аутентификации и авторизации необходимо добавить в систему предварительно настроенный сервер. После этого при входе в веб-интерфейс будет доступен выбор типа аутентификации.

В этом разделе:

- *RADIUS*
- *LDAP*
- *TACACS+*

3.3.4.1 Подключение внешних пользователей через LDAP

Вы можете включить и настроить аутентификацию и авторизацию для внешних пользователей через LDAP. Пользователям может быть назначена одна 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 не доступны и не отображаются в веб-интерфейсе.

Роли внешних пользователей определяются на основе принадлежности к LDAP-группам.

Для подключения внешних пользователей к системе вам необходимо:

1. включить внешнюю аутентификацию через LDAP и задать настройки сервера;
2. включить внешнюю авторизацию через LDAP и задать настройки сервера;
3. задать базовый DN и фильтры для поиска пользователей и групп на LDAP-сервере;
4. настроить соответствие LDAP-групп и ролей пользователей в Angie ADC.

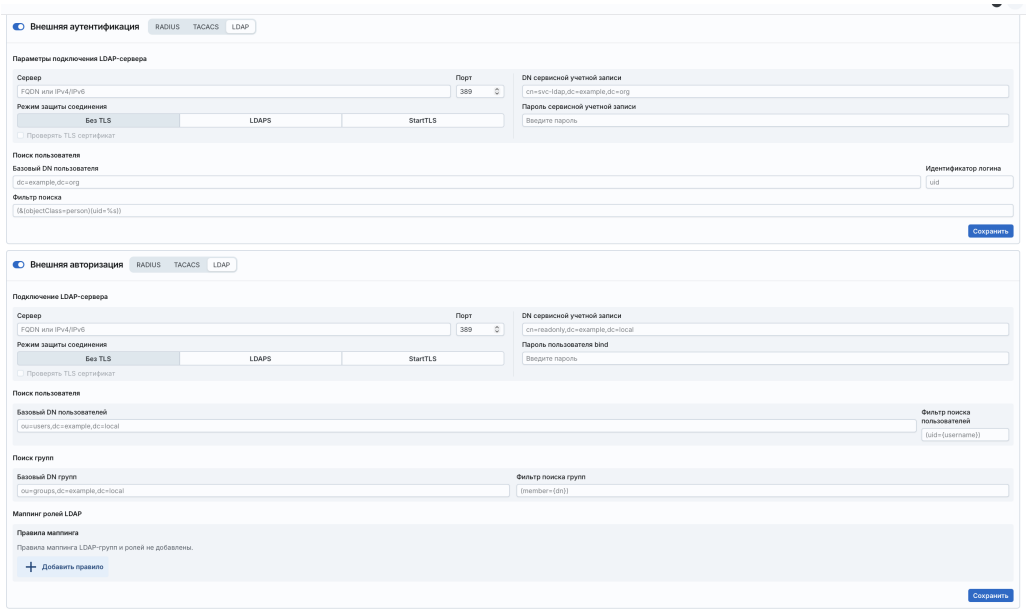
На стороне LDAP-сервера также должны быть настроены пользователи, группы и сервисная учетная запись для Angie ADC.

> **Предупреждение**
>
> Необходимо настроить и включить оба блока: аутентификацию и авторизацию. Если один из блоков не настроен или выключен, внешние пользователи не смогут получить доступ к системе.

Шаги

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 `Включить внешнюю аутентификацию` и выберите провайдера аутентификации LDAP.

> **Примечание**
>
> Одновременно поддерживается использование только одного провайдера внешней аутентификации. При добавлении нового провайдера аутентификации настройки предыдущего провайдера сбрасываются.

3. Укажите следующие параметры:

   - `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` для защищенного соединения).

     > **Примечание**
     >
     > При выборе режима защиты соединения `LDAPS` или `StartTLS` становится доступен флажок `Проверять TLS-сертификат`. По умолчанию флажок установлен.

   - `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`.

4. Нажмите `Сохранить`.

   Внешняя аутентификация с использованием провайдера LDAP будет включена.

5. В блоке `Внешняя авторизация` переведите переключатель `Включить внешнюю авторизацию` в положение "включено" и выберите провайдера авторизации LDAP.
6. Задайте параметры подключения к серверу:
   - `Сервер`: IP-адрес или доменное имя LDAP-сервера.
   - `Порт`: порт подключения к LDAP-серверу (по умолчанию `389`).
7. Укажите параметры защиты соединения: `Без TLS` (по умолчанию) или `TLS (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.

8. Укажите DN учетной записи, с которой будет выполняться подключение к LDAP-серверу (`DN сервисной учетная запись (bind)`). Можно использовать учетную запись администратора LDAP-сервера, например `cn=admin,dc=example,dc=com`.
9. Укажите пароль сервисной учетной записи (`Пароль пользователя bind`).
10. В блоке `Поиск пользователя` укажите следующие параметры:
    - `Базовый DN пользователей`, например `ou=users,dc=example,dc=com`;
    - `Фильтр поиска пользователей`, например `(uid=%s)`.
11. В блоке `Поиск групп` укажите следующие параметры:
    - `Базовый DN групп`, например `ou=groups,dc=example,dc=com`;
    - `Фильтр поиска групп`, например `(member=%s)`.
12. 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)`.
13. 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.

3.3.4.2 Подключение внешних пользователей через TACACS

Вы можете включить и настроить аутентификацию и авторизацию для внешних пользователей через TACACS. Пользователям может быть назначена одна 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 не доступны и не отображаются в веб-интерфейсе.

Роли для внешних пользователей определяются на основе соответствия атрибутам этих пользователей в TACACS+.

Для подключения внешних пользователей к системе вам необходимо:

1. включить внешнюю аутентификацию через TACACS и задать настройки сервера;
2. включить внешнюю авторизацию через TACACS+ и задать настройки сервера;
3. настроить соответствие атрибутов TACACS+ ролям пользователей в Angie ADC.

На стороне TACACS-сервера также должны быть настроены пользователи и группы.

Пример настройки:

```
group = admin {
    service = shell {
        set priv-lvl = 15
    }
}

user = admin {
    password = clear admin
    member = admin
}
```

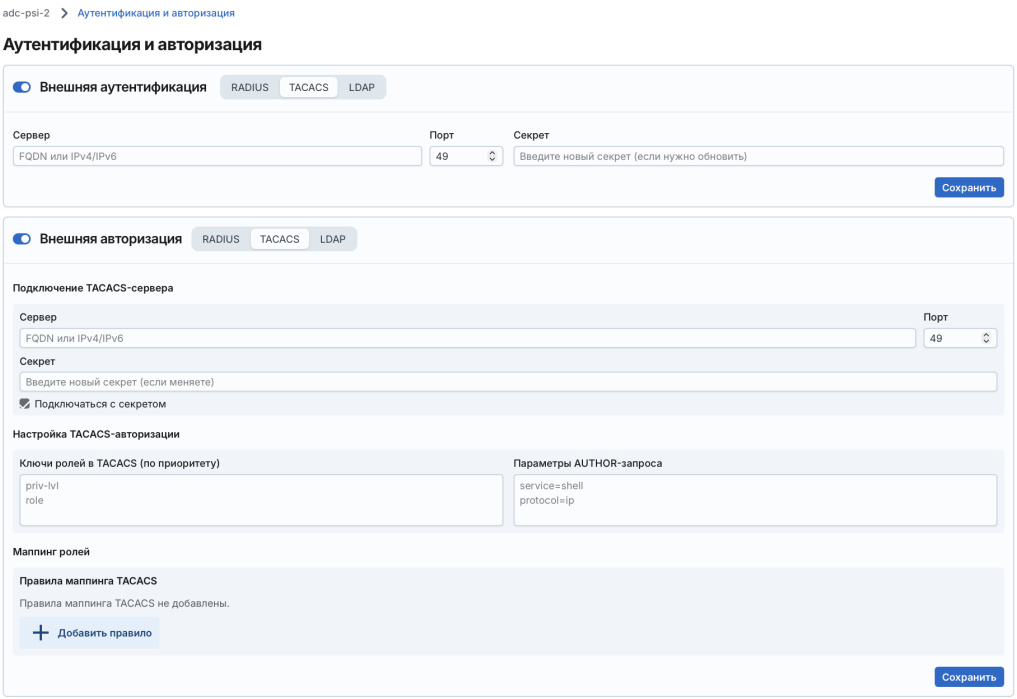
Предупреждение

Необходимо настроить и включить оба блока: аутентификацию и авторизацию. Если один из блоков не настроен или выключен, внешние пользователи не смогут получить доступ к системе.

Шаги

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 `Включить внешнюю аутентификацию` и выберите провайдера аутентификации TACACS.

> **Примечание**
>
> Одновременно поддерживается использование только одного провайдера внешней аутентификации. При добавлении нового провайдера аутентификации настройки предыдущего провайдера сбрасываются.

3. Укажите следующие параметры:
   - `Адрес`: IP-адрес или доменное имя TACACS-сервера.
   - `Порт`: порт подключения к TACACS-серверу (по умолчанию `49`).
   - `Секрет`: общий секрет для шифрования паролей.
4. Нажмите `Сохранить`.

   Внешняя аутентификация с использованием провайдера TACACS будет включена.
5. В блоке `Внешняя авторизация` переведите переключатель `Включить внешнюю авторизацию` в положение "включено" и выберите провайдера авторизации TACACS.
6. Задайте параметры подключения к серверу:
   - `Адрес`: IP-адрес или доменное имя TACACS-сервера.
   - `Порт`: порт подключения к TACACS-серверу (по умолчанию `49`).
   - `Секрет`: общий секрет для шифрования паролей.
7. Укажите в порядке приоритета атрибуты ролей пользователя в TACACS+, например `priv-lvl`, затем `role`. По этим атрибутам Angie ADC будет определять роль для пользователя.
8. 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`.

9. Задайте соответствие значений атрибутов TACACS+ ролям в Angie ADC, например `priv-lvl=15` → `Администратор` или `role=adc-admin` → `Администратор`.
10. 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.

3.3.4.3 Подключение внешних пользователей через RADIUS

Вы можете включить и настроить аутентификацию и авторизацию для внешних пользователей через RADIUS. Пользователям может быть назначена одна 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 не доступны и не отображаются в веб-интерфейсе.

Роли для внешних пользователей определяются на основе соответствия атрибутам этих пользователей в RADIUS.

> **Примечание**
>
> RADIUS-авторизация доступна только при аутентификации через RADIUS.

Для подключения внешних пользователей к системе вам необходимо:

1. включить внешнюю аутентификацию через RADIUS и задать настройки сервера;
2. включить внешнюю авторизацию через RADIUS и задать настройки сервера;
3. настроить соответствие атрибутов RADIUS ролям пользователей в Angie ADC.

На стороне RADIUS-сервера также должны быть настроены пользователи и их атрибуты.

Пример настройки:

```
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"
```

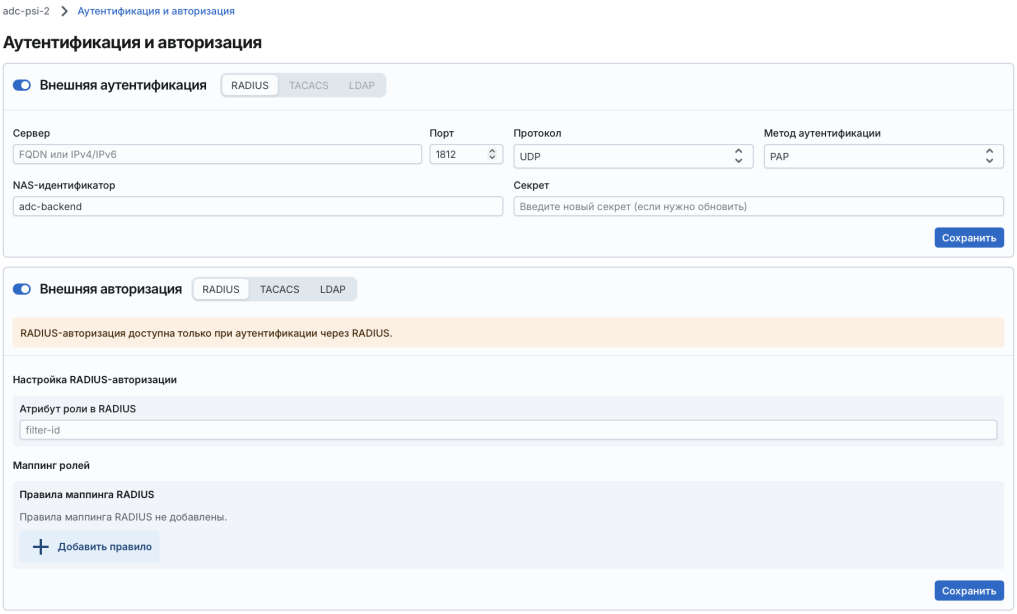
Предупреждение

Необходимо настроить и включить оба блока: аутентификацию и авторизацию. Если один из блоков не настроен или выключен, внешние пользователи не смогут получить доступ к системе.

Шаги

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 `Включить внешнюю аутентификацию` и выберите провайдера аутентификации RADIUS.

   Примечание

   Одновременно поддерживается использование только одного провайдера внешней аутентификации. При добавлении нового провайдера аутентификации настройки предыдущего провайдера сбрасываются.

3. Укажите следующие параметры:

   - `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.

4. Нажмите `Сохранить`.

   Внешняя аутентификация с использованием RADIUS будет включена.

5. В блоке `Внешняя авторизация` переведите переключатель `Включить внешнюю авторизацию` в положение "включено" и выберите провайдера авторизации RADIUS.

6. 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.

   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`).

7. 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`.

8. Нажмите `Сохранить`.

Внешняя авторизация через RADIUS 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.

3.4 Обновление системы

В этом разделе:

- *Обновление Angie ADC*
- *Приложение: пути обновления Angie ADC*

3.4.1 Обновление Angie ADC

Поддерживается обновление Angie ADC:

- *с версии 1.1.1 до версии 1.2*.
- с версии 1.1 до версии 1.1.1;
- с версии 1.0 до версии 1.1.

Обновление более ранних версий см. здесь.

3.4.1.1 Предварительные действия

Перед обновлением рекомендуется создать или обновить резервную копию узла, а также сохранить ее во внешнем хранилище.

3.4.1.2 Откат обновления

Важно

Откат после обновления версии Angie ADC не предусмотрен.

В случае необходимости откатиться к предыдущей версии Angie ADC можно выполнить миграцию узла (перенести сохраненную резервную копию на новое оборудование). Подробнее см. adc_backup-and-restore.

3.4.1.3 Обновление с версии 1.1.1 до версии 1.2

Обновление Angie ADC с версии 1.1.1 до версии 1.2 выполняется с помощью файла обновления `adc-update-1.1.1-to-1.2.angie`, который находится по ссылке https://download.angie.software/adc/updates/.

Предварительные действия

- Скачайте файл обновления `adc-update-1.1.1-to-1.2.angie` из репозитория по ссылке https://download.angie.software/adc/updates/.
- Убедитесь, что файл обновления имеет права 755, т.е. полный доступ (чтение, запись, выполнение) есть только у владельца, а у группы и остальных — доступ на чтение и запуск.
- Расформируйте пару высокой доступности, если она была создана, иначе обновление пары завершится ошибкой.
- Если у вас был развернут кластер, то процедуру обновления необходимо начинать с узла, который является точкой входа. Затем, не меняя конфигурацию на узле точке-входа, обновите остальные узлы кластера. После завершения обновления всех узлов кластера можно вносить изменения в конфигурацию.

Шаги обновления

1. Запустите *интерфейс командной строки* на порту 2222 и скопируйте файл обновления в корневую папку Angie ADC, сохраняя права файлов.

```
$ scp -p -P 2222 adc-update-1.1.1-to-1.2.angie admin@adc.example.com:/
```

Примечание

Если нет возможности скопировать файл обновления с сохранением прав, то права можно скорректировать на целевой системе клиентом `sftp`.

Пример:

```
sftp -P 2222 admin@adc.example.com
admin@adc.example.com's password:
Connected to adc.example.com.
sftp> ls -l
----------    1 0        0        379487220 September 25 10:07 adc-update-1.1.
↪1-to-1.2.angie
sftp> chmod 755 adc-update-1.1.1-to-1.2.angie
Changing mode on /adc-update-1.1.1-to-1.2.angie
sftp> ls -l
-rwxr-xr-x    1 0        0        379487220 September 25 10:07 adc-update-1.1.
↪1-to-1.2.angie
sftp>
```

2. Запустите файл обновления `adc-update-1.1.1-to-1.2.angie`:

```
ssh -p 2222 admin@adc.example.com
admin@adc.example.com's password:
$$ system
(system)$$ upgrade adc-update-1.1.1-to-1.2.angie

WARNING!
==========
You are about to upgrade the ADC system.
This operation may cause service interruption.
IMPORTANT: Once started, the upgrade process CANNOT be interrupted!
Please make sure you have:
  1. Scheduled maintenance window
  2. Backed up your data
  3. Notified relevant stakeholders

Do you want to proceed with the upgrade? [y/N] y
Checking script signature...
Verified OK
[2026-09-25 10:32:23] ADC Update Package
...
```

В процессе обновления соединение с CLI Angie ADC может прерваться. В таком случае через несколько минут заново подключитесь к CLI.

Можно просмотреть журнал обновления Angie ADC (`logs upgrade`). Если в сообщениях есть строка `Upgrade completed successfully`, то обновление прошло успешно:

```
$$ logs upgrade
...
[2026-09-25 11:43:17] Upgrade completed successfully
[2026-09-25 11:43:17] WARNING: All cli sessions may be terminated within the␣
↪next 3 minutes to complete the upgrade procedure.
```

3.4.2 Приложение: пути обновления Angie ADC

Обновление выполняется с помощью файла(ов) обновления. Все файлы обновления можно просмотреть и скачать по ссылке https://download.angie.software/adc/updates/. Инструкции по обновлению см. *Обновление Angie ADC*.

В таблицах ниже приведены пути обновления до целевой версии Angie ADC. В левом столбце указаны исходные версии, а в верхней строке — целевые версии, до которых можно обновиться. В ячейках приведены ссылки на скачивание файлов обновления соответствующих версий.

Важно

Обновление с версии 1.0-rc2 до версии 1.0 не поддерживается.

3.4.2.1 Обновление с версии 1.0 и выше

Поддерживается обновление Angie ADC версии 1.0 до версии 1.2.

Примечание

Если для вашей исходной версии отсутствует прямое обновление до целевой версии, то рекомендуется последовательное обновление.

Версия	1.1	1.1.1	1.2
1.0	1.0-to-1.1	--	--
1.1	--	1.1-to-1.1.1	--
1.1.1	--	--	1.1.1-to-1.2

3.4.2.2 Обновление до версии 1.0-rc2

Поддерживается обновление Angie ADC версии 0.4.0 до версии 1.0-rc2.

Примечание

Если для вашей исходной версии отсутствует прямое обновление до целевой версии, то рекомендуется последовательное обновление. Пример пути обновления: 0.6.0 → 0.7.3 → 0.8.1 → 0.8.2 → 1.0-rc1 → 1.0-rc2.

Версия	0.5.0	0.5.2	0.6.0	0.7.0	0.7.1	0.7.2	0.7.3	0.8.0	0.8.1	0.8.2	1.0-rc1	1.0-rc2
0.4.0	0.4.0 to-0.5.0	--	--	--	--	--	--	--	--	--	--	--
0.5.0	--	0.5.0 to-0.5.2	0.5.x to-0.6.0	--	--	--	--	--	--	--	--	--
0.5.2	--	--	0.5.x to-0.6.0	--	--	--	--	--	--	--	--	--
0.6.0	--	--	--	--	0.6.0-to-0.7.1.stag 0.6.0-to-0.7.1.stag 0.6.0-to-0.7.x.stag	0.6.0-to-0.7.2.stag 0.6.0-to-0.7.2.stag 0.6.0-to-0.7.x.stag	0.6.0-to-0.7.3.stag 0.6.0-to-0.7.3.stag 0.6.0-to-0.7.x.stag	--	--	--	--	--
0.7.0	--	--	--	--	--	--	--	--	--	--	--	--
0.7.1	--	--	--	--	--	0.7.x-to-0.7.2	0.7.x-to-0.7.3	0.7.x-to-0.8.0.st 0.7.x-to-0.8.0.st	0.7.x-to-0.8.1.st 0.7.x-to-0.8.1.st	--	--	--
0.7.2	--	--	--	--	--	--	0.7.x-to-0.7.3	0.7.x-to-0.8.0.st 0.7.x-to-0.8.0.st	0.7.x-to-0.8.1.st 0.7.x-to-0.8.1.st	--	--	--
0.7.3	--	--	--	--	--	--	--	0.7.x-to-0.8.0.st 0.7.x-to-0.8.0.st	0.7.x-to-0.8.1.st 0.7.x-to-0.8.1.st	--	--	--
0.8.0	--	--	--	--	--	--	--	--	0.8.0-to-0.8.1.st 0.8.0-to-0.8.1.st	0.8.x-to-0.8.2.st 0.8.x-to-0.8.2.st	--	--
0.8.1	--	--	--	--	--	--	--	--	--	0.8.x-to-0.8.2.st 0.8.x-to-0.8.2.st	--	--
0.8.2	--	--	--	--	--	--	--	--	--	--	0.8.2-to-1.0-rc1.stag 0.8.2-to-1.0-rc1.stag	--
1.0-rc1	--	--	--	--	--	--	--	--	--	--	--	1.0-rc1-to-1.0-

ГЛАВА 4

Интерфейс командной строки (CLI) Angie ADC

Рекомендуемый интерфейс для всех операций кроме настройки VRRP — CLI на порту 2222 или 22.

Примечание

Настройка VRRP поддерживается только через CLI на порту 2022 (подробнее см. VRRP-маршрутизация).

Возможности: автодополнение команд по `TAB`; поддержка истории команд; подсказки по синтаксису команд по нажатию `?`; поддержка цветовой схемы; поддержка сокращенных команд.

Запуск CLI на порту 2222

При запуске Angie ADC интерфейс командной строки Angie ADC будет доступен по SSH-протоколу на порту 2222. Доступ осуществляется с помощью SSH-клиента.

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 `?`.

3. Для настройки протоколов BGP, OSPF и BFD дополнительно перейдите в настройки `vtysh`:

   ```
   vtysh
   ```

   Команда переключит вас в конфигурационный режим, где можно вносить изменения.

Запуск CLI на порту 2022

При запуске Angie ADC интерфейс командной строки Angie ADC будет доступен по SSH-протоколу на порту 2022. Доступ осуществляется с помощью SSH-клиента.

Чтобы запустить интерфейс командной строки (CLI), выполните следующие действия:

1. Подключитесь к SSH-серверу:

   ```
   ssh -p 2022 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 `?`.

3. Для настройки протоколов BGP, OSPF и BFD дополнительно перейдите в настройки `vtysh`:

   ```
   vtysh
   ```

   Команда переключит вас в конфигурационный режим, где можно вносить изменения.

4.1 Поддерживаемые команды

Ниже приведен список команд в алфавитном порядке для новой версии CLI (на порту 2222).

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*	Переход в режим настройки Angie ADC
commit	Применение конфигурации-кандидата вместо текущей конфигурации.
end	Выход из режима настройки `configuration`.
rollback	Отмена всех изменений в конфигурации-кандидате.
set	Изменение текущей конфигурации: добавление строки (создает конфигурацию-кандидат): • системные настройки: hostname / interface / sysctl / timezone; • настройки маршрутизации: ip route / rule.
show	Просмотр текущей конфигурации и конфигурации-кандидата.
unset	Изменение текущей конфигурации: удаление строки (создает конфигурацию-кандидат).
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.

продолжается на следующей странице

Таблица 1 – продолжение с предыдущей страницы

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 параметров ядра Linux в реальном времени
syslog	Управление syslog/Logstash-серверами логирования.
10. *system*	Перезагрузка и обновление Angie ADC
ntp	Просмотр и настройка NTP
reboot	Перезагрузка системы Angie ADC
stat	Просмотр статистики системы Angie ADC
time	Просмотр и установка системного времени
timezone	Просмотр часового пояса системы
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

продолжается на следующей странице

Таблица 1 – продолжение с предыдущей страницы

13. *vtysh*	Переход к настройкам маршрутизации по протоколам BGP и OSPF
14. *web*	Настройка веб-интерфейса Angie ADC
upload-cert	Загрузка сертификата управления и ключа
tls	Включение / выключение HTTPS

Служебные команды:

`exit` или `Ctrl+Z`	Выход из контекста
`quit` или `Ctrl+Q`	Завершение сессии
`show`	Вывод текущего состояния
`?`	Список доступных команд

4.2 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

4.3 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

4.3.1 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
```

4.3.2 info

Просмотр информации о сертификате.

Синтаксис: `info <name>`.

Параметры:

- `<name>` — имя сертификата.

Пример:

```
(certificates)$$ info cert1
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C = RU, ST = Moscow, O = Angie, OU = EVO, CN = Root CA
        Validity
            Not Before: Feb 18 12:23:08 2025 GMT
            Not After : Feb 18 12:23:08 2027 GMT
        Subject: CN = Demo Certificate, ST = Moscow, C = RU, O = Angie, OU = EVO
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
...
(certificates)$$
```

4.3.3 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 управления*.

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.

4.3.4 remove

Удаление сертификатов и ключей Angie ADC.

Синтаксис: `remove <name>`.

Параметры:

- `<name>` — имя сертификата.

Пример:

```
(certificates)$$ remove cert1
Certificate 'cert1' deleted successfully
```

4.4 configuration

Режим настройки Angie ADC. В этом режиме можно изменять текущую конфигурацию Angie ADC.

Чтобы внести изменения:

1. Задайте необходимые параметры с помощью команд `set` (добавляет строку) и `unset` (удаляет строку).
2. Сравните текущую конфигурацию и конфигурацию-кандидат с помощью команды `show`.
3. Примените изменения с помощью команды `commit`.

> **Примечание**
>
> Изменения будут применены только после выполнения команды `commit`.

Если необходимо, вы можете откатить всю конфигурацию-кандидат с помощью команды `rollback` до ее сохранения.

Пример:

```
$$ configuration
## set system interface enp0s2 type dhcp
## show
```

```
-> Current configuration
set system interface enp0s2 type static
set system interface enp0s2 ip address 10.21.20.31/22
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 dns 1.1.1.1

-> Candidate configuration
set system interface enp0s2 type dhcp
## commit
```

Поддерживаемые команды:

`configuration`	Вход в режим настройки
commit	Применение конфигурации-кандидата вместо текущей конфигурации.
end	Выход из режима настройки `configuration`.
rollback	Отменяет все изменения в конфигурации-кандидате.
set	Изменение текущей конфигурации: добавление строки (создает конфигурацию-кандидат).
show	Просмотр текущей конфигурации и конфигурации-кандидата.
unset	Изменение текущей конфигурации: удаление строки (создает конфигурацию-кандидат).

4.4.1 commit

Применение конфигурации-кандидата в качестве активной конфигурации.

4.4.2 end

Выход из режима `configuration`.

4.4.3 rollback

Отменяет все изменения в конфигурации-кандидате.

4.4.4 set

Переход к изменению текущей конфигурации Angie ADC.

Примечание

Будет создана конфигурация-кандидат. Изменения будут применены только после выполнения команды `commit`.

Синтаксис: `set system <system_input> | ip <ip_input>`, где:

- `system <system_input>` — изменение параметров конфигурации (hostname / interface / sysctl / timezone);
- `ip <ip_input>` — настройка маршрутов и правил IP-трафика (route / rule).

Возможные варианты `<system_input>`:

- `set system hostname <name>` — установка имени хоста для Angie ADC.
- `set system interface <name> {ip <keyword> <value> | type {static | dhcp}}` — настройка интерфейса.

  - Возможные значения для `<keyword>`:
    - `address` — установка IP-адреса для интерфейса.
    - `gateway` — установка шлюза для интерфейса.
    - `dns` — установка DNS-адреса для интерфейса.
    - `searches` — установка доменов поиска для интерфейса (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.

- `set system sysctl <variable> <value>` — настройка параметров ядра Linux (`variable` — настраиваемый параметр, `value` — его значение).
- `set system timezone <value>`

  Часовой пояс определяет смещение локального времени относительно UTC. Изменение часового пояса не изменяет системное время (Unix timestamp), а только влияет на его отображение. Часовой пояс должен быть указан в формате IANA Time Zone Database (например, `Europe/Moscow`) или в виде аббревиатуры (например, `UTC`, `EST`, `PST`).

Примеры:

```
$$ configuration
## set system hostname adc-home
## 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 sysctl net.ipv4.ip_forward 1
## set system sysctl net.core.somaxconn 1024
## set system timezone Europe/Moscow
```

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
```

4.4.5 show

Просмотр текущей конфигурации и конфигурации-кандидата.

4.4.6 unset

Переход к изменению текущей конфигурации Angie ADC. Удаляет параметр из конфигурации-кандидата.

> **Примечание**
>
> Будет создана конфигурация-кандидат. Изменения будут применены только после выполнения команды `commit`.

Пример:

```
$$ configuration
## unset ip rule from 0.0.0.0/0 table 100
## show
-> Current configuration
set system interface enp0s2 type static
set system interface enp0s2 ip address 10.21.20.31/22
set ip rule from 0.0.0.0/0 table 100

-> Candidate configuration
set system interface enp0s2 type static
set system interface enp0s2 ip address 10.21.20.31/22
 ## commit
```

4.5 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.

4.5.1 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.

4.5.2 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`

4.5.3 nslookup

Выполнение DNS-запросов.

4.5.3.1 Разовый запрос

Синтаксис: `nslookup <host>`

Примеры:

- `(diagnostics)$$ nslookup example.com` — прямой DNS-запрос.
- `(diagnostics)$$ nslookup 203.0.113.10` — обратный DNS-запрос (PTR).

4.5.3.2 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`.

4.5.4 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.

4.5.5 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).

4.5.6 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>]`

4.5.6.1 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 `""`.

4.5.6.2 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.

4.5.6.3 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.

4.5.6.4 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 `=`.

4.5.7 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.

4.5.8 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.

4.5.9 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.

4.6 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

4.6.1 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)$$ list ip
tcp 9999 enp0s2
(firewall)$$
```

4.6.2 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`.

4.6.3 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, 2022, 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

4.6.4 save

Сохранение правил брандмауэра Angie ADC.

Синтаксис: `save`.

4.7 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*.

4.8 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`.

4.8.1 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.

4.8.1.1 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
```

4.8.1.2 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/" "-"
```

4.8.1.3 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
```

4.8.1.4 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/" "-"
```

4.8.1.5 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/" "-"
```

4.9 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

4.9.1 info

Получение информации о динамическом модуле Angie ADC.

Синтаксис: `info <module>`.

Параметры:

- `<module>` — имя модуля.

4.9.2 list

Получение списка доступных динамических модулей Angie ADC.

Синтаксис: `list`.

4.10 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.

4.11 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 параметров ядра Linux в реальном времени
syslog	Управление syslog-серверами

4.11.1 angie debug

Включение режима отладки для локального балансировщика нагрузки.

Синтаксис: `angie debug`.

4.11.2 no angie debug

Отключение режима отладки `angie`.

Синтаксис: `no angie debug`.

4.11.3 reload

Перезагрузка элементов Angie ADC.

Синтаксис: `reload {angie|prometheus}`.

Параметры:

- `angie` — перезагрузка `angie-mgmt`.
- `prometheus` — перезагрузка `prometheus`.

4.11.4 sysctl

Просмотр конкретного параметра ядра Linux или всех параметров в реальном времени.

Синтаксис: `sysctl show {<variable> | all}`.

4.11.5 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.

4.12 system

Контекст `system` для управления системой Angie ADC.

Поддерживаемые команды:

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 часового пояса системы
upgrade	Обновление Angie ADC
version	Просмотр версии Angie ADC

4.12.1 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
```

4.12.2 reboot

Перезагрузка системы Angie ADC.

Синтаксис: `reboot [force]`

Параметры:

- `force` — принудительная перезагрузка.

4.12.3 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.

4.12.4 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.

4.12.5 timezone

Просмотр часового пояса системы. Часовой пояс определяет смещение локального времени относительно UTC.

Синтаксис: `timezone`.

Примеры:

- `(system)$$ timezone` — показать текущий часовой пояс.

> **Примечание**
>
> Настройка timezone проводится через меню конфигурации (*configuration*).

4.12.6 upgrade

Обновление Angie ADC.

Синтаксис: `upgrade <filename>`

Параметры:

- `<filename>` — имя файла.

4.12.7 version

Просмотр версии Angie ADC.

Синтаксис: `version [detail]`

Параметры:

- `detail` — подробный вывод версии.

4.13 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`

4.13.1 edit

Позволяет редактировать файлы в текущей директории.

Синтаксис: `edit [<filename>]`.

Параметры:

- `<filename>` — имя файла, который необходимо отредактировать (обязательный параметр).

4.13.2 ls

Получение списка файлов в директории `transfer`.

Синтаксис: `ls`.

4.13.3 rm

Удаление файла в директории `transfer`.

Синтаксис: `rm <filename>`.

Параметры:

- `<filename>` — имя файла.

4.13.4 view

Просмотр содержимого файла в директории `transfer`.

Синтаксис: `view <filename> [page]`.

Параметры:

- `<filename>` — имя файла;
- `page` — вывод записей в режиме постраничного просмотра.

4.14 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

4.14.1 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.

4.14.2 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
```

4.14.3 info

Просмотр информации о доверенном сертификате.

Синтаксис: `info <name>`.

Параметры:

- `<name>` — имя сертификата.

Пример:

```
(trusted-ca)$$ info ca-test
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            52:58:66:fb:72:68:1b:4b:b4:97:67:0f:a8:91:ca:c7:09:7e:fa:16
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=RU, ST=Test, L=Test, O=ADC-TestCA, CN=ADC Test CA
        Validity
            Not Before: May 22 09:35:12 2026 GMT
            Not After : Apr 28 09:35:12 2126 GMT
        Subject: C=RU, ST=Test, L=Test, O=ADC-TestCA, CN=ADC Test CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
...
                CA:TRUE
...
(trusted-ca)$$
```

4.14.4 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.
```

4.15 vtysh

Переход к настройкам маршрутизации по протоколам BGP и OSPF.

Синтаксис: `vtysh`.

Подробнее о настройке BGP и OSPF см. BGP-маршрутизация и OSPF-маршрутизация.

4.16 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

4.16.1 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 управления*.

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.

4.16.2 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 5

Права на интеллектуальную собственность

Документация на программный продукт Angie ADC является интеллектуальной собственностью ООО «Веб-Сервер».

Copyright © 2026, ООО «Веб-Сервер». Все права защищены.