ООО «Веб-Сервер», ОГРН 1227700436578, ИНН 9704151517
ул. Льва Толстого, д. 14, этаж 1, кв. 2, г. Москва, 119021

Руководство по эксплуатации

версия 1.7.0

ООО «Веб-Сервер»

сент. 25, 2024

Оглавление

1 Аннотация **1**

2 Общие сведения **2**

3 Настройка **4**
3.1 Общие сведения . . . 4
3.1.1 Конфигурационные файлы . . . 4
3.1.2 Управление во время выполнения . . . 7
3.1.3 Соединения, сессии, запросы, логирование . . . 10
3.2 Справочники и указатели . . . 19
3.2.1 Встроенные модули . . . 20
3.2.2 Встроенные переменные . . . 460
3.3 Инструкции . . . 462
3.3.1 Миграция с nginx на Angie . . . 463
3.3.2 Настройка модуля ModSecurity . . . 467
3.3.3 Настройка SSL . . . 468
3.3.4 Веб-панель мониторинга Console Light . . . 473
3.3.5 Настройка панели Prometheus . . . 490

4 Отладка **492**
4.1 Отладочный лог . . . 492
4.1.1 Лог для отдельных адресов . . . 494
4.1.2 Кольцевой буфер в памяти . . . 494

5 Права на интеллектуальную собственность **495**

Алфавитный указатель **496**

ГЛАВА 1

Аннотация

Настоящий документ содержит информацию, необходимую для эксплуатации программного обеспечения Angie PRO.

ГЛАВА 2

Общие сведения

Angie PRO – единственный коммерческий веб-сервер, разработка которого локализована в России.

Веб-сервер — это класс программного обеспечения, предоставляющего доступ к сетевым ресурсам по протоколу HTTP конечным пользователям. Angie PRO, например, может использоваться для работы интернет-сайтов, мобильных приложений, киосков самообслуживания в метрополитене, мультимедийных систем в поездах дальнего следования. Каждый раз, когда пользователь открывает сайт, мобильное приложение, пользуется киоском самообслуживания в метрополитене, или даже мультимедийной системой в поезде «Сапсан», запрос пользователя может быть обработан Angie PRO.

Angie PRO — это:

- **Веб-сервер общего назначения.** Написан на языке C.
- **Балансировщик L4-L7.** Позволяет балансировать нагрузку между серверами как по протоколам TCP/UDP, так и по HTTP.
- **Проксирующий и кэширующий сервер.** Позволяет ускорять работу веб-сервисов с помощью гибкого механизма кэширования.
- **Доступен под все популярные платформы.** Собирается и тестируется под Alpine, Debian, Oracle, RED OS, Rocky, Ubuntu.
- **Производительность.** Один из самых производительных веб-серверов в мире.

Почему Angie PRO:

- **Совместимость с NGINX OSS.** Angie PRO полностью совместим с Nginx, таким образом любой существующий пользователь Nginx может без серьёзных затрат и простоя сервисов перейти на Angie PRO.
- **Расширенная статистика и мониторинг в реальном времени.** Angie PRO имеет возможность полного мониторинга нагрузки сервера в режиме реального времени, что позволяет динамически управлять конфигурациями по профилю нагрузки и соблюдать полную доступность сервиса.
- **Динамическая конфигурация групп проксируемых серверов.** Возможность управлять настройками групп проксируемых серверов с помощью удобного REST интерфейса без остановки сервиса.
- **Удаление элементов кэша.** Возможность удаления элементов кеша через удобное API без остановки сервиса.

- **Активная проверка состояния проксируемых серверов.** Проверка на «живучесть» и проксирование только на те группы проксируемых серверов, которые отвечают по заданному алгоритму.
- **Динамическое хранилище ключ-значение».** Динамическое управление переменными конфигурации Angie PRO через HTTP API.
- **Динамическое обновление DNS.**
- **Проксирование с привязкой сессий.**
- **Репозиторий с динамическими сторонними модулями.** Angie PRO поддерживает большинство сторонних модулей NGINX и даёт возможность без проблем устанавливать их, предоставляя гарантию их работоспособности и поддержку.
- **Синхронизация зон разделяемой памяти.** Возможность использовать зоны кеша, limit_req и т.д. в кластере Angie PRO.
- **Сокрытие или персональный брендинг имени сервера в заголовках ответа.** Возможность изменить или скрыть название и версию веб-сервера от пользователей.

Перечень иностранного программного обеспечения, имеющего сходство функциональных характеристик с программным обеспечением Angie PRO: Nginx, Nginx Plus, Apache, Envoy, продукты, использующие решения NGINX (OpenResty, Tengine, Cloudflare), облачные решения Яндекса.

ГЛАВА 3

Настройка

На этой странице собраны статьи, справочники, указатели и инструкции по настройке Angie PRO.

3.1 Общие сведения

В этих статьях рассказывается об установке и настройке Angie PRO, запуске и остановке веб-сервера, управлении им, а также различных аспектах обработки запросов и взаимодействия с другими серверами.

3.1.1 Конфигурационные файлы

Angie PRO использует текстовый конфигурационный файл. По умолчанию этот файл называется `angie.conf` и находится в соответствии с параметром сборки –conf-path, обычно в директории `/etc/angie`.

Конфигурационный файл обычно состоит из следующих контекстов:

- `events` — Общая обработка соединений
- `http` — HTTP трафик
- `mail` — Почтовый трафик
- `stream` — TCP и UDP трафик

Директивы, размещенные вне этих контекстов, считаются находящимися в контексте `main`:

```
user angie; # директива в контексте 'main'

events {

    # конфигурация обработки соединений
}

http {

    # Конфигурация трафика HTTP, для всех вложенных виртуальных серверов
```

```
    server {

        # конфигурация виртуального HTTP сервера 1
        location /one {

            # конфигурация обработки HTTP запросов с URI, начинающимися с '/one'
        }
        location /two {

            # конфигурация обработки HTTP запросов с URI, начинающимися с '/two'
        }
    }

    server {

        # конфигурация виртуального HTTP сервера 2
    }
}

stream {

    # Конфигурация трафика TCP/UDP, для всех вложенных виртуальных серверов
    server {

        # конфигурация виртуального TCP сервера 1
    }
}
```

Для упрощения управления конфигурацией рекомендуется использовать директиву *include* в основном файле `angie.conf`, чтобы ссылаться на содержимое файлов, специфичных для функций:

```
include /etc/angie/http.d/*.conf;
include /etc/angie/stream.d/*.conf;
```

Наследование

В общем случае дочерний контекст (тот, который содержится в другом контексте, который считается родительским) унаследует настройки директив, определенных на уровне родителя. Некоторые директивы могут появляться в нескольких контекстах; в таких случаях вы можете переопределить настройки, унаследованные от родителя, включив директиву в дочерний контекст.

Синтаксис

Единицы измерения

Размеры могут быть указаны в байтах (без суффикса), килобайтах (суффиксы `k` и `K`) или мегабайтах (суффиксы `m` и `M`), например, `"1024"` (байт), `"8k"`, `"1m"`.

Интервалы времени могут быть указаны в миллисекундах, секундах, минутах, часах, днях и так далее, с использованием следующих суффиксов:

`ms`	Миллисекунды
`s`	Секунды
`m`	Минуты
`h`	Часы
`d`	Дни
`w`	Недели
`M`	Месяцы (принято считать равными 30 дням)
`y`	Годы (принято считать равными 365 дням)

Несколько единиц могут быть объединены в одном значении, указывая их в порядке от наиболее значимого к наименее значимому, при необходимости разделяя пробелами. Например, `"1h 30m"` обозначает тот же промежуток времени, что и `"90m"` или `"5400s"`. Значение без суффикса интерпретируется как секунды. Рекомендуется всегда указывать суффикс.

Некоторые интервалы времени могут быть указаны только с разрешением в секундах.

Директивы

Каждая директива состоит из имени и набора параметров. Если какая-либо часть директивы должна содержать пробелы, они должна быть заключены в кавычки или экранированы:

```
add_header X-MyHeader "foo bar";
add_header X-MyHeader foo\ bar;
```

Если именованный параметр требует пробелов и вы используете кавычки, его имя также должно быть заключено в кавычки:

```
server example.com "sid=server 1";
```

Настройка хэшей

Для эффективной обработки статических наборов данных, таких как имена серверов, значения директивы *map*, MIME-типы и имена заголовков запросов, Angie PRO использует хэш-таблицы. При запуске и каждом переопределении конфигурации Angie PRO определяет оптимальный размер для этих хэш-таблиц, чтобы размер корзины, которая хранит ключи с одинаковыми хэш-значениями, не превышал заданный параметр (*hash bucket size*). Размер таблицы измеряется в корзинах и корректируется до тех пор, пока не превысит параметр *hash max size*. Большинство хэш-таблиц имеют соответствующие директивы для настройки этих параметров, такие как *server_names_hash_max_size* и *server_names_hash_bucket_size* для имен серверов.

Параметр *hash bucket size* выравнивается по кратности размера линии кэша процессора. Такое выравнивание улучшает эффективность поиска ключей на современных процессорах, уменьшая количество обращений к памяти. Если *hash bucket size* равен размеру одной линии кэша, максимальное количество обращений к памяти во время поиска ключа будет два: одно для вычисления адреса корзины и второе для поиска внутри корзины. Поэтому, если Angie PRO сообщает, что следует увеличить либо *hash max size*, либо *hash bucket size*, начните с увеличения *hash max size*.

Перезагрузка конфигурации

Чтобы применить изменения в конфигурационном файле, его необходимо перезагрузить. Вы можете либо перезапустить процесс Angie PRO с предварительной проверкой синтаксиса конфигурации:

```
$ sudo angie -t && sudo service angie restart
```

Либо перезагрузить службу, чтобы применить новую конфигурацию без прерывания обработки текущих запросов:

```
$ sudo angie -t && sudo service angie reload
```

3.1.2 Управление во время выполнения

Чтобы запустить Angie PRO, используйте `systemd` и следующую команду:

```
$ sudo service angie start
```

Рекомендуется предварительно проверить синтаксис конфигурации. Вот как это сделать:

```
$ sudo angie -t && sudo service angie start
```

Чтобы перезагрузить конфигурацию:

```
$ sudo angie -t && sudo service angie reload
```

Чтобы остановить Angie PRO:

```
$ sudo service angie stop
```

После установки выполните следующую команду, чтобы убедиться, что Angie PRO работает:

```
$ curl localhost:80
```

> **Примечание**
>
> Методы запуска открытой версии Angie могут различаться в зависимости от метода установки.

Angie PRO имеет один главный процесс и несколько рабочих процессов. Главный процесс отвечает за чтение и оценку конфигурации и управление рабочими процессами. Рабочие процессы обрабатывают фактические запросы. Angie PRO использует модель на основе событий и механизмы, зависящие от ОС, для эффективного распределения запросов между рабочими процессами. Количество рабочих процессов определяется в конфигурационном файле и может быть фиксированным для данной конфигурации или автоматически регулироваться в зависимости от числа доступных ядер CPU (см. *worker_processes*).

Использование сигналов

Angie PRO также можно управлять с помощью сигналов. По умолчанию идентификатор процесса главного процесса записывается в файл `/var/run/angie.pid`. Это имя файла можно изменить во время конфигурации или в файле `angie.conf` с помощью директивы *pid*. Главный процесс поддерживает следующие сигналы:

`TERM`, `INT`	Быстрое завершение работы
`QUIT`	*Постепенное завершение* работы
`HUP`	Перезагрузка конфигурации, обновление часового пояса (только для FreeBSD и Linux), запуск новых рабочих процессов с обновленной конфигурацией, *постепенное завершение* старых рабочих процессов
`USR1`	Перезапуск файлов журналов
`USR2`	Обновление исполняемого файла
`WINCH`	*Постепенное завершение* рабочих процессов

Отдельные рабочие процессы также можно контролировать с помощью сигналов, хотя это не обязательно. Поддерживаются следующие сигналы:

`TERM`, `INT`	Быстрое завершение работы
`QUIT`	*Постепенное завершение* работы
`USR1`	Перезапуск файлов журналов
`WINCH`	Аномальное завершение работы для отладки (требуется включение *debug_points*)

Изменение конфигурации

Чтобы Angie PRO перечитал конфигурационный файл, необходимо отправить сигнал `HUP` главному процессу. Сначала главный процесс проверяет корректность синтаксиса, а затем пытается применить новую конфигурацию, что включает в себя открытие новых файлов журналов и сокетов для прослушивания. Если применение новой конфигурации не удалось, главный процесс откатывает изменения и продолжает работу со старой конфигурацией. Если применение прошло успешно, главный процесс запускает новые рабочие процессы и отправляет сообщения старым рабочим процессам с просьбой завершиться *постепенно*. Старые рабочие процессы закрывают свои сокеты для прослушивания и продолжают обслуживать существующих клиентов. После того как все клиенты будут обслужены, старые рабочие процессы завершатся.

Angie PRO отслеживает изменения конфигурации для каждого процесса. Номера поколений начинаются с 1, когда сервер запускается впервые. Эти номера увеличиваются с каждым перезагрузкой конфигурации и видны в заголовках процессов:

```
$ sudo angie
$ ps aux | grep angie

   angie: master process v1.7.0 #1 [angie]
   angie: worker process #1
```

После успешной перезагрузки конфигурации (независимо от того, были ли фактические изменения), Angie PRO увеличивает номер поколения для процессов, которые получили новую конфигурацию:

```
$ sudo angie -s reload
$ ps aux | grep angie

   angie: master process v1.7.0 #2 [angie]
   angie: worker process #2
```

Если какие-либо рабочие процессы из предыдущих поколений продолжают работать, они сразу же станут заметны:

```
$ ps aux | grep angie

   angie: worker process #1
   angie: worker process #2
```

Примечание

Не путайте номер поколения конфигурации с неким „номером процесса“; Angie PRO не использует непрерывную нумерацию процессов для практических целей.

Ротация лог-файлов

Для ротации лог-файлов сначала переименуйте файлы. Затем отправьте сигнал `USR1` главному процессу. Главный процесс снова откроет все открытые лог-файлы и назначит их непривилегированному пользователю, под которым работают рабочие процессы. После успешного открытия файлов главный процесс закроет все открытые файлы и уведомит рабочие процессы о необходимости открыть свои лог-файлы. Рабочие процессы также немедленно откроют новые файлы и закроют старые. В результате старые файлы становятся доступными для последующей обработки, такой как сжатие, почти сразу.

Обновление исполняемого файла на лету

Чтобы обновить исполняемый файл сервера, сначала замените старый исполняемый файл на новый. Затем отправьте сигнал `USR2` главному процессу. Главный процесс переименует свой текущий файл с идентификатором процесса в новый файл с суффиксом `.oldbin`, например, `/usr/local/angie/logs/angie.pid.oldbin`, и затем запустит новый исполняемый файл, который, в свою очередь, запустит новые рабочие процессы.

Обратите внимание, что старый главный процесс не закрывает свои сокеты для прослушивания и может быть управляем для перезапуска своих рабочих процессов в случае необходимости. Если новый исполняемый файл работает не так, как ожидалось, вы можете предпринять следующие действия:

- Отправьте сигнал `HUP` старому главному процессу. Это запустит новые рабочие процессы без повторного чтения конфигурации. После этого вы можете завершить все новые процессы *постепенно*, отправив сигнал `QUIT` новому главному процессу.
- Отправьте сигнал `TERM` новому главному процессу. Он отправит сообщение своим рабочим процессам с просьбой немедленно выйти. Если какие-либо процессы не выходят, отправьте сигнал `KILL`, чтобы заставить их выйти. Когда новый главный процесс завершится, старый главный процесс автоматически запустит новые рабочие процессы.

Если новый главный процесс завершится, старый главный процесс удалит суффикс `.oldbin` из имени файла с идентификатором процесса.

Если обновление прошло успешно, отправьте сигнал `QUIT` старому главному процессу, и останутся только новые процессы.

Параметры командной строки

`-?`, `-h`	Вывод справки по параметрам командной строки, затем выход.
`--build-env`	Вывод вспомогательной информации об окружении сборки, затем выход.
`-c` *файл*	Запуск с альтернативным *файлом* конфигурации вместо *файла по умолчанию*.
`-e` *файл*	Запуск с альтернативным лог-*файлом* ошибок вместо *файла по умолчанию*. Специальное значение `stderr` задает стандартный файл ошибок.
`-g` *директивы*	Запуск с установкой *глобальных директив конфигурации*, например: `angie -g "pid /var/run/angie.pid; worker_processes `sysctl -n hw.ncpu`;"`.
`-m`, `-M`	Вывод списка встроенных (`-m`) или встроенных и загруженных (`-M`) модулей, затем выход.
`-p` *префикс*	Запуск с заданным *префиксом* пути `angie` (каталога, в котором будут находиться файлы сервера; по умолчанию — `/usr/local/angie/`).
`-q`	Вывод только сообщений об ошибках, если заданы `-t` или `-T`; иначе эффекта нет.
`-s` *сигнал*	Отправка *сигнала* главному процессу: `stop`, `quit`, `reopen`, `reload` и так далее.
`-t`	Тестирование файла конфигурации, затем выход. Angie PRO проверяет синтаксис конфигурации, рекурсивно включая файлы, упомянутые в ней.
`-T`	То же, что `-t`, но с выводом сводной конфигурации в стандартный поток вывода после рекурсивного включения всех упомянутых в ней файлов.
`-v`	Вывод версии Angie PRO, затем выход.
`-V`	Вывод версии Angie PRO, версии компилятора и использованных параметров сборки, затем выход.

3.1.3 Соединения, сессии, запросы, логирование

Механизмы обработки соединений

Angie PRO поддерживает различные методы обработки соединений. Доступность конкретного метода зависит от используемой платформы. На платформах, поддерживающих несколько методов, Angie PRO обычно автоматически выбирает наиболее эффективный метод. Однако, при необходимости, метод обработки соединений можно явно выбрать с помощью директивы *use*.

Доступны следующие методы обработки соединений:

Метод	Описание
`select`	Стандартный метод. Соответствующий модуль собирается автоматически на платформах, не имеющих более эффективных методов. Опции сборки `--with-select_module` и `--without-select_module` могут быть использованы для принудительного включения или отключения сборки этого модуля.
`poll`	Стандартный метод. Соответствующий модуль собирается автоматически на платформах, не имеющих более эффективных методов. Опции сборки `--with-poll_module` и `--without-poll_module` могут быть использованы для принудительного включения или отключения сборки этого модуля.
`kqueue`	Эффективный метод, доступный на FreeBSD 4.1+, OpenBSD 2.9+, NetBSD 2.0 и macOS.
`epoll`	Эффективный метод, доступный на Linux 2.6+.
`/dev/poll`	Эффективный метод, доступный на Solaris 7 11/99+, HP/UX 11.22+ (eventport), IRIX 6.5.15+ и Tru64 UNIX 5.1A+.
`eventport`	Метод `event ports` доступен на Solaris 10+. (Из-за известных проблем рекомендуется использовать метод `/dev/poll`.)

Обработка HTTP-сессий

Каждый HTTP-запрос проходит через ряд фаз, на каждой из которых выполняется определенный тип обработки.

`Post-read`	Начальная фаза. Модуль *RealIP* вызывается на этой фазе.
`Server-rewrite`	Фаза, на которой обрабатываются директивы из модуля *Rewrite*, определенные в блоке `server` (но вне блока `location`).
`Find-config`	Специальная фаза, на которой выбирается *location* на основе URI запроса.
`Rewrite`	Похожа на фазу `Server-rewrite`, но применяется к правилам *rewrite*, определенным в блоке location, выбранном на предыдущей фазе.
`Post-rewrite`	Специальная фаза, на которой запрос перенаправляется в новое место, как на фазе `Find-config`, если его URI был изменен во время фазы `Rewrite`.
`Preaccess`	На этой фазе стандартные модули Angie PRO, такие как *Limit Req*, регистрируют свои обработчики.
`Access`	Фаза, на которой проверяется право клиента на выполнение запроса, обычно с помощью стандартных модулей Angie PRO, таких как *Auth Basic*.
`Post-access`	Специальная фаза, на которой обрабатывается директива *satisfy any*.
`Precontent`	На этой фазе стандартные модули, такие как директивы *try_files* и *mirror*, регистрируют свои обработчики.
`Content`	Фаза, на которой обычно генерируется ответ. На этом этапе несколько стандартных модулей Angie PRO регистрируют свои обработчики, включая *Index*. Обработчики вызываются последовательно, пока один из них не произведет вывод.
`Log`	Финальная фаза, на которой выполняется логирование запросов. В настоящее время только модуль *Log* регистрирует свой обработчик на этом этапе для ведения журнала доступа.

Обработка TCP/UDP-сессий

TCP/UDP-сессия от клиента проходит через ряд фаз, на каждой из которых выполняется определенный тип обработки:

`Post-accept`	Начальная фаза после принятия соединения от клиента. На этой фазе вызывается модуль *RealIP*.
`Pre-access`	Предварительная фаза для проверки доступа. Модули *Set* вызываются на этой фазе.
`Access`	Фаза для ограничения доступа клиента перед фактической обработкой данных. На этом этапе вызывается модуль *Access*.
`SSL`	Фаза, на которой происходит завершение TLS/SSL. На этой фазе вызывается модуль *SSL*.
`Preread`	Фаза для чтения начальных байт данных в *preread buffer*, чтобы позволить таким модулям, как *SSL Preread*, проанализировать данные до их обработки.
`Content`	Обязательная фаза, на которой данные фактически обрабатываются, обычно с участием модуля *Return*, который отправляет ответ клиенту.
`Log`	Финальная фаза, на которой фиксируется результат обработки сессии клиента. На этой фазе вызывается модуль *Log*.

Обработка запросов

Выбор виртуального сервера

Изначально соединение создается в контексте сервера по умолчанию. Имя сервера может быть определено на следующих этапах обработки запроса, каждый из которых участвует в выборе конфигурации сервера:

- Во время SSL-рукопожатия, заранее, в соответствии с SNI.
- После обработки строки запроса.
- После обработки поля заголовка `Host`.

Если имя сервера не определено после обработки строки запроса или поля заголовка `Host`, Angie PRO использует пустое имя в качестве имени сервера.

На каждом из этих этапов могут применяться различные конфигурации сервера. Поэтому некоторые директивы следует указывать с осторожностью:

- В случае директивы *ssl_protocols* список протоколов устанавливается библиотекой OpenSSL до применения конфигурации сервера в соответствии с именем, запрошенным через SNI. В результате протоколы следует указывать только для сервера по умолчанию.
- Директивы *client_header_buffer_size* и *merge_slashes* применяются до чтения строки запроса. Поэтому эти директивы используют либо конфигурацию сервера по умолчанию, либо конфигурацию сервера, выбранную через SNI.
- В случае директив *ignore_invalid_headers*, *large_client_header_buffers* и *underscores_in_headers*, которые участвуют в обработке полей заголовков запроса, конфигурация сервера дополнительно зависит от того, была ли она обновлена в соответствии со строкой запроса или полем заголовка `Host`.
- Ответ с ошибкой обрабатывается с использованием директивы *error_page* на сервере, который в данный момент обрабатывает запрос.

Виртуальные серверы на основе имен

Сначала Angie PRO определяет, какой сервер должен обрабатывать запрос. Рассмотрим простую конфигурацию, где все три виртуальных сервера слушают на порту 80:

```
server {

    listen 80;
    server_name example.org www.example.org;
    # ...
}

server {

    listen 80;
    server_name example.net www.example.net;
    #  ...
}

server {

    listen 80;
    server_name example.com www.example.com;
    #  ...
}
```

В этой конфигурации Angie PRO определяет, какой сервер должен обработать запрос, основываясь исключительно на поле заголовка `Host`. Если значение этого заголовка не совпадает ни с одним из имен серверов или если запрос не содержит этого заголовка, Angie PRO направит запрос к серверу по умолчанию для этого порта. В приведенной выше конфигурации сервером по умолчанию является первый — что является стандартным поведением Angie PRO. Также можно явно указать, какой сервер должен быть сервером по умолчанию, используя параметр `default_server` в директиве *listen*:

```
server {

    listen 80 default_server;
    server_name example.net www.example.net;
    #  ...
}
```

Примечание

Обратите внимание, что сервер по умолчанию является свойством слушающего сокета, а не имени сервера.

Международные имена

Международные доменные имена (IDNs) должны указываться в директиве *server_ name* с использованием представления ASCII (Punycode):

```
server {

    listen 80;
    server_name xn--e1afmkfd.xn--80akhbyknj4f; # пример.испытание
    #    ...
}
```

Запрет запросов с неопределенными именами серверов

Если запросы без заголовка `Host` нежелательны, можно определить сервер, который просто отклоняет такие запросы:

```
server {

    listen 80;
    server_name "";
    return 444;
}
```

В этой конфигурации имя сервера задано пустой строкой, что соответствует запросам без заголовка `Host`. Затем возвращается специальный нестандартный код 444, который закрывает соединение.

Сочетание виртуальных серверов, основанных на именах и IP-адресах

Рассмотрим более сложную конфигурацию, где некоторые виртуальные серверы слушают на разных адресах:

```
server {

    listen 192.168.1.1:80;
    server_name example.org www.example.org;
    #  ...
}

server {

    listen 192.168.1.1:80;
    server_name example.net www.example.net;
    #  ...
}

server {

    listen 192.168.1.2:80;
    server_name example.com www.example.com;
    #  ...
}
```

В этой конфигурации Angie PRO сначала проверяет IP-адрес и порт запроса по директивам *listen* блоков *server*. Затем он проверяет поле заголовка `Host` запроса по записям *server_name* блоков *server*, которые совпали с IP-адресом и портом. Если имя сервера не найдено, запрос будет обработан сервером по умолчанию. Например, запрос к `www.example.com`, полученный на порту 192.168.1.1:80, будет обработан сервером по умолчанию для этого порта — т.е. первым сервером — поскольку `www.example.com` не определен для этого порта.

Как упоминалось ранее, сервер по умолчанию является свойством слушающего сокета, и можно определить разные серверы по умолчанию для разных портов:

```
server {

    listen 192.168.1.1:80;
    server_name example.org www.example.org;
    #  ...
}

server {

    listen 192.168.1.1:80 default_server;
    server_name example.net www.example.net;
    #  ...
}

server {

    listen 192.168.1.2:80 default_server;
    server_name example.com www.example.com;
    #  ...
}
```

Выбор локаций

Рассмотрим простую конфигурацию PHP-сайта:

```
server {

    listen 80;
    server_name example.org www.example.org;
    root /data/www;

    location / {

        index index.html index.php;
    }

    location ~* \.(gif|jpg|png)$ {

        expires 30d;
    }

    location ~ \.php$ {

        fastcgi_pass localhost:9000;
        fastcgi_param SCRIPT_FILENAME
        $document_root$fastcgi_script_name;
        include fastcgi_params;
    }
}
```

Angie PRO сначала ищет наиболее конкретный префикс `location`, заданный буквальными строками, независимо от их порядка в списке. В приведенной выше конфигурации единственный префикс локации — это `location /`, который соответствует любому запросу и будет использоваться в качестве последнего средства. Затем Angie PRO проверяет локации, определенные с помощью регулярных выражений, в порядке их появления в конфигурационном файле. Первое совпадающее выражение завершает поиск, и Angie PRO использует эту `location`. Если ни одно регулярное выражение не совпадает с запросом, Angie PRO использует наиболее конкретную префиксную `location`, найденную ранее.

Примечание

Локации всех типов проверяют только URI часть строки запроса, исключая аргументы. Это связано с тем, что аргументы в строке запроса могут быть указаны разными способами, например:

- `/index.php?user=john&page=1`
- `/index.php?page=1&user=john`

Кроме того, строка запроса может содержать любое количество параметров:

- `/index.php?page=1&something+else&user=john`

Теперь давайте рассмотрим, как запросы будут обрабатываться в приведенной выше конфигурации:

- Запрос `/logo.gif` сначала соответствует префиксу `location /`, а затем регулярному выражению `.(gif|jpg|png)$`. Поэтому он обрабатывается последней локацией. Используя директиву `root /data/www`, запрос сопоставляется с файлом `/data/www/logo.gif`, и файл отправляется клиенту.

- Запрос `/index.php` также изначально соответствует префиксу `location /`, а затем регулярному выражению `.(php)$`. Следовательно, он обрабатывается последней локацией, и запрос передается серверу FastCGI, слушающему на `localhost:9000`. Директива *fastcgi_param* устанавливает параметр FastCGI `SCRIPT_FILENAME` в `/data/www/index.php`, и сервер FastCGI выполняет файл. Переменная *$document_root* устанавливается в значение директивы `root`, а переменная *$fastcgi_script_name* устанавливается в URI запроса, т.е. `/index.php`.
- Запрос `/about.html` соответствует только префиксу `location /`, поэтому он обрабатывается в этой локации. Используя директиву `root /data/www`, запрос сопоставляется с файлом `/data/www/about.html`, и файл отправляется клиенту.

Обработка запроса `/` более сложна. Он соответствует только префиксу `location /`, поэтому он обрабатывается в этой локации. Директива *index* затем проверяет наличие индексных файлов в соответствии с её параметрами и директивой `root /data/www`. Если файл `/data/www/index.html` не существует, но файл `/data/www/index.php` существует, директива выполняет внутреннюю переадресацию на `/index.php`, и Angie PRO снова ищет локации, как если бы запрос был отправлен клиентом. Как упоминалось ранее, переадресованный запрос в конечном итоге будет обработан сервером FastCGI.

Проксирование и балансировка нагрузки

Одним из распространенных способов использования Angie PRO является настройка в качестве прокси-сервера. В этой роли Angie PRO принимает запросы, перенаправляет их на проксируемые серверы, получает ответы от этих серверов и отправляет ответы обратно клиентам.

Простой прокси-сервер:

```
server {

    location / {

        proxy_pass http://backend:8080;
    }
```

Директива *proxy_pass* заставит Angie PRO передавать запросы клиентов на сервер `backend:8080` (прокси-сервер). Существует множество дополнительных *директив*, которые можно использовать для дальнейшей настройки прокси-соединения.

Проксирование FastCGI

Angie PRO может использоваться для маршрутизации запросов на FastCGI-серверы, которые выполняют приложения, построенные с использованием различных фреймворков и языков программирования, таких как PHP.

Простейшая конфигурация Angie PRO для работы с FastCGI-сервером включает использование директивы *fastcgi_pass* вместо директивы *proxy_pass*, а также директив *fastcgi_param* для установки параметров, передаваемых FastCGI-серверу. Предположим, что FastCGI-сервер доступен по адресу `localhost:9000`. В PHP параметр `SCRIPT_FILENAME` используется для определения имени скрипта, а параметр `QUERY_STRING` используется для передачи параметров запроса. Результирующая конфигурация будет следующей:

```
server {

    location / {

        fastcgi_pass localhost:9000;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_param QUERY_STRING $query_string;
    }
```

```
    location ~ \.(gif|jpg|png)$ {

        root /data/images;
    }
}
```

Эта конфигурация настраивает сервер, который направляет все запросы, кроме запросов к статическим изображениям, на проксируемый сервер, работающий на `localhost:9000` через протокол FastCGI.

Проксирование WebSocket

Для обновления соединения с HTTP/1.1 до WebSocket используется механизм *протокольного переключения <https://datatracker.ietf.org/doc/html/rfc2616#section-14.42>*, доступный в HTTP/1.1.

Однако есть тонкость: поскольку заголовок `Upgrade` является *заголовком перехода <https://datatracker.ietf.org/doc/html/rfc2616#section-13.5.1>*, он не передается от клиента к проксируемому серверу. При использовании прямого проксирования клиенты могут использовать метод CONNECT для обхода этой проблемы. Этот подход не работает при обратном проксировании, так как клиенты не осведомлены о каких-либо прокси-серверах, и требуется специальная обработка на прокси-сервере.

Angie PRO реализует специальный режим работы, который позволяет установить туннель между клиентом и проксируемым сервером, если проксируемый сервер возвращает ответ с кодом 101 (Switching Protocols), а клиент запрашивает переключение протокола через заголовок `Upgrade` в запросе.

Как уже упоминалось, заголовки перехода, включая `Upgrade` и `Connection`, не передаются от клиента к проксируемому серверу. Поэтому, чтобы проксируемый сервер был осведомлен о намерении клиента переключиться на протокол WebSocket, эти заголовки должны быть переданы явно:

```
location /chat/ {

    proxy_pass http://backend;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
}
```

Более сложный пример демонстрирует, как значение поля заголовка `Connection` в запросе к проксируемому серверу зависит от наличия поля `Upgrade` в заголовке запроса клиента:

```
http {

    map $http_upgrade $connection_upgrade {

        default upgrade;
        '' close;
    }

    server {

        ...

        location /chat/ {

            proxy_pass http://backend;
```

```
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection $connection_upgrade;
        }
    }
}
```

По умолчанию соединение будет закрыто, если проксируемый сервер не передает никаких данных в течение 60 секунд. Этот тайм-аут можно увеличить с помощью директивы *proxy_read_timeout*. В качестве альтернативы: на проксируемом сервере можно настроить периодическую отправку кадров WebSocket ping для сброса тайм-аута и проверки того, активно ли соединение.

Балансировка нагрузки

Балансировка нагрузки между несколькими экземплярами приложения — это широко используемая техника для оптимизации использования ресурсов, максимизации пропускной способности, уменьшения задержек и обеспечения отказоустойчивых конфигураций.

Angie PRO можно использовать в качестве высокоэффективного HTTP-балансировщика нагрузки для распределения трафика между несколькими серверами приложений, тем самым улучшая производительность, масштабируемость и надежность веб-приложений.

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

```
http {

    upstream myapp1 {

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

    server {

        listen 80;

        location / {

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

В приведенном примере три экземпляра одного и того же приложения работают на серверах с `srv1` по `srv3`. Когда метод балансировки нагрузки не настроен явно, по умолчанию используется круговой метод (round-robin). Другие поддерживаемые механизмы балансировки нагрузки включают: *weight*, *least_conn* и *ip_hash*. Реализация обратного прокси в Angie PRO также поддерживает встроенные (или пассивные) проверки состояния серверов. Эти проверки настраиваются с помощью директив *max_fails* и *fail_timeout* внутри блока *server* в контексте *upstream*.

Логирование

> **Примечание**
>
> В дополнение к перечисленным здесь опциям, вы также можете включить *отладочный лог*.

Syslog

Директивы *error_log* и *access_log* поддерживают логирование в `syslog`. Для настройки логирования в `syslog` используются следующие параметры:

`server=`*address*	Указывает адрес сервера `syslog`. Адрес может быть доменным именем или IP-адресом с необязательным портом, либо путем к UNIX-доменному сокету, указанным после префикса `"unix:"`. Если порт не указан, используется UDP-порт 514. Если доменное имя разрешается в несколько IP-адресов, используется первый разрешенный адрес.
`facility=`*string*	Устанавливает уровень для сообщений `syslog`, как определено в RFC 3164. Возможные уровни включают: `"kern"`, `"user"`, `"mail"`, `"daemon"`, `"auth"`, `"intern"`, `"lpr"`, `"news"`, `"uucp"`, `"clock"`, `"authpriv"`, `"ftp"`, `"ntp"`, `"audit"`, `"alert"`, `"cron"`, `"local0"`..`"local7"`. По умолчанию используется `"local7"`.
`severity=`*string*	Определяет уровень серьезности сообщений `syslog` для *access_log*, как указано в RFC 3164. Возможные значения те же, что и для второго параметра (уровень) директивы *error_log*. По умолчанию используется `"info"`. Серьезность сообщений об ошибках определяется Angie PRO, поэтому этот параметр игнорируется в директиве *error_log*.
`tag=`*string*	Устанавливает тег для сообщений `syslog`. По умолчанию используется тег `"angie"`.
`nohostname`	Отключает добавление поля `hostname` в заголовок сообщения `syslog`.

Пример конфигурации `syslog`:

```
error_log syslog:server=192.168.1.1 debug;

access_log syslog:server=unix:/var/log/angie.sock,nohostname;
access_log syslog:server=[2001:db8::1]:12345,facility=local7,tag=angie,severity=info␣
↪combined;
```

> **Примечание**
>
> Сообщения в `syslog` записываются не чаще раза в секунду, чтобы предотвратить переполнение.

3.2 Справочники и указатели

В этих сводных разделах представлены справочные сведения о встроенных модулях, примеры их настройки, а также поддерживаемые ими директивы и переменные.

3.2.1 Встроенные модули

В этом справочнике описаны собственные модули Angie PRO, даны примеры конфигурации, перечислены их директивы и параметры, а также встроенные переменные.

Основной модуль

Модуль предоставляет основную функциональность и директивы конфигурации, необходимые для базовой работы сервера, а также решает важные задачи, такие как управление рабочими процессами, настройка событийно-ориентированных моделей и обработка входящих соединений и запросов. Он включает ключевые директивы для настройки основного процесса, ведения журналов ошибок и контроля поведения сервера на низком уровне.

Пример конфигурации

```
user www www;
worker_processes 2;

error_log /var/log/error.log info;

events {

    use kqueue; worker_connections 2048;
}
```

Директивы

accept_mutex

Синтаксис	`accept_mutex on	off;`
По умолчанию	`accept_mutex off;`
Контекст	events

Когда `accept_mutex` включен, рабочие процессы будут принимать новые соединения поочередно. Иначе уведомления о новых соединениях получают все рабочие процессы, что может привести к неэффективному использованию системных ресурсов, если количество новых соединений невелико.

Примечание

Нет необходимости включать `accept_mutex` на системах, которые поддерживают флаг `EPOLLEXCLUSIVE`, или при использовании директивы *reuseport*.

accept_mutex_delay

Синтаксис	`accept_mutex_delay` *время*;
По умолчанию	`accept_mutex_delay 500ms;`
Контекст	events

Если *accept_mutex* включен, эта директива указывает максимальное время, в течение которого рабочий процесс ждет, чтобы продолжить принимать новые соединения, если другой рабочий процесс уже обрабатывает новые соединения.

daemon

Синтаксис	`daemon on | off;`
По умолчанию	`daemon on;`
Контекст	main

Определяет, будет ли Angie PRO запускаться в режиме демона. Используется в основном для разработки.

debug_connection

Синтаксис	`debug_connection` *адрес* | *CIDR* | unix:;
По умолчанию	—
Контекст	events

Включает отладочный лог для отдельных клиентских соединений. Для остальных соединений используется уровень лога, заданный директивой *error_log*. Указывать соединения можно по IPv4- или IPv6-адресу, сети или имени хоста. Используйте параметр `unix:`, чтобы включить отладочный лог для соединений через UNIX-сокеты.

```
events {

    debug_connection 127.0.0.1;
    debug_connection localhost;
    debug_connection 192.0.2.0/24;
    debug_connection ::1;
    debug_connection 2001:0db8::/32;
    debug_connection unix:;
    #  ...
}
```

Важно

Чтобы эта директива работала, в сборке Angie PRO должен быть включен *отладочный лог*.

debug_points

Синтаксис	`debug_points` abort | stop;
По умолчанию	—
Контекст	main

Эта директива используется для отладки.

В случае обнаружения внутренней ошибки, например, утечки сокетов в момент перезапуска рабочих процессов, включение `debug_points` либо создаст файл дампа памяти (`abort`), либо остановит процесс (`stop`) для анализа с помощью отладчика.

env

Синтаксис	`env` *переменная* [=*значение*];
По умолчанию	`env TZ;`
Контекст	main

По умолчанию Angie PRO удаляет все переменные окружения, унаследованные от родительского процесса, кроме переменной `TZ`. Эта директива позволяет сохранить часть унаследованных переменных, поменять их значения или создать новые переменные окружения.

Эти переменные затем:

- наследуются во время *обновления исполняемого файла на лету*;
- используются модулем *Perl*;
- доступны рабочими процессами.

Обратите внимание, что управление системными библиотеками таким образом может быть не всегда эффективным, поскольку библиотеки часто проверяют переменные только во время инициализации, которая происходит до срабатывания этой директивы. Переменная `TZ` всегда наследуется и доступна модулю *Perl*, если не задано явно иное поведение.

Пример:

```
env MALLOC_OPTIONS;
env PERL5LIB=/data/site/modules;
env OPENSSL_ALLOW_PROXY_CERTS=1;
```

Примечание

Переменная окружения `ANGIE` используется внутри Angie PRO и не должна задаваться напрямую пользователем.

error_log

Синтаксис	`error_log` *файл* [*уровень*];
По умолчанию	`error_log logs/error.log error;`
Контекст	main, http, mail, stream, server, location

Настраивает логирование, позволяя указывать несколько логов на одном уровне конфигурации. Если файл лога не указан явно на уровне конфигурации `main`, будет использоваться файл по умолчанию.

Первый параметр указывает файл для хранения лога. Специальное значение `stderr` задает стандартный поток ошибок. Для настройки логирования в *syslog* используйте префикс `"syslog:"`. Для логирования в *циклический буфер памяти* используйте префикс `"memory:"`, за которым следует размер буфера; обычно он используется для отладки.

Второй параметр задает уровень логирования одним из следующих значений: `debug`, `info`, `notice`, `warn`, `error`, `crit`, `alert` или `emerg`. Уровни перечислены в порядке возрастания серьезности. При задании уровня будут логироваться сообщения равного и более высокого уровня:

Настройка	Уровни записи
`debug`	`debug`, `info`, `notice`, `warn`, `error`, `crit`, `alert`, `emerg`
`info`	`info`, `notice`, `warn`, `error`, `crit`, `alert`, `emerg`
`notice`	`notice`, `warn`, `error`, `crit`, `alert`, `emerg`
`warn`	`warn`, `error`, `crit`, `alert`, `emerg`
`error`	`error`, `crit`, `alert`, `emerg`
`crit`	`crit`, `alert`, `emerg`
`alert`	`alert`, `emerg`
`emerg`	*emerg*

Если этот параметр не задан, по умолчанию используется уровень логирования `error`.

Важно

Чтобы эта директива работала, в сборке Angie PRO должен быть включен *отладочный лог*.

events

Синтаксис	`events { ... };`
По умолчанию	—
Контекст	main

Предоставляет контекст конфигурационного файла для директив, влияющих на обработку соединений.

include

Синтаксис	`include` *файл* | *маска*;
По умолчанию	—
Контекст	любой

Включает в конфигурацию другой файл или файлы, подходящие под заданную *маску*. Включаемые файлы должны содержать синтаксически верные директивы и блоки.

Пример:

```
include mime.types;
include vhosts/*.conf;
```

load_module

Синтаксис	`load_module` *файл*;
По умолчанию	—
Контекст	main

Загружает динамический модуль из указанного файла. Относительные пути задаются от параметра сборки `--prefix`, уточнить который можно так:

```
$ sudo angie -V
```

Пример:

```
load_module modules/ngx_mail_module.so;
```

lock_file

Синтаксис	`lock_file` *файл*;
По умолчанию	`lock_file logs/angie.lock;`
Контекст	main

Angie PRO использует механизм блокировок для реализации *accept_mutex* и сериализации доступа к разделяемой памяти. На большинстве систем блокировки управляются с помощью атомарных операций, что делает эту директиву ненужной. Однако на некоторых системах используется альтернативный механизм *lock file*. Эта директива устанавливает префикс для имен файлов блокировок.

master_process

Синтаксис	`master_process on	off;`
По умолчанию	`master_process on;`
Контекст	main

Определяет, будут ли запускаться рабочие процессы. Эта директива предназначена для разработчиков Angie PRO.

multi_accept

Синтаксис	`multi_accept on	off;`
По умолчанию	`multi_accept off;`
Контекст	events

`on`	Рабочий процесс будет принимать сразу все новые соединения.
`off`	Рабочий процесс будет принимать только одно новое соединение за раз.

Примечание

Директива игнорируется при использовании метода обработки соединений *kqueue*, так как он сам задает число новых соединений, ожидающих приема.

pcre_jit

Синтаксис	`pcre_jit on	off;`
По умолчанию	`pcre_jit off;`
Контекст	main

Разрешает или запрещает использование JIT-компиляции (PCRE JIT) для регулярных выражений, известных на момент парсинга конфигурации.

Использование PCRE JIT заметно ускоряет обработку регулярных выражений.

Важно

Для работы JIT необходима библиотека PCRE версии 8.20 или выше, собранная с параметром сборки `--enable-jit`. Если Angie PRO собирается с библиотекой PCRE (`--with-pcre=`), поддержка JIT включается с помощью параметра `--with-pcre-jit`.

pid

Синтаксис	`pid` *файл* | off;
По умолчанию	`pid logs/angie.pid;`
Контекст	main

Указывает *файл*, где будет храниться идентификатор главного процесса Angie PRO. Файл создается атомарно, что обеспечивает корректность его содержимого. Настройка `off` отключает создание этого файла.

Примечание

Если значение *file* изменяется при переконфигурации, но указывает на симлинк предыдущего PID-файла, файл не будет создан заново.

ssl_engine

Синтаксис	`ssl_engine` *устройство*;
По умолчанию	—
Контекст	main

Задает название аппаратного SSL-акселератора.

thread_pool

Синтаксис	`thread_pool` *имя* threads=*число* [max_queue=*число*];
По умолчанию	`thread_pool default threads=32 max_queue=65536;`
Контекст	main

Задает *имя* и параметры пула потоков, используемого для многопоточной обработки операций чтения и отправки файлов *без блокирования* рабочих процессов.

Параметр `threads` задает число потоков в пуле.

Если все потоки в пуле заняты выполнением заданий, новые задания ждут в очереди. Параметр `max_queue` ограничивает число заданий, ожидающих своего выполнения в очереди. По умолчанию в очереди может находиться до 65536 заданий. Если очередь переполнена, новые задания завершаются с ошибкой.

timer_resolution

Синтаксис	`timer_resolution` *интервал*;
По умолчанию	—
Контекст	main

Уменьшает разрешение таймеров времени в рабочих процессах, за счет чего уменьшается число системных вызовов `gettimeofday()`. По умолчанию `gettimeofday()` вызывается при каждом получении событий из ядра. При уменьшении разрешения функция вызывается только раз за указанный интервал.

Пример:

```
timer_resolution 100ms;
```

Внутренняя реализация интервала зависит от используемого метода:

- Фильтр `EVFILT_TIMER`, если используется *kqueue*.
- Функция `timer_create()`, если используется *eventport*.
- Функция `setitimer()`, в противном случае.

use

Синтаксис	`use` *метод*;
По умолчанию	—
Контекст	events

Задает *метод*, используемый для *обработки соединений*. Обычно нет необходимости задавать его явно, поскольку по умолчанию Angie PRO выбирает наиболее эффективный метод.

user

Синтаксис	`user` *пользователь* [*группа*];
По умолчанию	`user <параметр сборки --user> <параметр сборки --group>;`
Контекст	main

Задает пользователя и группу для рабочих процессов (см. также параметры сборки). Если задан только пользователь, для группы также задается указанное имя пользователя.

worker_aio_requests

Синтаксис	`worker_aio_requests` *число*;
По умолчанию	`worker_aio_requests 32;`
Контекст	events

При использовании *aio* с методом обработки соединений *epoll* задает максимум операций асинхронного ввода-вывода, ожидающих обработки, для одного рабочего процесса.

worker_connections

Синтаксис	`worker_connections` *число*;
По умолчанию	`worker_connections 512;`
Контекст	events

Задает максимум соединений, которые одновременно может открыть рабочий процесс.

Обратите внимание, что это число включает все соединения, такие как соединения с проксируемыми серверами, а не только клиентские. Кроме того, фактическое количество одновременных соединений не может превышать системный лимит на открытые файлы, который можно настроить с помощью *worker_rlimit_nofile*.

worker_cpu_affinity

Синтаксис	`worker_cpu_affinity` *маска_CPU* ...; `worker_cpu_affinity` auto [*маска_CPU*];
По умолчанию	—
Контекст	main

Привязывает рабочие процессы к группам процессоров. Каждая группа процессоров задается битовой маской разрешенных процессоров. Для каждого рабочего процесса должна быть задана отдельная группа. По умолчанию рабочие процессы не привязаны к конкретным процессорам.

Пример:

```
worker_processes    4;
worker_cpu_affinity 0001 0010 0100 1000;
```

Эта конфигурация привязывает каждый рабочий процесс к отдельному процессору.

В качестве альтернативы:

```
worker_processes    2;
worker_cpu_affinity 0101 1010;
```

Это привязывает первый рабочий процесс к CPU0 и CPU2, а второй рабочий процесс к CPU1 и CPU3. Такая настройка подходит для гипертредининга.

Специальное значение `auto` позволяет автоматически привязывать рабочие процессы к доступным процессорам:

```
worker_processes auto;
worker_cpu_affinity auto;
```

С помощью необязательной маски можно ограничить процессоры, доступные для автоматической привязки:

```
worker_cpu_affinity auto 01010101;
```

Важно

Директива доступна только на FreeBSD и Linux.

worker_priority

Синтаксис	`worker_priority` *число*;
По умолчанию	`worker_priority 0;`
Контекст	main

Задает приоритет планирования рабочих процессов подобно тому, как это делается командой `nice`: отрицательное *число* означает более высокий приоритет. Диапазон возможных значений — от -20 до 20.

Пример:

```
worker_priority -10;
```

worker_processes

Синтаксис	`worker_processes` *число* | auto;
По умолчанию	`worker_processes 1;`
Контекст	main

Задает число рабочих процессов.

Оптимальное значение зависит от разных факторов, включая число ядер процессора, количество жестких дисков и характер нагрузки. Если вы не уверены, рекомендуется начать с числа доступных ядер процессора. Значение `auto` пытается автоматически определить оптимальное количество.

worker_rlimit_core

Синтаксис	`worker_rlimit_core` *размер*;
По умолчанию	—
Контекст	main

Меняет ограничение на наибольший размер дампа памяти (`RLIMIT_CORE`) для рабочих процессов. Используется для увеличения ограничения без перезапуска главного процесса.

worker_rlimit_nofile

Синтаксис	`worker_rlimit_nofile` *число*;
По умолчанию	—
Контекст	main

Меняет ограничение на максимальное число открытых файлов (`RLIMIT_NOFILE`) для рабочих процессов. Используется для увеличения ограничения без перезапуска главного процесса.

worker_shutdown_timeout

Синтаксис	`worker_shutdown_timeout` *время*;
По умолчанию	—
Контекст	main

Задает таймаут в секундах для постепенного завершения рабочих процессов. По истечении указанного времени Angie PRO попытается закрыть все открытые сейчас соединения, чтобы ускорить завершение работы.

Постепенное завершение работы инициируется отправкой *сигнала QUIT* главному процессу, который приказывает рабочим процессам прекратить принимать новые подключения, позволяя завершить уже существующие. Рабочие процессы продолжают обрабатывать активные запросы до их завершения, после чего корректно завершают свою работу. Если соединения остаются открытыми дольше `worker_shutdown_timeout`, Angie PRO принудительно закроет эти соединения для завершения работы.

working_directory

Синтаксис	`working_directory` *каталог*;
По умолчанию	—
Контекст	main

Задает каталог, который будет текущим для рабочего процесса. Основное применение — запись дампа памяти, поэтому рабочий процесс должен иметь права на запись в этот каталог.

HTTP-модуль

Access

Модуль управляет доступом к ресурсам сервера на основе IP-адресов клиентов или сетей. Он позволяет разрешать или блокировать доступ для определенных IP-адресов, IP-диапазонов или UNIX-сокетов, чтобы повысить безопасность, ограничивая доступ к важным разделам веб-сайта или приложения.

Доступ также можно ограничить с помощью пароля, используя модуль *Auth Basic*, или на основе результата подзапроса, используя модуль *Auth Request*. Чтобы одновременно применять ограничения по адресу и паролю, используйте директиву *satisfy*.

Пример конфигурации

```
location / {

    deny 192.168.1.1;
    allow 192.168.1.0/24;
    allow 10.1.1.0/16;
    allow 2001:0db8::/32;
    deny all;
}
```

Правила обрабатываются последовательно до первого совпадения. В этом примере доступ разрешен только для IPv4-сетей `10.1.1.0/16` и `192.168.1.0/24`, за исключением отдельного адреса `192.168.1.1`, и для IPv6-сети `2001:0db8::/32`. Когда правил много, предпочтительно использовать переменные из модуля *Geo*.

Директивы

allow

Синтаксис	`allow` *адрес* | *CIDR* | `unix:` | `all`;
По умолчанию	—
Контекст	http, server, location, limit_except

Разрешает доступ для указанной сети или адреса. Специальное значение `all` означает все IP-адреса клиентов.

Добавлено в версии 1.5.1: Специальное значение `unix:` разрешает доступ для любых UNIX-сокетов.

deny

Синтаксис	`deny` *адрес* | *CIDR* | `unix:` | `all`;
По умолчанию	—
Контекст	http, server, location, limit_except

Запрещает доступ для указанной сети или адреса. Специальное значение `all` означает все IP-адреса клиентов.

Добавлено в версии 1.5.1: Специальное значение `unix:` запрещает доступ для любых UNIX-сокетов.

ACME

Обеспечивает автоматическое получение сертификатов с использованием протокола ACME.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_acme_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Шаги для включения запроса сертификатов в конфигурации:

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

2. **Укажите домены, для которых запрашиваются сертификаты**: для доменных имен, перечисленных во всех директивах *server_name* всех блоков `server` с директивами *acme*, указывающими на один и тот же клиент ACME, будет выдан единый сертификат.
3. **Обеспечьте прием вызовов ACME**, открыв порт 80; остальное сделает модуль. Сейчас Angie PRO поддерживает проверку доменных имен только по HTTP, что требует ответа на специальный запрос от удостоверяющего центра (CA); это так называемый вызов ACME.
4. **Настройте SSL с использованием полученного сертификата и ключа**: Модуль делает сертификаты и ключи доступными в виде *встроенных переменных*, которые можно использовать в *конфигурации* для заполнения *ssl_certificate* и *ssl_certificate_key*.

Детали реализации

Ключи и сертификаты клиентов хранятся в кодировке PEM в соответствующих подкаталогах каталога, заданного с помощью параметра сборки `--http-acme-client-path`:

```
$ ls /var/lib/angie/acme/example/

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

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

> **Примечание**
>
> Если у вас уже есть ключ учетной записи, поместите его в подкаталог клиента перед запуском для повторного использования учетной записи.

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

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

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

Пример конфигурации

Здесь клиент ACME с именем `example` управляет доменами `example.com` и `www.example.com`. Сертификат и его ключ доступны через префиксные переменные *$acme_cert_<name>* и *$acme_cert_key_<name>*. Они содержат соответствующие файлы, которые используются с *ssl_certificate* и *ssl_certificate_key*:

```
http {

    resolver 127.0.0.53; # требуется для директивы 'acme_client'

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

    server {

        listen               80;      # Может стоять в другом блоке 'server'
```

```
                                    # с другим списком доменов
                                    # или даже без него

        listen                443 ssl;

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

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

Как уже отмечалось, порт 80 должен быть открыт для приема вызовов ACME по HTTP. Однако, как указывает предыдущий пример, директива *listen* для этого порта может стоять в отдельном блоке *server*. Если существующего блока с такой директивой нет, можно ограничить новый блок одними только вызовами ACME:

```
server {
    listen 80;
    return 444; # Нет ответа, соединение закрыто
}
```

Почему это работает? Модуль перехватывает запросы к `/.well-known/acme-challenge/<TOKEN>` после чтения заголовков, но до выбора виртуального сервера и обработки директив *rewrite* и *location*. Такие перехваченные запросы обрабатываются, если значение `TOKEN` соответствует ожидаемому для конкретного вызова. Обращения к директории не будет; запрос полностью обрабатывается модулем.

Директивы

acme

Синтаксис	`acme` *имя*;
По умолчанию	—
Контекст	server

Для всех доменов, указанных в директивах *server_ name* во всех блоках *server*, которые ссылаются на *клиент ACME* с именем *имя*, будет получен единый сертификат; если изменится конфигурация `server_name`, сертификат будет обновлен для учета изменений.

> **Примечание**
>
> Сейчас домены со звездочкой и домены, заданные через регулярные выражения, не поддерживаются и будут пропущены.

Эта директива может быть указана несколько раз для загрузки сертификатов разных типов, например RSA и ECDSA:

```
server {

    listen 443 ssl;
    server_name example.com www.example.com;
```

```
    ssl_certificate $acme_cert_rsa;
    ssl_certificate_key $acme_cert_key_rsa;

    ssl_certificate $acme_cert_ecdsa;
    ssl_certificate_key $acme_cert_key_ecdsa;

    acme rsa;
    acme ecdsa;
}
```

acme_client

Синтаксис	`acme_client` *имя uri* [enabled=on|off] [key_type=*тип*] [key_bits=*число*] [email=*email*] [renew_before_expiry=*время*] [retry_after_error=off|*время*];
По умолчанию	—
Контекст	http

Определяет клиент ACME с глобально уникальным *именем*. Оно должно быть допустимым для каталога и будет использоваться без учета регистра.

Вторым обязательным параметром является *uri* каталога ACME. Например, URI каталога Let's Encrypt ACME указан как https://acme-v02.api.letsencrypt.org/directory.

Чтобы директива работала, в том же контексте должен быть настроен *resolver*.

Примечание

Для тестирования удостоверяющие центры обычно предоставляют отдельные тестовые среды. Например, среда тестирования Let's Encrypt — https://acme-staging-v02.api.letsencrypt.org/directory.

`enabled`	Включает или отключает клиент; это полезно, например, для временного отключения клиента без его удаления из конфигурации. По умолчанию: `on`.
`key_type`	Тип алгоритма закрытого ключа для сертификата. Допустимые значения: `rsa`, `ecdsa`. По умолчанию: `ecdsa`.
`key_bits`	Количество битов в ключе сертификата. По умолчанию: 256 для `ecdsa`, 2048 для `rsa`.
`email`	Необязательный адрес электронной почты для обратной связи; используется при создании учетной записи на сервере CA.
`renew_before_exp`	*Время* до истечения срока действия сертификата, когда должно начаться его обновление. По умолчанию: `30d`.
`retry_after_erro`	*Время* до повторной попытки, если получить сертификат не удалось. Если задано значение `off`, клиент не будет снова пытаться получить сертификат после ошибки. По умолчанию: `2h`.

acme_client_path

Синтаксис	`acme_client_path` *путь*;
По умолчанию	—
Контекст	http

Переопределяет *путь* к каталогу для хранения сертификатов и ключей, заданному при сборке с помощью параметра сборки `--http-acme-client-path`.

Встроенные переменные

`$acme_cert_<name>`

Содержимое последнего файла сертификата (если он есть), полученного клиентом с этим *именем*.

`$acme_cert_key_<name>`

Содержимое файла ключа сертификата, используемого клиентом с этим *именем*.

Важно

Файл сертификата доступен, только если клиент ACME получил хотя бы один сертификат, а вот файл ключа доступен сразу после запуска.

Addition

Фильтр, добавляющий текст до и после ответа.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_addition_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
location / {
    add_before_body /before_action;
    add_after_body  /after_action;
}
```

Директивы

add_before_body

Синтаксис	`add_before_body` uri;
По умолчанию	—
Контекст	http, server, location

Добавляет перед телом ответа текст, выдаваемый в результате работы заданного подзапроса. Пустая строка (`""`) в качестве параметра отменяет добавление, унаследованное с предыдущего уровня конфигурации.

add_after_body

Синтаксис	`add_after_body` uri;
По умолчанию	—
Контекст	http, server, location

Добавляет после тела ответа текст, выдаваемый в результате работы заданного подзапроса. Пустая строка (`""`) в качестве параметра отменяет добавление, унаследованное с предыдущего уровня конфигурации.

addition_types

Синтаксис	`addition_types` mime-*тип* ...;
По умолчанию	`addition_types text/html;`
Контекст	http, server, location

Разрешает добавлять текст в ответах с указанными MIME-типами в дополнение к `text/html`. Специальное значение `*` соответствует любому MIME-типу.

API

Модуль `API` реализует HTTP RESTful интерфейс для получения базовой информации о веб-сервере в формате JSON, а также *статистики* по клиентским соединениям, зонам разделяемой памяти, DNS-запросам, HTTP-запросам, кэшу HTTP-ответов, сессиям модуля *stream* и зонам модулей *limit_conn http*, *limit_conn stream*, *limit_req* и *http upstream*.

Интерфейс принимает HTTP-методы `GET` и `HEAD`; запрос с другим методом вызовет ошибку:

```
{
    "error": "MethodNotAllowed",
    "description": "The POST method is not allowed for the requested API element \"/\
↪"."
}
```

В Angie PRO в этом интерфейсе есть раздел *динамической конфигурации*, позволяющий менять настройки без перезагрузки конфигурации или перезапуска; сейчас доступна конфигурация отдельных серверов в составе *upstream*.

Директивы

api

Синтаксис	`api` *путь*;
По умолчанию	—
Контекст	location

Включает HTTP RESTful интерфейс в `location`.

Параметр *путь* является обязательным. Подобно директиве *alias*, задает путь для замены указанного в `location`, но по дереву API, а не файловой системы.

Если указан в префиксном `location`:

```
location /stats/ {
    api /status/http/server_zones/;
}
```

часть URI запроса, совпадающая с префиксом */stats/*, будет заменена на путь, указанный в параметре *путь*: */status/http/server_zones/*. К примеру, по запросу */stats/foo/* будет доступен элемент API `/status/http/server_zones/foo/`.

Допускается использование переменных: *api /status/$module/server_zones/$name/* и использование внутри regex location:

```
location ~^/api/([^/]+)/(.*)$ {
    api /status/http/$1_zones/$2;
}
```

Здесь параметр *путь* определяет полный путь к элементу API; так, из запроса к `/api/location/data/` будут выделены переменные:

```
$1 = "location"
$2 = "data/"
```

И конечный запрос будет иметь вид `/status/http/location_zones/data/`.

Примечание

В Angie PRO можно разделить *API динамической конфигурации* и неизменяемый *API статуса*, отражающий текущее состояние:

```
location /config/ {
    api /config/;
}

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

Также параметр *путь* позволяет управлять доступом к API:

```
location /status/ {
    api /status/;

    allow 127.0.0.1;
    deny  all;
}
```

Или же:

```
location /blog/requests/ {
    api /status/http/server_zones/blog/requests/;

    auth_basic           "blog";
    auth_basic_user_file conf/htpasswd;
}
```

api_config_files

Синтаксис	`api_config_files` on | off;
По умолчанию	off
Контекст	location

Включает или отключает добавление объекта `config_files`, перечисляющего содержимое всех файлов конфигурации Angie PRO, загруженных сейчас экземпляром сервера, в состав раздела API */status/angie/*. Например, при такой конфигурации:

```
location /status/ {
    api /status/;
    api_config_files on;
}
```

Запрос к `/status/angie/` возвращает приблизительно следующее:

```
{
    "version":"1.7.0",
    "address":"192.168.16.5",
    "generation":1,
    "load_time":"2024-09-19T12:58:39.789Z",
    "config_files": {
        "/etc/angie/angie.conf": "...",
        "/etc/angie/mime.types": "..."
    }
}
```

По умолчанию вывод отключен, так как файлы конфигурации могут содержать особо чувствительные, конфиденциальные сведения.

Метрики

Angie PRO публикует статистику использования в разделе API `/status/`; открыть доступ к ней можно, задав соответствующий `location`. Полный доступ:

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

Пример частичного доступа, уже приводившийся выше:

```
location /stats/ {
    api /status/http/server_zones/;
}
```

Пример конфигурации

С конфигурацией, включающей `location /status/`, зоны `resolver`, `http` в `upstream`, `http server`, `location`, `cache`, `limit_conn` в `http` и `limit_req`:

```
http {

    resolver 127.0.0.53 status_zone=resolver_zone;
    proxy_cache_path /var/cache/angie/cache keys_zone=cache_zone:2m;
    limit_conn_zone $binary_remote_addr zone=limit_conn_zone:10m;
    limit_req_zone $binary_remote_addr zone=limit_req_zone:10m rate=1r/s;

    upstream upstream {
        zone upstream 256k;
        server backend.example.com service=_example._tcp resolve max_conns=5;
       keepalive 4;
    }

    server {
        server_name www.example.com;
        listen 443 ssl;

        status_zone http_server_zone;
        proxy_cache cache_zone;

        access_log /var/log/access.log main;

        location / {
            root /usr/share/angie/html;
            status_zone location_zone;
            limit_conn limit_conn_zone 1;
            limit_req zone=limit_req_zone burst=5;
        }
        location /status/ {
            api /status/;

            allow 127.0.0.1;
            deny all;
        }

    }
}
```

В ответ на запрос `curl https://www.example.com/status/` Angie PRO возвращает:

дерево JSON


```
{
    "angie": {
        "version":"1.7.0",
        "address":"192.168.16.5",
        "generation":1,
        "load_time":"2024-09-19T12:58:39.789Z"
    },

    "connections": {
        "accepted":2257,
        "dropped":0,
        "active":3,
        "idle":1
    },

    "slabs": {
        "cache_zone": {
            "pages": {
                "used":2,
                "free":506
            },

            "slots": {
                "64": {
                    "used":1,
                    "free":63,
                    "reqs":1,
                    "fails":0
                },

                "512": {
                    "used":1,
                    "free":7,
                    "reqs":1,
                    "fails":0
                }
            }
        },

        "limit_conn_zone": {
            "pages": {
                "used":2,
                "free":2542
            },

            "slots": {
                "64": {
                    "used":1,
                    "free":63,
                    "reqs":74,
                    "fails":0
                },
```

```
                "128": {
                    "used":1,
                    "free":31,
                    "reqs":1,
                    "fails":0
                }
            }
        },

        "limit_req_zone": {
            "pages": {
                "used":2,
                "free":2542
            },

            "slots": {
                "64": {
                    "used":1,
                    "free":63,
                    "reqs":1,
                    "fails":0
                },

                "128": {
                    "used":2,
                    "free":30,
                    "reqs":3,
                    "fails":0
                }
            }
        }
    },

    "http": {
        "server_zones": {
            "http_server_zone": {
                "ssl": {
                    "handshaked":4174,
                    "reuses":0,
                    "timedout":0,
                    "failed":0
                },

                "requests": {
                    "total":4327,
                    "processing":0,
                    "discarded":8
                },

                "responses": {
                    "200":4305,
                    "302":12,
                    "404":4
                },

                "data": {
                    "received":733955,
```

```
                "sent":59207757
            }
        }
    },

    "location_zones": {
        "location_zone": {
            "requests": {
                "total":4158,
                "discarded":0
            },

            "responses": {
                "200":4157,
                "304":1
            },

            "data": {
                "received":538200,
                "sent":177606236
            }
        }
    },
    "caches": {
        "cache_zone": {
            "size":0,
            "cold":false,
            "hit": {
                "responses":0,
                "bytes":0
            },

            "stale": {
                "responses":0,
                "bytes":0
            },

            "updating": {
                "responses":0,
                "bytes":0
            },

            "revalidated": {
                "responses":0,
                "bytes":0
            },

            "miss": {
                "responses":0,
                "bytes":0,
                "responses_written":0,
                "bytes_written":0
            },

            "expired": {
                "responses":0,
                "bytes":0,
```

```
                "responses_written":0,
                "bytes_written":0
            },

            "bypass": {
                "responses":0,
                "bytes":0,
                "responses_written":0,
                "bytes_written":0
            }
        }
    },

    "limit_conns": {
        "limit_conn_zone": {
            "passed":73,
            "skipped":0,
            "rejected":0,
            "exhausted":0
        }
    },

    "limit_reqs": {
        "limit_req_zone": {
            "passed":54816,
            "skipped":0,
            "delayed":65,
            "rejected":26,
            "exhausted":0
        }
    },

    "upstreams": {
        "upstream": {
            "peers": {
                "192.168.16.4:80": {
                    "server":"backend.example.com",
                    "service":"_example._tcp",
                    "backup":false,
                    "weight":5,
                    "state":"up",
                    "selected": {
                        "current":2,
                        "total":232
                    },

                    "max_conns":5,
                    "responses": {
                        "200":222,
                        "302":12
                    },

                    "data": {
                        "sent":543866,
                        "received":27349934
                    },
```

```
                        "health": {
                            "fails":0,
                            "unavailable":0,
                            "downtime":0
                        },

                        "sid":"<server_id>"
                    }
                },

                "keepalive":2
            }
        }
    },

    "resolvers": {
        "resolver_zone": {
            "queries": {
                "name":442,
                "srv":2,
                "addr":0
            },

            "responses": {
                "success":440,
                "timedout":1,
                "format_error":0,
                "server_failure":1,
                "not_found":1,
                "unimplemented":0,
                "refused":1,
                "other":0
            }
        }
    }
}
```

Набор метрик можно запросить по отдельной ветви JSON, построив соответствующий запрос. Например:

```
$ curl https://www.example.com/status/angie
$ curl https://www.example.com/status/connections
$ curl https://www.example.com/status/slabs
$ curl https://www.example.com/status/slabs/<zone>/slots
$ curl https://www.example.com/status/slabs/<zone>/slots/64
$ curl https://www.example.com/status/http/
$ curl https://www.example.com/status/http/server_zones
$ curl https://www.example.com/status/http/server_zones/<http_server_zone>
$ curl https://www.example.com/status/http/server_zones/<http_server_zone>/ssl
```

Примечание

По умолчанию модуль использует для дат строки в формате ISO 8601; чтобы вместо этого использовать целочисленный формат эпохи UNIX, добавьте параметр `date=epoch` к строке запроса:

```
$ curl https://www.example.com/status/angie/load_time
```

```
  "2024-04-01T00:59:59+01:00"

$ curl https://www.example.com/status/angie/load_time?date=epoch

  1711929599
```

Состояние сервера

`/status/angie`

```
{
    "version": "1.7.0",
    "address": "192.168.16.5",
    "generation": 1,
    "load_time": "2024-09-19T16:15:43.805Z"
    "config_files": {
        "/etc/angie/angie.conf": "...",
        "/etc/angie/mime.types": "..."
    }
}
```

`version`	Строка; версия запущенного сервера Angie PRO
`build` (PRO)	Строка; сборка, если указана при компиляции
`address`	Строка; адрес сервера, принявшего запрос к API
`generation`	Число; версия (поколение) конфигурации, отсчитываемая с последнего запуска Angie PRO
`load_time`	Строка; время последней перезагрузки конфигурации в формате *даты*; строковые значения даются с миллисекундным разрешением
`config_files`	Объект; его члены — абсолютные имена всех файлов конфигурации Angie PRO, загруженных сейчас экземпляром сервера, а их значения — строковые представления содержимого файлов, например: `{ "/etc/angie/angie.conf": "server {\n  listen 80;\n  # ...\n\n}\n" }` **Осторожно** Объект `config_files` есть в `/status/angie/`, только если включена директива *api_ config_ files*.

Соединения

`/status/connections`

```
{
  "accepted": 2257,
  "dropped": 0,
  "active": 3,
  "idle": 1
}
```

`accepted`	Число; суммарное количество принятых клиентских соединений
`dropped`	Число; суммарное количество сброшенных клиентских соединений
`active`	Число; текущее количество активных клиентских соединений
`idle`	Число; текущее количество бездействующих клиентских соединений

Зоны разделяемой памяти с распределением slab

`/status/slabs/<zone>`

Статистика для зон разделяемой памяти с распределением slab, таких как *limit_ conn*, *limit_ req* и *HTTP cache*:

```
limit_conn_zone $binary_remote_addr zone=limit_conn_zone:10m;
limit_req_zone $binary_remote_addr zone=limit_req_zone:10m rate=1r/s;
proxy_cache cache_zone;
```

В указанной таким образом зоне разделяемой памяти будет собираться следующая статистика:

`pages`	Объект; статистика по страницам памяти
`used`	Число; текущее количество используемых страниц памяти
`free`	Число; текущее количество свободных страниц памяти
`slots`	Объект; статистика по слотам памяти, по каждому из размеров. `slots` содержит данные по размеру слота памяти (`8`, `16`, `32`, и т.д., вплоть до половины размера страницы памяти в байтах)
`used`	Число; текущее количество используемых слотов памяти заданного размера
`free`	Число; текущее количество свободных слотов памяти заданного размера
`reqs`	Число; суммарное количество попыток выделения памяти указанного размера
`fails`	Число; количество неудавшихся попыток выделения памяти указанного размера

Пример:

```
{
  "pages": {
    "used": 2,
    "free": 506
  },

  "slots": {
    "64": {
```

```
      "used": 1,
      "free": 63,
      "reqs": 1,
      "fails": 0
  }
}
```

DNS-запросы к резолверу

`/status/resolvers/<zone>`

Для сбора статистики в директиве *resolver* нужно задать параметр `status_zone` (*HTTP* или *Stream*):

```
resolver 127.0.0.53 status_zone=resolver_zone;
```

В указанной таким образом зоне разделяемой памяти будет собираться следующая статистика:

`queries`	Объект; статистика запросов
`name`	Число; количество запросов на преобразование имен в адреса (A- и AAAA-запросы)
`srv`	Число; количество запросов на преобразование сервисов в адреса (SRV запросы)
`addr`	Число; количество запросов на преобразование адресов в имена (PTR-запросы)
`responses`	Объект; статистика ответов
`success`	Число; количество успешных ответов
`timedout`	Число; количество запросов, не дождавшихся ответа
`format_error`	Число; количество ответов с кодом 1 (Format Error)
`server_failure`	Число; количество ответов с кодом 2 (Server Failure)
`not_found`	Число; количество ответов с кодом 3 (Name Error)
`unimplemented`	Число; количество ответов с кодом 4 (Not Implemented)
`refused`	Число; количество ответов с кодом 5 (Refused)
`other`	Число; количество запросов, завершенных с другим ненулевым кодом
`sent`	Объект; статистика отправленных DNS-запросов
`a`	Число; количество запросов типа A
`aaaa`	Число; количество запросов типа AAAA
`ptr`	Число; количество запросов типа PTR
`srv`	Число; количество запросов типа SRV

Коды ответов описаны в RFC 1035, часть 4.1.1.

Различные типы DNS-записей описаны в RFC 1035, RFC 2782 и RFC 3596.

Пример:

```
{
  "queries": {
    "name": 442,
    "srv": 2,
    "addr": 0
  },

  "responses": {
    "success": 440,
    "timedout": 1,
```

```
    "format_error": 0,
    "server_failure": 1,
    "not_found": 1,
    "unimplemented": 0,
    "refused": 1,
  },

  "sent": {
    "a": 185,
    "aaaa": 245,
    "srv": 2,
    "ptr": 12
  }
}
```


HTTP server и location

`/status/http/server_zones/<zone>`

Для сбора статистики в контексте *server* нужно задать директиву *status_ zone*:

```
server {
    ...
    status_zone server_zone;
}
```

В указанной таким образом зоне разделяемой памяти будет собираться следующая статистика:

`ssl`	Объект; SSL-метрики. Присутствует, если в `server` есть `listen ssl;`
`handshaked`	Число; суммарное количество успешных SSL-рукопожатий
`reuses`	Число; суммарное количество повторных использований SSL-сессий во время SSL-рукопожатий
`timedout`	Число; суммарное количество SSL-рукопожатий с истекшим таймаутом
`failed`	Число; суммарное количество неуспешных SSL-рукопожатий
`requests`	Объект; метрики запросов
`total`	Число; суммарное количество клиентских запросов
`processing`	Число; текущее количество обслуживаемых клиентских запросов
`discarded`	Число; суммарное количество запросов завершенных без отправки ответа
`responses`	Объект; метрики ответов
`<code>`	Число; ненулевое количество ответов со статусом <code> (100-599)
`xxx`	Число; ненулевое количество ответов с другим кодом статуса
`data`	Объект; метрики данных
`received`	Число; суммарное количество байт, полученное от клиентов
`sent`	Число; суммарное количество байт, отправленное клиентам

Пример:


```
"ssl": {
  "handshaked": 4174,
  "reuses": 0,
  "timedout": 0,
  "failed": 0
},
```

```
"requests": {
  "total": 4327,
  "processing": 0,
  "discarded": 0
},

"responses": {
  "200": 4305,
  "302": 6,
  "304": 12,
  "404": 4
},

"data": {
  "received": 733955,
  "sent": 59207757
}
```

`/status/http/location_zones/<zone>`

Для сбора статистики в контексте *location* или *if в location* нужно задать директиву *status_zone*:

```
location / {
    root /usr/share/angie/html;
    status_zone location_zone;

    if ($request_uri ~* "^/condition") {
        # ...
        status_zone if_location_zone;
    }
}
```

В указанной таким образом зоне разделяемой памяти будет собираться следующая статистика:

`requests`	Объект; метрики запросов
`total`	Число; суммарное количество клиентских запросов
`discarded`	Число; суммарное количество запросов завершенных без отправки ответа
`responses`	Объект; метрики ответов
`<code>`	Число; ненулевое количество ответов со статусом <code> (100-599)
`xxx`	Число; ненулевое количество ответов с другим кодом статуса
`data`	Объект; метрики данных
`received`	Число; суммарное количество байт, полученное от клиентов
`sent`	Число; суммарное количество байт, отправленное клиентам

Пример:

```
{
  "requests": {
    "total": 4158,
    "discarded": 0
  },

  "responses": {
    "200": 4157,
```

```
    "304": 1
  },

  "data": {
    "received": 538200,
    "sent": 177606236
  }
}
```


Stream server

`/status/stream/server_zones/<zone>`

Для сбора статистики в контексте *server* нужно задать директиву *status_ zone*:

```
server {
    ...
    status_zone server_zone;
}
```

В указанной таким образом зоне разделяемой памяти будет собираться следующая статистика:

`ssl`	Объект; SSL-метрики. Присутствует, если в `server` есть `listen ssl;`
`handshaked`	Число; суммарное количество успешных SSL-рукопожатий
`reuses`	Число; суммарное количество повторных использований SSL-сессий во время SSL-рукопожатий
`timedout`	Число; суммарное количество SSL-рукопожатий с истекшим таймаутом
`failed`	Число; суммарное количество неуспешных SSL-рукопожатий
`connections`	Объект; метрики соединений
`total`	Число; суммарное количество клиентских соединений
`processing`	Число; текущее количество обслуживаемых клиентских соединений
`discarded`	Число; суммарное количество клиентских соединений, завершенных без создания сессии
`passed`	Число; суммарное количество клиентских соединений, переданных на другой прослушивающий порт директивами `pass`
`sessions`	Объект; метрики сессий
`success`	Число; количество сессий, завершенных с кодом 200, что означает успешное завершение
`invalid`	Число; количество сессий, завершенных с кодом 400, случается, когда сервер не может прочитать данные от клиента, например, заголовок PROXY protocol
`forbidden`	Число; количество сессий, завершенных с кодом 403, когда доступ запрещен, например, ограничен для определенного адреса клиента
`internal_error`	Число; количество сессий, завершенных с кодом 500, внутренняя ошибка сервера
`bad_gateway`	Число; количество сессий, завершенных с кодом 502, Bad Gateway, если, например, сервер в upstream недоступен или не может быть выбран
`service_unavailable`	Число; количество сессий, завершенных с кодом 503, Service Unavailable, если, например, доступ ограничен числом входящих соединений
`data`	Объект; метрики данных
`received`	Число; суммарное количество байт, полученное от клиентов
`sent`	Число; суммарное количество байт, отправленное клиентам

Пример:

```
{
  "ssl": {
    "handshaked": 24,
    "reuses": 0,
    "timedout": 0,
    "failed": 0
  },

  "connections": {
    "total": 24,
    "processing": 1,
    "discarded": 0,
    "passed": 2
  },

  "sessions": {
    "success": 24,
    "invalid": 0,
    "forbidden": 0,
    "internal_error": 0,
    "bad_gateway": 0,
    "service_unavailable": 0
  },

  "data": {
    "received": 2762947,
    "sent": 53495723
  }
}
```


HTTP caches

```
proxy_cache cache_zone;
```

`/status/http/caches/<cache>`

Для каждой зоны, сконфигурированной в *proxy_ cache*, хранятся следующие данные:


```
{
  "name_zone": {
    "size": 0,
    "cold": false,
    "hit": {
      "responses": 0,
      "bytes": 0
    },

    "stale": {
      "responses": 0,
      "bytes": 0
    },

    "updating": {
      "responses": 0,
```

```
      "bytes": 0
    },

    "revalidated": {
      "responses": 0,
      "bytes": 0
    },

    "miss": {
      "responses": 0,
      "bytes": 0,
      "responses_written": 0,
      "bytes_written": 0
    },

    "expired": {
      "responses": 0,
      "bytes": 0,
      "responses_written": 0,
      "bytes_written": 0
    },

    "bypass": {
      "responses": 0,
      "bytes": 0,
      "responses_written": 0,
      "bytes_written": 0
    }
  }
}
```

`size`	Число; текущий размер кэша
`max_size`	Число; ограничение на максимальный размер кэша, если задано в конфигурации
`cold`	Логическое значение; `true`, пока *загрузчик кэша* подгружает данные с диска
`hit`	Объект; метрики возвращенных из кэша ответов (*proxy_cache_valid*)
`responses`	Число; суммарное количество ответов, прочитанных из кэша
`bytes`	Число; суммарное количество байт, прочитанных из кэша
`stale`	Объект; метрики просроченных ответов, возвращенных из кэша (*proxy_cache_use_stale*)
`responses`	Число; суммарное количество ответов, прочитанных из кэша
`bytes`	Число; суммарное количество байт, прочитанных из кэша
`updating`	Объект; метрики просроченных ответов, возвращенных из кэша, пока данные в кэше обновляются (*proxy_cache_use_stale* updating)
`responses`	Число; суммарное количество ответов, прочитанных из кэша
`bytes`	Число; суммарное количество байт, прочитанных из кэша
`revalidated`	Объект; метрики просроченных и ревалидированных ответов, возвращенных из кэша (*proxy_cache_revalidate*)
`responses`	Число; суммарное количество ответов, прочитанных из кэша
`bytes`	Число; суммарное количество байт, прочитанных из кэша
`miss`	Объект; метрики ответов, не найденных в кэше
`responses`	Число; суммарное количество соответствующих ответов
`bytes`	Число; суммарное количество байт, прочитанных с проксируемого сервера
`responses_written`	Число; суммарное количество ответов, записанных в кэш
`bytes_written`	Число; суммарное количество байт, записанных в кэш
`expired`	Объект; количество ответов, возвращенных не из кэша, т.к. просрочены
`responses`	Число; суммарное количество соответствующих ответов
`bytes`	Число; суммарное количество байт, прочитанных с проксируемого сервера
`responses_written`	Число; суммарное количество ответов, записанных в кэш
`bytes_written`	Число; суммарное количество байт, записанных в кэш
`bypass`	Объект; статистика ответов, возвращенных в обход кэша (*proxy_cache_bypass*)
`responses`	Число; суммарное количество соответствующих ответов
`bytes`	Число; суммарное количество байт, прочитанных с проксируемого сервера
`responses_written`	Число; суммарное количество ответов, записанных в кэш
`bytes_written`	Число; суммарное количество байт, записанных в кэш

Добавлено в версии 1.2.0: PRO

В Angie PRO при включении *шардинга кэша* с помощью директив *proxy_cache_path* отдельные шарды указываются как объекты-члены в объекте `shards`:

`shards`	Объект; его члены — отдельные шарды
`<shard>`	Объект; представляет отдельный шард, а имя объекта — путь кэша
`sizes`	Число; текущий размер шарда
`max_size`	Число; максимальный размер шарда, если задан в конфигурации
`cold`	Логическое значение; `true`, пока *загрузчик кэша* подгружает данные с диска

```
{
  "name_zone": {
    "shards": {
        "/path/to/shard1": {
```

```
            "size": 0,
            "cold": false
        },

        "/path/to/shard2": {
            "size": 0,
            "cold": false
        }
    }
}
```

limit_conn

```
limit_conn_zone $binary_remote_addr zone=limit_conn_zone:10m;
```

`/status/http/limit_conns/<zone>`, `/status/stream/limit_conns/<zone>`

Каждая из сконфигурированных зон: *limit_conn в http* или *limit_conn в stream* содержит следующие данные

```
{
  "passed": 73,
  "skipped": 0,
  "rejected": 0,
  "exhausted": 0
}
```

passed	Число; суммарное количество переданных на проксируемый сервер соединений
skipped	Число; суммарное количество соединений, переданных с нулевым или превосходящим 255 байт <key>
rejected	Число; суммарное количество соединений сверх сконфигурированного ограничения
exhausted	Число; суммарное количество соединений, сброшенных из-за переполнения хранилища зоны

limit_req

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

`/status/http/limit_reqs/<zone>`

Каждая из сконфигурированных зон *limit_req* содержит следующие данные

```
{
  "passed": 54816,
  "skipped": 0,
  "delayed": 65,
  "rejected": 26,
  "exhausted": 0
}
```

`passed`	Число; суммарное количество проксированых соединений
`skipped`	Число; суммарное количество соединений, переданных с нулевым или превосходящим 255 байт <key>
`delayed`	Число; суммарное количество задержанных соединений
`rejected`	Число; суммарное количество сброшенных соединений
`exhausted`	Число; суммарное количество соединений, сброшенных из-за переполнения хранилища зоны

HTTP upstream

Добавлено в версии 1.1.0.

Чтобы включить сбор следующих метрик, задайте директиву *zone* в контексте *upstream*, например:

```
upstream upstream {
    zone upstream 256k;
    server backend.example.com service=_example._tcp resolve max_conns=5;
    keepalive 4;
}
```

`/status/http/upstreams/<upstream>`

где <*upstream*> — имя *апстрима*, в конфигурации которого указана директива *zone*.

```
{
    "peers": {
        "192.168.16.4:80": {
            "server": "backend.example.com",
            "service": "_example._tcp",
            "backup": false,
            "weight": 5,
            "state": "up",
            "selected": {
                "current": 2,
                "total": 232
            },

            "max_conns": 5,
            "responses": {
                "200": 222,
                "302": 12
            },

            "data": {
                "sent": 543866,
                "received": 27349934
            },

            "health": {
                "fails": 0,
                "unavailable": 0,
                "downtime": 0
            },
```

```
            "sid": "<server_id>"
        }
    },

    "keepalive": 2
}
```

`peers`	Объект; содержит метрики всех пиров апстрима во вложенных объектах, имена которых — канонические представления адресов этих пиров. Внутри каждого вложенного объекта:
`server`	Строка; сервер, как он указан в директиве *server*
`service`	Строка; имя сервиса, указанное в директиве *server*, если сконфигурировано
`slow_start` (PRO 1.4.0+)	Число; заданное для сервера значение *slow_start*, выраженное в секундах. При задании значения через *соответствующий подраздел* API динамической конфигурации можно указать не только число секунд, но и *время* с точностью до миллисекунд.
`backup`	Логическое значение; `true` для backup серверов
`weight`	Число; сконфигурированный *weight*
`state`	Строка; текущее состояние пира, и какие запросы ему отправляются: • `checking` (PRO): настроен как `essential` и проверяется, отправляются только *проверочные запросы*; • `down`: отключен вручную, не отправляются никакие запросы; • `draining` (PRO): аналогичен `down`, но отправляются запросы сессий, привязанных ранее через *sticky*; • `recovering`: восстанавливается после сбоя согласно *slow_start*, отправляется все больше запросов; • `unavailable`: достиг предела *max_fails*, отправляются пробные клиентские запросы с интервалом *fail_timeout*; • `unhealthy` (PRO): неработающий, отправляются только *проверочные запросы*; • `up`: работоспособен, запросы отправляются как обычно.
`selected`	Объект; статистика выбора пиров
`current`	Число; текущее количество соединений к пиру
`total`	Число; общее количество запросов переданных пиру
`last`	Строка или число; время последнего выбора пира в формате *даты*
`max_conns`	Число; *максимальное* количество одновременных активных соединений к пиру, если сконфигурировано
`responses`	Объект; статистика ответов
`<code>`	Число; ненулевое количество ответов со статусом <code> (100-599)
`xxx`	Число; ненулевое количество ответов с другим кодом статуса
`data`	Объект; метрики данных
`received`	Число; суммарное количество байт, полученное от пира
`sent`	Число; суммарное количество байт, отправленное пиру
`health`	Объект; статистика по состоянию пира
`fails`	Число; общее количество неудачных попыток работы с пиром
`unavailable`	Число; столько раз пир становился `unavailable` по достижении значения *max_fails*
`downtime`	Число; суммарное время (в миллисекундах), в течение которого пир был недоступен для выбора как `unavailable`
`downstart`	Строка или число; время, когда пир стал `unavailable`, в формате *даты*
`header_time` (PRO 1.3.0+)	Число; среднее время (в миллисекундах) получения заголовков ответа от сервера; см. директиву *response_time_factor (PRO)*
`response_time` (PRO 1.3.0+)	Число; среднее время (в миллисекундах) получения ответа от сервера; см. директиву *response_time_factor (PRO)*
`sid`	Строка; *id сервера*, указанный в конфигурации апстрима
`keepalive`	Число; текущее количество кэшированных соединений

`health/probes` (PRO)

Изменено в версии 1.2.0: PRO

Если для апстрима настроены проверки *upstream_probe (PRO)*, то в объекте `health` также есть вложенный объект `probes`, содержащий счетчики проверок работоспособности сервера, а `state`, помимо значений из таблицы выше, может принимать значения `checking` и `unhealthy`:

```
{
    "192.168.16.4:80": {
        "state": "unhealthy",
        "...": "...",
        "health": {
            "...": "...",
            "probes": {
                "count": 10,
                "fails": 10,
                "last": "2024-09-19T09:56:07Z"
            }
        }
    }
}
```

Значение `checking` у `state` не учитывается в `downtime` и означает, что сервер, проверка которого настроена с параметром `essential`, еще не проверялся; значение `unhealthy` — что сервер неработающий. Оба эти состояния также означают, что сервер не участвует в балансировке. Детали проверок см. в описании *upstream_probe*.

Счетчики в `probes`:

`count`	Число; общее количество проверок этого сервера
`fails`	Число; количество неуспешных проверок
`last`	Строка или число; время последней проверки в формате *даты*

`queue` (PRO)

Изменено в версии 1.4.0: PRO

Если для апстрима настроена *очередь запросов*, то в объекте апстрима также есть вложенный объект `queue`, содержащий счетчики запросов в очереди:

```
{
    "queue": {
        "queued": 20112,
        "waiting": 1011,
        "dropped": 6031,
        "timedout": 560,
        "overflows": 13
    }
}
```

Значения счетчиков суммируются по всем рабочим процессам:

`queued`	Число; общее количество запросов, попавших в очередь
`waiting`	Число; текущее количество запросов в очереди
`dropped`	Число; общее количество запросов, удаленных из очереди из-за того, что клиент преждевременно закрыл соединение
`timedout`	Число; общее количество запросов, удаленных из очереди по таймауту
`overflows`	Число; общее количество случаев переполнения очереди

Stream upstream

Чтобы включить сбор следующих метрик, задайте директиву *zone* в контексте *upstream*, например:

```
upstream upstream {
    zone upstream 256k;
    server backend.example.com service=_example._tcp resolve max_conns=5;
    keepalive 4;
}
```

`/status/stream/upstreams/<upstream>`

Здесь *<upstream>* — имя *апстрима*, в конфигурации которого использована директива *zone*.

```
{
    "peers": {
        "192.168.16.4:1935": {
            "server": "backend.example.com",
            "service": "_example._tcp",
            "backup": false,
            "weight": 5,
            "state": "up",
            "selected": {
                "current": 2,
                "total": 232
            },

            "max_conns": 5,
            "data": {
                "sent": 543866,
                "received": 27349934
            },

            "health": {
                "fails": 0,
                "unavailable": 0,
                "downtime": 0
            }
        }
    }
}
```

`peers`	Объект; содержит метрики всех пиров апстрима во вложенных объектах, имена которых — канонические представления адресов этих пиров. Внутри каждого вложенного объекта:
`server`	Строка; адрес, заданный директивой *server*
`service`	Строка; имя сервиса, если оно указано в директиве *server*
`slow_start` (PRO 1.4.0+)	Число; заданное для сервера значение *slow_start*, выраженное в секундах. При задании значения через *соответствующий подраздел* API динамической конфигурации можно указать не только число секунд, но и *время* с точностью до миллисекунд.
`backup`	Логическое значение; `true` для запасных серверов
`weight`	Число; заданный для пира *вес*
`state`	Строка; текущее состояние пира: • `up`: работоспособен, запросы отправляются как обычно; • `down`: отключен вручную, не отправляются никакие запросы; • `draining` (PRO): аналогичен `down`, но отправляются запросы сессий, привязанных ранее через *sticky*; • `unavailable`: достиг предела *max_fails*, отправляются пробные клиентские запросы с интервалом *fail_timeout*; • `recovering`: восстанавливается после сбоя согласно *slow_start*, отправляется все больше запросов; • `checking` (PRO): настроен как `essential` и проверяется, отправляются только *проверочные запросы*; • `unhealthy` (PRO): неработающий, отправляются только *проверочные запросы*.
`selected`	Объект; статистика выбора этого пира для подключения
`current`	Число; текущее количество подключений к пиру
`total`	Число; общее количество подключений, направленных этому пиру
`last`	Строка или число; время, когда пир был выбран в последний раз, в формате *даты*
`max_conns`	Число; *максимальное* количество одновременных активных подключений к пиру, если оно задано
`data`	Объект; статистика передачи данных
`received`	Число; общее количество байт, полученное от пира
`sent`	Число; общее количество байт, отправленное пиру
`health`	Объект; статистика по состоянию пира
`fails`	Число; общее количество неудачных попыток связаться с пиром
`unavailable`	Число; общее количество переходов в состояние `unavailable` по достижении значения *max_fails*
`downtime`	Число; общее время в миллисекундах, в течение которого пир находился в состоянии `unavailable` (недоступен для выбора)
`downstart`	Строка или число; время, когда пир последний раз стал `unavailable`, в формате *даты*
`connect_time` (PRO 1.4.0+)	Число; среднее время (в миллисекундах) установления соединения с сервером; см. директиву *response_time_factor (PRO)*
`first_byte_time` (PRO 1.4.0+)	Число; среднее время (в миллисекундах) получения первого байта ответа от сервера; см. директиву *response_time_factor (PRO)*
`last_byte_time` (PRO 1.4.0+)	Число; среднее время (в миллисекундах) получения полного ответа от сервера; см. директиву *response_time_factor (PRO)*

Изменено в версии 1.4.0: PRO

Если в Angie PRO для апстрима настроены проверки *upstream_probe (PRO)*, то в объекте `health` также есть вложенный объект `probes`, содержащий счетчики проверок работоспособности сервера, а `state`, помимо значений из таблицы выше, может принимать значения `checking` и `unhealthy`:

```
{
    "192.168.16.4:80": {
        "state": "unhealthy",
        "...": "...",
        "health": {
            "...": "...",
            "probes": {
                "count": 2,
                "fails": 2,
                "last": "2024-09-19T11:03:54Z"
            }
        }
    }
}
```

Значение `checking` у `state` означает, что сервер, проверка которого настроена с параметром `essential`, еще не проверялся; значение `unhealthy` — что сервер неработающий. Оба эти состояния также означают, что сервер не участвует в балансировке. Детали проверок см. в описании *upstream_probe*.

Счетчики в `probes`:

`count`	Число; общее количество проверок этого сервера
`fails`	Число; количество неуспешных проверок
`last`	Строка или число; время последней проверки в формате *даты*

API динамической конфигурации (PRO)

Добавлено в версии 1.2.0: PRO

В составе API есть раздел `/config`, позволяющий динамически менять конфигурацию Angie PRO в формате JSON с помощью HTTP-запросов `PUT`, `PATCH` и `DELETE`. Все изменения атомарны: новые настройки применяются целиком либо не применяются вовсе. При ошибке Angie PRO сообщит, в чем причина.

Подразделы `/config`

Сейчас в разделе `/config` доступна настройка отдельных серверов в составе апстримов для модулей *HTTP* и *stream*; число настроек, к которым применима динамическая конфигурация, планомерно увеличивается.

`/config/http/upstreams/<upstream>/servers/<name>`

Позволяет настраивать отдельные серверы в составе апстрима, в том числе добавлять новые и удалять настроенные.

Параметры в составе пути URI:

`<upstream>`	Имя блока `upstream`; чтобы настраивать его через `/config`, в нем должна быть задана директива *zone*, определяющая зону разделяемой памяти.
`<name>`	Имя конкретного сервера в составе указанного `<upstream>`; задается в формате `<service>@<host>`, где: • `<service>@` — необязательная часть, задающая имя сервиса в целях разрешения SRV-записей. • `<host>` — доменное имя сервиса (при наличии *resolve*) или IP-адрес; также можно указать порт.

Например, для следующей конфигурации:

```
upstream backend {
    server backend.example.com:8080 service=_http._tcp resolve;
    server 127.0.0.1;
    zone backend 1m;
}
```

Допустимы такие имена серверов:

```
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/_http._tcp@backend.
↪example.com:8080/
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/127.0.0.1/
```

Этот подраздел API позволяет задавать параметры `weight`, `max_conns`, `max_fails`, `fail_timeout`, `backup`, `down` и `sid`, описанные в разделе *server*.

Примечание

Отдельного параметра `drain` здесь нет; включить режим `drain` можно, задав для `down` строковое значение `drain`:

```
$ curl -X PUT -d "drain" \
  http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com/down
```

Пример:

```
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com?
↪defaults=on
```

```
{
    "weight": 1,
    "max_conns": 0,
    "max_fails": 1,
    "fail_timeout": 10,
    "backup": true,
    "down": false,
    "sid": ""
}
```

Фактически доступны будут только те параметры, которые поддерживает текущий метод балансировки нагрузки *апстрима*. Так, если апстрим настроен с методом балансировки `random`:

```
upstream backend {
    zone backend 256k;
```

```
    server backend.example.com resolve max_conns=5;
    random;
}
```

То добавить в него новый сервер с параметром `backup` невозможно:

```
$ curl -X PUT -d '{ "backup": true }' \
    http://127.0.0.1/config/http/upstreams/backend/servers/backend1.example.com
```

```
{
    "error": "FormatError",
    "description": "The \"backup\" field is unknown."
}
```

Примечание

Даже с совместимым методом балансировки параметр `backup` можно задать лишь при добавлении нового сервера.

При удалении серверов можно установить аргумент `connection_drop=<значение>` (PRO), чтобы переопределить настройки *proxy_connection_drop*, *grpc_connection_drop*, *fastcgi_connection_drop*, *scgi_connection_drop* и *uwsgi_connection_drop*:

```
$ curl -X DELETE \
    http://127.0.0.1/config/http/upstreams/backend/servers/backend1.example.com?
↪connection_drop=off

$ curl -X DELETE \
    http://127.0.0.1/config/http/upstreams/backend/servers/backend2.example.com?
↪connection_drop=on

$ curl -X DELETE \
    http://127.0.0.1/config/http/upstreams/backend/servers/backend3.example.com?
↪connection_drop=1000
```

`/config/stream/upstreams/<upstream>/servers/<name>`

Позволяет настраивать отдельные серверы в составе апстрима, в том числе добавлять новые и удалять настроенные.

Параметры в составе пути URI:

`<upstream>`	Имя блока `upstream`; чтобы настраивать его через `/config`, в нем должна быть задана директива *zone*, определяющая зону разделяемой памяти.
`<name>`	Имя конкретного сервера в составе указанного `<upstream>`; задается в формате `<service>@<host>`, где: • `<service>@` — необязательная часть, задающая имя сервиса в целях разрешения SRV-записей. • `<host>` — доменное имя сервиса (при наличии *resolve*) или IP-адрес; также можно указать порт.

Например, для следующей конфигурации:

```
upstream backend {
    server backend.example.com:8080 service=_example._tcp resolve;
    server 127.0.0.1:12345;
    zone backend 1m;
}
```

Допустимы такие имена серверов:

```
$ curl http://127.0.0.1/config/stream/upstreams/backend/servers/_example._tcp@backend.
↪example.com:8080/
$ curl http://127.0.0.1/config/stream/upstreams/backend/servers/127.0.0.1:12345/
```

Этот подраздел API позволяет задавать параметры `weight`, `max_conns`, `max_fails`, `fail_timeout`, `backup` и `down`, описанные в разделе *server*.

Примечание

Отдельного параметра `drain` здесь нет; включить режим `drain` можно, задав для `down` строковое значение `drain`:

```
$ curl -X PUT -d "drain" \
  http://127.0.0.1/config/stream/upstreams/backend/servers/backend.example.com/down
```

Пример:

```
curl http://127.0.0.1/config/stream/upstreams/backend/servers/backend.example.com?
↪defaults=on
```

```
{
    "weight": 1,
    "max_conns": 0,
    "max_fails": 1,
    "fail_timeout": 10,
    "backup": true,
    "down": false,
}
```

Фактически доступны будут только те параметры, которые поддерживает текущий метод балансировки нагрузки *апстрима*. Так, если апстрим настроен с методом балансировки `random`:

```
upstream backend {
    zone backend 256k;
    server backend.example.com resolve max_conns=5;
    random;
}
```

То добавить в него новый сервер с параметром `backup` невозможно:

```
$ curl -X PUT -d '{ "backup": true }' \
    http://127.0.0.1/config/stream/upstreams/backend/servers/backend1.example.com
```

```
{
    "error": "FormatError",
    "description": "The \"backup\" field is unknown."
}
```

> **Примечание**
>
> Даже с совместимым методом балансировки параметр `backup` можно задать лишь при добавлении нового сервера.

При удалении серверов можно установить аргумент `connection_drop=<значение>` (PRO), чтобы переопределить настройки *proxy_connection_drop*:

```
$ curl -X DELETE \
    http://127.0.0.1/config/stream/upstreams/backend/servers/backend1.example.com?
↪connection_drop=off

$ curl -X DELETE \
    http://127.0.0.1/config/stream/upstreams/backend/servers/backend2.example.com?
↪connection_drop=on

$ curl -X DELETE \
    http://127.0.0.1/config/stream/upstreams/backend/servers/backend3.example.com?
↪connection_drop=1000
```

HTTP-методы

Рассмотрим семантику каждого из применимых к этому разделу HTTP-методов на примере следующей конфигурации апстрима:

```
http {
    # ...

    upstream backend {
        zone upstream 256k;
        server backend.example.com resolve max_conns=5;
        # ...
    }

    server {
        # ...

        location /config/ {
            api /config/;

            allow 127.0.0.1;
            deny all;
        }
    }
}
```

GET

HTTP-метод `GET` позволяет запросить сущность по любому существующему пути в пределах `/config` так же, как это делается в других разделах API.

Например, для ветки серверов апстрима `/config/http/upstreams/backend/servers/` допустимы такие запросы:

```
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com/max_
↪conns
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com
$ curl http://127.0.0.1/config/http/upstreams/backend/servers
$ # ...
$ curl http://127.0.0.1/config
```

Получить параметры по умолчанию можно с аргументом `defaults=on`:

```
$ curl http://127.0.0.1/config/http/upstreams/backend/servers?defaults=on
```

```
{
    "backend.example.com": {
        "weight": 1,
        "max_conns": 5,
        "max_fails": 1,
        "fail_timeout": 10,
        "backup": false,
        "down": false,
        "sid": ""
    }
}
```

PUT

HTTP-метод `PUT` позволяет создать новую JSON-сущность по указанному пути или *полностью* заменить существующую.

Например, чтобы добавить не заданный ранее параметр `max_fails` у сервера `backend.example.com` в апстриме `backend`:

```
$ curl -X PUT -d '2' \
    http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com/max_
↪fails
```

```
{
    "success": "Updated",
    "description": "Existing configuration API entity \"/config/http/upstreams/
↪backend/servers/backend.example.com/max_fails\" was updated with replacing."
}
```

Проверим изменения:

```
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com
```

```
{
    "max_conns": 5,
    "max_fails": 2
}
```

DELETE

HTTP-метод `DELETE` удаляет *ранее заданные* настройки по указанному пути; при этом восстанавливаются значения по умолчанию, если они есть.

Например, чтобы удалить измененный ранее параметр `max_fails` у сервера `backend.example.com` в апстриме `backend`:

```
$ curl -X DELETE \
    http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com/max_
↪fails
```

```
{
    "success": "Reset",
    "description": "Configuration API entity \"/config/http/upstreams/backend/servers/
↪backend.example.com/max_fails\" was reset to default."
}
```

Проверим изменения с аргументом `defaults=on`:

```
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com?
↪defaults=on
```

```
{
    "weight": 1,
    "max_conns": 5,
    "max_fails": 1,
    "fail_timeout": 10,
    "backup": false,
    "down": false,
    "sid": ""
}
```

Параметр `max_fails` вернулся к значению по умолчанию.

PATCH

HTTP-метод `PATCH` позволяет создать новую сущность по указанному пути либо частично заменить или дополнить существующую (RFC 7386), отправив в данных JSON-определение.

Метод работает так: если сущности, указанные в новом определении, уже есть в конфигурации, они будут перезаписаны; если их нет, то они будут добавлены.

Например, чтобы поменять значение параметра `down` у сервера `backend.example.com` в апстриме `backend`, оставив прочее без изменений:

```
$ curl -X PATCH -d '{ "down": true }' \
    http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com
```

```
{
    "success": "Updated",
    "description": "Existing configuration API entity \"/config/http/upstreams/
↪backend/servers/backend.example.com\" was updated with merging."
}
```

Проверим изменения:

```
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com
```

```
{
    "max_conns": 5,
    "down": true
}
```

Обратите внимание, что переданный с запросом `PATCH` JSON-объект *слился* с уже существующим, а не заменил его целиком, как было бы с `PUT`.

Особый случай представляют значения `null`; они используются для удаления отдельных элементов конфигурации в ходе такого слияния.

Примечание

Такое удаление аналогично действию `DELETE`; в частности, восстанавливаются значения по умолчанию.

Например, чтобы удалить добавленный ранее параметр `down` и одновременно с этим изменить `max_conns`:

```
$ curl -X PATCH -d '{ "down": null, "max_conns": 6 }' \
    http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com
```

```
{
    "success": "Updated",
    "description": "Existing configuration API entity \"/config/http/upstreams/
↪backend/servers/backend.example.com\" was updated with merging."
}
```

Проверим изменения:

```
$ curl http://127.0.0.1/config/http/upstreams/backend/servers/backend.example.com
```

```
{
    "max_conns": 6
}
```

Параметр `down`, для которого было передано значение `null`, удален; значение `max_conns` изменено.

Auth Basic

Позволяет ограничить доступ к ресурсам с проверкой имени и пароля пользователя по протоколу «HTTP Basic Authentication».

Ограничить доступ можно также по *адресу* или по *результату подзапроса*. Одновременное ограничение доступа по адресу и паролю управляется директивой *satisfy*.

Пример конфигурации

```
location / {
    auth_basic           "closed site";
    auth_basic_user_file conf/htpasswd;
}
```

Директивы

auth_basic

Синтаксис	`auth_basic` *строка* | off;
По умолчанию	`auth_basic off;`
Контекст	http, server, location, limit_except

Включает проверку имени и пароля пользователя по протоколу «HTTP Basic Authentication». Заданный параметр используется в качестве *realm*. В значении параметра допустимо использование переменных.

`off`	отменяет действие унаследованной с предыдущего уровня конфигурации директивы *auth_basic*

auth_basic_user_file

Синтаксис	`auth_basic_user_file` *файл*;
По умолчанию	—
Контекст	http, server, location, limit_except

Задает *файл*, в котором хранятся имена и пароли пользователей. Формат файла следующий:

```
# комментарий имя1:пароль1 имя2:пароль2:комментарий имя3:пароль3
```

В имени *файла* можно использовать переменные.

Поддерживаются следующие типы паролей:

- зашифрованные функцией *crypt()*; могут быть созданы с помощью утилиты `htpasswd` из дистрибутива HTTP-сервера Apache или команды «*openssl passwd*»;
- хэшированные с помощью алгоритма, основанного на MD5, по версии Apache (apr1); могут быть созданы теми же инструментами;
- заданные согласно синтаксису «*{схема}данные*» как описано в RFC 2307; в настоящий момент реализованы схемы *PLAIN* (в качестве примера, не следует применять), *SHA* (простое SHA-1 хэширование, не следует применять) и *SSHA* (SHA-1 хэширование с солью, используется в некоторых программах, в частности OpenLDAP и Dovecot).

Осторожно

Поддержка схемы SHA была добавлена лишь для облегчения процесса миграции файлов паролей с других веб-серверов. Ее не следует применять для новых паролей, т.к. используемое при этом SHA-1 хэширование без соли уязвимо к взлому при помощи радужных таблиц.

Auth Request

Предоставляет возможность авторизации клиента, основанной на результате подзапроса. Если подзапрос возвращает код ответа 2xx, доступ разрешается. Если 401 или 403 — доступ запрещается с соответствующим кодом ошибки. Любой другой код ответа, возвращаемый подзапросом, считается ошибкой.

При ошибке 401 клиенту также передается заголовок «WWW-Authenticate» из ответа подзапроса.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_auth_request_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Модуль может быть скомбинирован с другими модулями доступа, такими как *Access* и *Auth Basic* с помощью директивы *satisfy*.

Пример конфигурации

```
location /private/ {
    auth_request /auth;
#    ...
}

location = /auth {
    proxy_pass ...
    proxy_pass_request_body off;
    proxy_set_header Content-Length "";
    proxy_set_header X-Original-URI $request_uri;
}
```

Директивы

auth_request

Синтаксис	`auth_request uri | off;`
По умолчанию	`auth_request off;`
Контекст	http, server, location

Включает авторизацию, основанную на результате выполнения подзапроса, и задает URI, на который будет отправлен подзапрос.

auth_request_set

Синтаксис	`auth_request_set` *$переменная значение*;
По умолчанию	—
Контекст	http, server, location

Устанавливает переменную в запросе в заданное значение после завершения запроса авторизации. Значение может содержать переменные из запроса авторизации, например, *$upstream_http_**.

AutoIndex

Обслуживает запросы, оканчивающиеся косой чертой (/), и выдает листинг каталога. Обычно запрос попадает к модулю *AutoIndex*, когда модуль *Index* не нашел индексный файл.

Пример конфигурации

```
location / {
    autoindex on;
}
```

Директивы

autoindex

Синтаксис	`autoindex` on | off;
По умолчанию	`autoindex off;`
Контекст	http, server, location

Разрешает или запрещает вывод листинга каталога.

autoindex_exact_size

Синтаксис	`autoindex_exact_size` on | off;
По умолчанию	`autoindex_exact_size on;`
Контекст	http, server, location

Для *формата* HTML определяет, как выводить размеры файлов в листинге каталога: точно или округляя до килобайт, мегабайт и гигабайт.

autoindex_format

Синтаксис	`autoindex_format` html | xml | json | jsonp;
По умолчанию	`autoindex_format html;`
Контекст	http, server, location

Задает формат вывода листинга каталога.

При использовании формата JSONP имя callback-функции задается в аргументе запроса *callback*. Если аргумент отсутствует или имеет пустое значение, то используется формат JSON.

Вывод в формате XML может быть преобразован при помощи модуля *XSLT*.

autoindex_localtime

Синтаксис	`autoindex_localtime` on | off;
По умолчанию	`autoindex_localtime off;`
Контекст	http, server, location

Для *формата* HTML определяет, в какой временной зоне выводить время в листинге каталога: в локальной или в UTC.

Browser

Создает переменные, значения которых зависят от значения поля «User-Agent» в заголовке запроса.

Переменные

`$modern_browser`

равна значению, заданному директивой *modern_browser_value*, если браузер опознан как современный;

`$ancient_browser`

равна значению, заданному директивой *ancient_browser_value*, если браузер опознан как устаревший;

`$msie`

равна «1», если браузер опознан как MSIE любой версии.

Пример конфигурации

Выбор индексного файла:

```
modern_browser_value "modern.";

modern_browser msie      5.5;
modern_browser gecko     1.0.0;
modern_browser opera     9.0;
modern_browser safari    413;
modern_browser konqueror 3.0;

index index.${modern_browser}html index.html;
```

Перенаправление для старых браузеров:

```
modern_browser msie      5.0;
modern_browser gecko     0.9.1;
modern_browser opera     8.0;
modern_browser safari    413;
modern_browser konqueror 3.0;

modern_browser unlisted;

ancient_browser Links Lynx netscape4;

if ($ancient_browser) {
    rewrite ^ /ancient.html;
}
```

Директивы

ancient_browser

Синтаксис	`ancient_browser` *строка* ...;
По умолчанию	—
Контекст	http, server, location

Задает подстроки, при нахождении которых в поле «User-Agent» заголовка запроса браузер считается устаревшим. Специальная строка «netscape4» соответствует регулярному выражению «^Mozilla/[1-4]».

ancient_browser_value

Синтаксис	`ancient_browser_value` *строка*;
По умолчанию	`ancient_browser_value 1;`
Контекст	http, server, location

Задает значение для переменных *$ancient_browser*.

modern_browser

Синтаксис	`modern_browser` *браузер версия*; `modern_browser` unlisted;
По умолчанию	—
Контекст	http, server, location

Задает версию браузера, начиная с которой он считается современным. В качестве браузера можно задать *msie*, *gecko* (браузеры, созданные на основе Mozilla), *opera*, *safari* или *konqueror*.

Версии можно задать в форматах X, X.X, X.X.X или X.X.X.X. Максимальные значения для каждого из форматов соответственно — 4000, 4000.99, 4000.99.99 и 4000.99.99.99.

Специальное значение `unlisted` указывает считать современным браузер, не описанный директивами *modern_browser* и *ancient_browser*. В противном случае неперечисленный браузер будет считаться устаревшим. Если в заголовке запроса нет поля «User-Agent», то браузер считается неперечисленным.

modern_browser_value

Синтаксис	`modern_browser_value` *строка*;
По умолчанию	`modern_browser_value 1;`
Контекст	http, server, location

Задает значение для переменных *$modern_browser*.

Charset

Добавляет указанную кодировку в поле «Content-Type» заголовка ответа. Кроме того, модуль может перекодировать данные из одной кодировки в другую с некоторыми ограничениями:

- перекодирование осуществляется только в одну сторону — от сервера к клиенту,
- перекодироваться могут только однобайтные кодировки
- или однобайтные кодировки в UTF-8 и обратно.

Пример конфигурации

```
include        conf/koi-win;

charset        windows-1251;
source_charset koi8-r;
```

Директивы

charset

Синтаксис	`charset` *кодировка* | off;
По умолчанию	`charset off;`
Контекст	http, server, location, if в location

Добавляет указанную кодировку в поле «Content-Type» заголовка ответа. Если эта кодировка отличается от указанной в директиве *source_charset*, то выполняется перекодирование.

Параметр `off` отменяет добавление кодировки в поле «Content-Type» заголовка ответа.

Кодировка может быть задана с помощью переменной:

```
charset $charset;
```

В этом случае необходимо, чтобы все возможные значения переменной присутствовали хотя бы один раз в любом месте конфигурации в виде директив *charset_map*, *charset* или *source_charset*. Для кодировок *utf-8*, *windows-1251* и *koi8-r* для этого достаточно включить в конфигурацию файлы *conf/koi-win*, *conf/koi-utf* и *conf/win-utf*. Для других кодировок можно просто сделать фиктивную таблицу перекодировки, например:

```
charset_map iso-8859-5 _ { }
```

Кроме того, кодировка может быть задана в поле «X-Accel-Charset» заголовка ответа. Эту возможность можно запретить с помощью директив *proxy_ignore_headers*, *fastcgi_ignore_headers*, *uwsgi_ignore_headers*, *scgi_ignore_headers* и *grpc_ignore_headers*.

charset_map

Синтаксис	`charset_map` *кодировка1 кодировка2* { ... }
По умолчанию	—
Контекст	http

Описывает таблицу перекодирования из одной кодировки в другую. Таблица для обратного перекодирования строится на основании тех же данных. Коды символов задаются в шестнадцатеричном виде. Неописанные символы в пределах 80-FF заменяются на «*?*». При перекодировании из UTF-8 символы, отсутствующие в однобайтной кодировке, заменяются на «*&#XXXX;*».

Пример:

```
charset_map koi8-r windows-1251 {
    C0 FE ; # small yu
    C1 E0 ; # small a
```

```
    C2 E1 ; # small b
    C3 F6 ; # small ts
}
```

При описании таблицы перекодирования в UTF-8, коды кодировки UTF-8 должны быть указаны во второй колонке, например:

```
charset_map koi8-r utf-8 {
    C0 D18E ; # small yu
    C1 D0B0 ; # small a
    C2 D0B1 ; # small b
    C3 D186 ; # small ts
}
```

Полные таблицы преобразования из *koi8-r* в *windows-1251* и из *koi8-r* и *windows-1251* в *utf-8* входят в дистрибутив и находятся в файлах *conf/koi-win*, *conf/koi-utf* и *conf/win-utf*.

charset_types

Синтаксис	`charset_types` mime-*тип* ...;
По умолчанию	`charset_types text/html text/xml text/plain text/vnd.wap.wml application/javascript application/rss+xml;`
Контекст	http, server, location

Разрешает работу модуля в ответах с указанными MIME-типами в дополнение к «*text/html*». Специальное значение «*» соответствует любому MIME-типу.

override_charset

Синтаксис	`override_charset` on | off;
По умолчанию	`override_charset off;`
Контекст	http, server, location, if в location

Определяет, выполнять ли перекодирование для ответов, полученных от проксированного сервера или от FastCGI/uwsgi/SCGI/gRPC-сервера, если в ответах уже указана кодировка в поле «Content-Type» заголовка ответа. Если перекодирование разрешено, то в качестве исходной кодировки используется кодировка, указанная в полученном ответе.

Примечание

Если ответ был получен в подзапросе, то, независимо от значения директивы *override_charset*, всегда выполняется перекодирование из кодировки ответа в кодировку основного запроса.

source_charset

Синтаксис	`source_charset` *кодировка*;
По умолчанию	—
Контекст	http, server, location, if в location

Задает исходную кодировку ответа. Если эта кодировка отличается от указанной в директиве *charset*, то выполняется перекодирование.

DAV

Предназначен для автоматизации задач управления файлами на сервере по протоколу WebDAV. Модуль обрабатывает HTTP- и WebDAV-методы PUT, DELETE, MKCOL, COPY и MOVE.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_dav_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Важно

WebDAV-клиенты, которые требуют для работы дополнительных WebDAV-методов, не будут работать с этим модулем.

Пример конфигурации

```
location / {
    root                  /data/www;

    client_body_temp_path /data/client_temp;

    dav_methods PUT DELETE MKCOL COPY MOVE;

    create_full_put_path  on;
    dav_access            group:rw  all:r;

    limit_except GET {
        allow 192.168.1.0/32;
        deny  all;
    }
}
```

Директивы

create_full_put_path

Синтаксис	`create_full_put_path` on | off;
По умолчанию	`create_full_put_path off;`
Контекст	http, server, location

По спецификации WebDAV-метод PUT может создавать файл только в уже существующем каталоге. Данная директива разрешает создавать все необходимые промежуточные каталоги.

dav_access

Синтаксис	`dav_access` *пользователи*:*права* ...;
По умолчанию	`dav_access user:rw;`
Контекст	http, server, location

Задает права доступа для создаваемых файлов и каталогов, например,

```
dav_access user:rw group:rw all:r;
```

Если заданы какие-либо права для group или all, то права для user указывать необязательно:

```
dav_access group:rw all:r;
```

dav_methods

Синтаксис	`dav_methods` off | *метод* ...;
По умолчанию	`dav_methods off;`
Контекст	http, server, location

Разрешает указанные HTTP- и WebDAV-методы. Параметр `off` запрещает все методы, обрабатываемые данным модулем. Поддерживаются следующие методы: PUT, DELETE, MKCOL, COPY и MOVE.

Файл, загружаемый методом PUT, записывается во временный файл, а потом этот файл переименовывается. Временный файл и его постоянное место хранения могут располагаться на разных файловых системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если сохраняемые файлы будут находиться на той же файловой системе, что и каталог с временными файлами, задаваемый директивой *client_body_temp_path* для данного *location*.

При создании файла с помощью метода PUT можно задать дату модификации, передав ее в поле заголовка «Date».

min_delete_depth

Синтаксис	`min_delete_depth` *число*;
По умолчанию	`min_delete_depth 0;`
Контекст	http, server, location

Разрешает методу DELETE удалять файлы при условии, что число элементов в пути запроса не меньше заданного. Например, директива

```
min_delete_depth 4;
```

разрешает удалять файлы по запросам

```
/users/00/00/name
/users/00/00/name/pic.jpg
/users/00/00/page.html
```

и запрещает удаление

```
/users/00/00
```

Empty GIF

Выдает однопиксельный прозрачный GIF.

Пример конфигурации

```
location = /_.gif {
    empty_gif;
}
```

Директивы

empty_gif

Синтаксис	`empty_gif;`
По умолчанию	—
Контекст	location

Разрешает в содержащем location выдавать однопиксельный прозрачный GIF.

FastCGI

Позволяет передавать запросы FastCGI-серверу.

Пример конфигурации

```
location / {
    fastcgi_pass  localhost:9000;
    fastcgi_index index.php;

    fastcgi_param SCRIPT_FILENAME /home/www/scripts/php$fastcgi_script_name;
    fastcgi_param QUERY_STRING    $query_string;
    fastcgi_param REQUEST_METHOD  $request_method;
    fastcgi_param CONTENT_TYPE    $content_type;
    fastcgi_param CONTENT_LENGTH  $content_length;
}
```

Директивы

fastcgi_bind

Синтаксис	`fastcgi_bind` *адрес* [transparent] | off;
По умолчанию	—
Контекст	http, server, location

Задает локальный IP-адрес с необязательным портом, который будет использоваться в исходящих соединениях с FastCGI-сервером. В значении параметра допустимо использование переменных. Специальное значение `off` отменяет действие унаследованной с предыдущего уровня конфигурации директивы *fastcgi_bind*, позволяя системе самостоятельно выбирать локальный IP-адрес и порт.

Параметр `transparent` позволяет задать нелокальный IP-адрес, который будет использоваться в исходящих соединениях с FastCGI-сервером, например, реальный IP-адрес клиента:

```
fastcgi_bind $remote_addr transparent;
```

Для работы параметра обычно требуется запустить рабочие процессы Angie PRO с привилегиями *суперпользователя*. В Linux это не требуется, так как если указан параметр *transparent*, то рабочие процессы наследуют *capability CAP_NET_RAW* из главного процесса.

Важно

Необходимо настроить таблицу маршрутизации ядра для перехвата сетевого трафика с FastCGI-сервера.

fastcgi_buffer_size

Синтаксис	`fastcgi_buffer_size` *размер*;
По умолчанию	`fastcgi_buffer_size 4k|8k;`
Контекст	http, server, location

Задает размер буфера, в который будет читаться первая часть ответа, получаемого от FastCGI-сервера. В этой части ответа обычно находится небольшой заголовок ответа. По умолчанию размер одного буфера равен размеру страницы памяти. В зависимости от платформы это или 4K, или 8K, однако его можно сделать меньше.

fastcgi_buffering

Синтаксис	`fastcgi_buffering` on | off;
По умолчанию	`fastcgi_buffering on;`
Контекст	http, server, location

Разрешает или запрещает использовать буферизацию ответов FastCGI-сервера.

`off`	Angie PRO принимает ответ FastCGI-сервера как можно быстрее, сохраняя его в буферы, заданные директивами *fastcgi_buffer_size* и *fastcgi_buffers*. Если ответ не вмещается целиком в память, то его часть может быть записана на диск во *временный файл*. Запись во временные файлы контролируется директивами *fastcgi_max_temp_file_size* и *fastcgi_temp_file_write_size*.
`on`	ответ синхронно передается клиенту сразу же по мере его поступления. Angie PRO не пытается считать весь ответ FastCGI-сервера. Максимальный размер данных, который Angie PRO может принять от сервера за один раз, задается директивой *fastcgi_buffer_size*.

Буферизация может быть также включена или выключена путем передачи значения «yes» или «no» в поле «X-Accel-Buffering» заголовка ответа. Эту возможность можно запретить с помощью директивы *fastcgi_ignore_headers*.

fastcgi_buffers

Синтаксис	`fastcgi_buffers` *число размер*;
По умолчанию	`fastcgi_busy_buffers_size 8 4k|8k;`
Контекст	http, server, location

Задает число и размер буферов для одного соединения, в которые будет читаться ответ, получаемый от FastCGI-сервера. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

fastcgi_busy_buffers_size

Синтаксис	`fastcgi_busy_buffers_size` *размер*;
По умолчанию	`fastcgi_busy_buffers_size 8k|16k;`
Контекст	http, server, location

При включенной *буферизации* ответов FastCGI-сервера, ограничивает суммарный размер буферов, которые могут быть заняты для отправки ответа клиенту, пока ответ еще не прочитан целиком. Оставшиеся буферы тем временем могут использоваться для чтения ответа и, при необходимости, буферизации части ответа во временный файл. По умолчанию размер ограничен двумя буферами, заданными директивами *fastcgi_buffer_size* и *fastcgi_buffers*.

fastcgi_cache

Синтаксис	`fastcgi_cache` *зона* | off;
По умолчанию	`fastcgi_cache off;`
Контекст	http, server, location

Задает зону разделяемой памяти, используемой для кэширования. Одна и та же зона может использоваться в нескольких местах. В значении параметра можно использовать переменные. Параметр `off` запрещает кэширование, унаследованное с предыдущего уровня конфигурации.

fastcgi_cache_background_update

Синтаксис	`fastcgi_cache_background_update` on | off;
По умолчанию	`fastcgi_cache_background_update off;`
Контекст	http, server, location

Позволяет запустить фоновый подзапрос для обновления просроченного элемента кэша, в то время как клиенту возвращается устаревший кэшированный ответ. Использование устаревшего кэшированного ответа в момент его обновления должно быть *разрешено*.

fastcgi_cache_bypass

Синтаксис	`fastcgi_cache_bypass` *строка* ...;
По умолчанию	—
Контекст	http, server, location

Задает условия, при которых ответ не будет браться из кэша. Если значение хотя бы одного из строковых параметров непустое и не равно «0», то ответ не берется из кэша:

```
fastcgi_cache_bypass $cookie_nocache $arg_nocache$arg_comment;
fastcgi_cache_bypass $http_pragma    $http_authorization;
```

Можно использовать совместно с директивой *fastcgi_no_cache*.

fastcgi_cache_key

Синтаксис	`fastcgi_cache_key` *строка*;
По умолчанию	—
Контекст	http, server, location

Задает ключ для кэширования, например,

```
fastcgi_cache_key localhost:9000$request_uri;
```

fastcgi_cache_lock

Синтаксис	`fastcgi_cache_lock` on | off;
По умолчанию	`fastcgi_cache_lock off;`
Контекст	http, server, location

Если включено, одновременно только одному запросу будет позволено заполнить новый элемент кэша, идентифицируемый согласно директиве *fastcgi_cache_key*, передав запрос на FastCGI-сервер. Остальные запросы этого же элемента будут либо ожидать появления ответа в кэше, либо освобождения блокировки этого элемента, в течение времени, заданного директивой *fastcgi_cache_lock_timeout*.

fastcgi_cache_lock_age

Синтаксис	`fastcgi_cache_lock_age` *время*;
По умолчанию	`fastcgi_cache_lock_age 5s;`
Контекст	http, server, location

Если последний запрос, переданный на FastCGI-сервер для заполнения нового элемента кэша, не завершился за указанное время, на FastCGI-сервер может быть передан еще один запрос.

fastcgi_cache_lock_timeout

Синтаксис	`fastcgi_cache_lock_timeout` *время*;
По умолчанию	`fastcgi_cache_lock_timeout 5s;`
Контекст	http, server, location

Задает таймаут для *fastcgi_cache_lock*. По истечении указанного времени запрос будет передан на FastCGI-сервер, однако ответ не будет кэширован.

fastcgi_cache_max_range_offset

Синтаксис	`fastcgi_cache_max_range_offset` *число*;
По умолчанию	—
Контекст	http, server, location

Задает смещение в байтах для запросов с указанием диапазона запрашиваемых байт (byte-range requests). Если диапазон находится за указанным смещением, range-запрос будет передан на FastCGI-сервер и ответ не будет кэширован.

fastcgi_cache_methods

Синтаксис	`fastcgi_cache_methods` GET | HEAD | POST ...;
По умолчанию	`fastcgi_cache_methods GET HEAD;`
Контекст	http, server, location

Если метод запроса клиента указан в этой директиве, то ответ будет кэширован. Методы «GET» и «HEAD» всегда добавляются в список, но тем не менее рекомендуется перечислять их явно. См. также директиву *fastcgi_no_cache*.

fastcgi_cache_min_uses

Синтаксис	`fastcgi_cache_min_uses` *число*;
По умолчанию	`fastcgi_cache_min_uses 1;`
Контекст	http, server, location

Задает число запросов, после которого ответ будет кэширован.

fastcgi_cache_path

Синтаксис	`fastcgi_cache_path` *путь* [levels=*уровни*] [use_temp_path=on|off] keys_zone=*имя:размер* [inactive=*время*] [max_size=*размер*] [min_free=*размер*] [manager_files=*число*] [manager_sleep=*время*] [manager_threshold=*время*] [loader_files=*число*] [loader_sleep=*время*] [loader_threshold=*время*];
По умолчанию	`fastcgi_cache_min_uses 1;`
Контекст	http, server, location

Задает путь и другие параметры кэша. Данные кэша хранятся в файлах. Ключом и именем файла в кэше является результат функции MD5 от проксированного URL.

Параметр `levels` задает уровни иерархии кэша: можно задать от 1 до 3 уровней, на каждом уровне допускаются значения 1 или 2. Например, при использовании

```
fastcgi_cache_path /data/angie/cache levels=1:2 keys_zone=one:10m;
```

имена файлов в кэше будут такого вида:

```
/data/angie/cache/c/29/b7f54b2df7773722d382f4809d65029c
```

Кэшируемый ответ сначала записывается во временный файл, а потом этот файл переименовывается. Временные файлы и кэш могут располагаться на разных файловых системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если кэш будет находиться на той же файловой системе, что и каталог с временными файлами.

Какой из каталогов будет использоваться для временных файлов определяется параметром `use_temp_path`.

`on`	Если параметр не задан или установлен в значение «on», будет использоваться каталог, задаваемый директивой *fastcgi_temp_path* для данного *location*.
`off`	временные файлы будут располагаться непосредственно в каталоге кэша.

Кроме того, все активные ключи и информация о данных хранятся в зоне разделяемой памяти, имя и размер которой задаются параметром `keys_zone`. Зоны размером в 1 мегабайт достаточно для хранения около 8 тысяч ключей.

Если к данным кэша не обращаются в течение времени, заданного параметром `inactive`, то данные удаляются, независимо от их свежести. По умолчанию inactive равен 10 минутам.

Специальный процесс **cache manager** следит за максимальным размером кэша, а также за минимальным объемом свободного места на файловой системе с кэшем, и удаляет наименее востребованные данные при превышении максимального размера кэша или недостаточном объеме свободного места. Удаление данных происходит итерациями.

`max_size`	максимальное пороговое значение размера кэша
`min_free`	минимальное пороговое значение объема свободного места на файловой системе с кэшем
`manager_files`	максимальное количество удаляемых элементов кэша за одну итерацию По умолчанию *100*
`manager_threshol`	ограничивает время работы одной итерации По умолчанию *200* миллисекунд
`manager_sleep`	время, в течение которого выдерживается пауза между итерациями По умолчанию *50* миллисекунд

Через минуту после старта Angie PRO активируется специальный процесс **cache loader**, который загружает в зону кэша информацию о ранее кэшированных данных, хранящихся на файловой системе. Загрузка также происходит итерациями.

`loader_files`	максимальное количество элементов кэша к загрузке в одну итерацию По умолчанию *100*
`loader_threshold`	ограничивает время работы одной итерации По умолчанию *200* миллисекунд
`loader_sleep`	время, в течение которого выдерживается пауза между итерациями По умолчанию *50* миллисекунд

fastcgi_cache_revalidate

Синтаксис	`fastcgi_cache_revalidate` on | off;
По умолчанию	`fastcgi_cache_revalidate off;`
Контекст	http, server, location

Разрешает ревалидацию просроченных элементов кэша при помощи условных запросов с полями заголовка «If-Modified-Since» и «If-None-Match».

fastcgi_cache_use_stale

Синтаксис	`fastcgi_cache_use_stale` error | timeout | invalid_header | updating | http_500 | http_503 | http_403 | http_429 | off ...;
По умолчанию	`fastcgi_cache_use_stale off;`
Контекст	http, server, location

Определяет, в каких случаях можно использовать устаревший кэшированный ответ. Параметры директивы совпадают с параметрами директивы *fastcgi_next_upstream*.

`error`	позволяет использовать устаревший кэшированный ответ при невозможности выбора FastCGI-сервера для обработки запроса.
`updating`	дополнительный параметр, разрешает использовать устаревший кэшированный ответ, если на данный момент он уже обновляется. Это позволяет минимизировать число обращений к FastCGI-серверам при обновлении кэшированных данных.

Использование устаревшего кэшированного ответа может также быть разрешено непосредственно в заголовке ответа на определенное количество секунд после того, как ответ устарел.

- Расширение stale-while-revalidate поля заголовка «Cache-Control» разрешает использовать устаревший кэшированный ответ, если на данный момент он уже обновляется.
- Расширение stale-if-error поля заголовка «Cache-Control» разрешает использовать устаревший кэшированный ответ в случае ошибки.

Примечание

Такой способ менее приоритетен, чем задание параметров директивы.

Чтобы минимизировать число обращений к FastCGI-серверам при заполнении нового элемента кэша, можно воспользоваться директивой *fastcgi_cache_lock*.

fastcgi_cache_valid

Синтаксис	`fastcgi_cache_valid` [*код* ...] *время*;
По умолчанию	—
Контекст	http, server, location

Задает время кэширования для разных кодов ответа. Например, директивы

```
fastcgi_cache_valid 200 302 10m;
fastcgi_cache_valid 404      1m;
```

задают время кэширования 10 минут для ответов с кодами 200 и 302 и 1 минуту для ответов с кодом 404.

Если указано только время кэширования,

```
fastcgi_cache_valid 5m;
```

то кэшируются только ответы 200, 301 и 302.

Кроме того, можно кэшировать любые ответы с помощью параметра `any`:

```
fastcgi_cache_valid 200 302 10m;
fastcgi_cache_valid 301      1h;
fastcgi_cache_valid any      1m;
```

Примечание

Параметры кэширования могут также быть заданы непосредственно в заголовке ответа. Такой способ приоритетнее, чем задание времени кэширования с помощью директивы.

- Поле заголовка «X-Accel-Expires» задает время кэширования ответа в секундах. Значение *0* запрещает кэшировать ответ. Если значение начинается с префикса *@*, оно задает абсолютное время в секундах с начала эпохи, до которого ответ может быть кэширован.
- Если в заголовке нет поля «X-Accel-Expires», параметры кэширования определяются по полям заголовка «Expires» или «Cache-Control».
- Ответ, в заголовке которого есть поле «Set-Cookie», не будет кэшироваться.
- Ответ, в заголовке которого есть поле «Vary» со специальным значением «*», не будет кэшироваться. Ответ, в заголовке которого есть поле «Vary» с другим значением, будет кэширован с учетом соответствующих полей заголовка запроса.

Обработка одного или более из этих полей заголовка может быть отключена при помощи директивы *fastcgi_ignore_headers*.

fastcgi_catch_stderr

Синтаксис	`fastcgi_catch_stderr` *строка*;
По умолчанию	—
Контекст	http, server, location

Задает строку для поиска в потоке ошибок ответа, полученного от FastCGI-сервера. Если строка найдена, то считается, что FastCGI-сервер вернул *неверный* ответ. Это позволяет обрабатывать ошибки приложений в Angie PRO, например:

```
location /php/ {
    fastcgi_pass backend:9000;
    ...
    fastcgi_catch_stderr "PHP Fatal error";
    fastcgi_next_upstream error timeout invalid_header;
}
```

fastcgi_connect_timeout

Синтаксис	`fastcgi_connect_timeout` *время*;
По умолчанию	`fastcgi_connect_timeout 60s;`
Контекст	http, server, location

Задает таймаут для установления соединения с FastCGI-сервером. Необходимо иметь в виду, что этот таймаут обычно не может превышать 75 секунд.

fastcgi_connection_drop

Синтаксис	`fastcgi_connection_drop` *время* | on | off;
По умолчанию	`fastcgi_connection_drop off;`
Контекст	http, server, location

Настраивает завершение всех соединений с проксируемым сервером, если он был удален из группы или помечен как постоянно недоступный в результате процесса *reresolve* или *команды API* `DELETE`.

Соединение завершается, когда обрабатывается следующее событие чтения или записи для клиента или проксируемого сервера.

Установка *времени* включает *таймаут* до завершения соединения; при выборе значения `on` соединения завершаются немедленно.

fastcgi_force_ranges

Синтаксис	`fastcgi_force_ranges` on | off;
По умолчанию	`fastcgi_force_ranges off;`
Контекст	http, server, location

Включает поддержку диапазонов запрашиваемых байт (byte-range) для кэшированных и некэшированных ответов FastCGI-сервера вне зависимости от наличия поля «Accept-Ranges» в заголовках этих ответов.

fastcgi_hide_header

Синтаксис	`fastcgi_hide_header` *поле*;
По умолчанию	—
Контекст	http, server, location

По умолчанию Angie PRO не передает клиенту поля заголовка «Status» и «X-Accel-...» из ответа FastCGI-сервера. Директива *fastcgi_hide_header* задает дополнительные поля, которые не будут передаваться. Если же передачу полей нужно разрешить, можно воспользоваться директивой *fastcgi_pass_header*.

fastcgi_ignore_client_abort

Синтаксис	`fastcgi_ignore_client_abort` on | off;
По умолчанию	`fastcgi_ignore_client_abort off;`
Контекст	http, server, location

Определяет, закрывать ли соединение с FastCGI-сервером в случае, если клиент закрыл соединение, не дождавшись ответа.

fastcgi_ignore_headers

Синтаксис	`fastcgi_ignore_headers` *поле*;
По умолчанию	—
Контекст	http, server, location

Запрещает обработку некоторых полей заголовка из ответа FastCGI-сервера. В директиве можно указать поля «X-Accel-Redirect», «X-Accel-Expires», «X-Accel-Limit-Rate», «X-Accel-Buffering», «X-Accel-Charset», «Expires», «Cache-Control», «Set-Cookie» и «Vary».

Если не запрещено, обработка этих полей заголовка заключается в следующем:

- «X-Accel-Expires», «Expires», «Cache-Control», «Set-Cookie» и «Vary» задают *параметры кэширования* ответа;
- «X-Accel-Redirect» производит *внутреннее перенаправление* на указанный URI;

- «X-Accel-Limit-Rate» задает *ограничение скорости* передачи ответа клиенту;
- «X-Accel-Buffering» включает или выключает *буферизацию* ответа;
- «X-Accel-Charset» задает желаемую *кодировку* ответа.

fastcgi_index

Синтаксис	`fastcgi_index` *имя*;
По умолчанию	—
Контекст	http, server, location

Задает имя файла, который при создании переменной *$fastcgi_script_name* будет добавляться после URI, если URI заканчивается косой чертой. Например, при таких настройках

```
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME /home/www/scripts/php$fastcgi_script_name;
```

и запросе `/page.php` параметр SCRIPT_FILENAME будет равен `/home/www/scripts/php/page.php`,

а при запросе `/` - `/home/www/scripts/php/index.php`.

fastcgi_intercept_errors

Синтаксис	`fastcgi_intercept_errors` on | off;
По умолчанию	`fastcgi_intercept_errors off;`
Контекст	http, server, location

Определяет, передавать ли клиенту ответы FastCGI-сервера с кодом больше либо равным 300, или же перехватывать их и перенаправлять на обработку Angie PRO с помощью директивы *error_page*.

fastcgi_keep_conn

Синтаксис	`fastcgi_keep_conn` on | off;
По умолчанию	`fastcgi_keep_conn off;`
Контекст	http, server, location

По умолчанию FastCGI-сервер будет закрывать соединение сразу же после отправки ответа. При установке значения `on` Angie PRO указывает FastCGI-серверу оставлять соединения открытыми. Это в частности требуется для функционирования *постоянных соединений* с FastCGI-серверами.

fastcgi_limit_rate

Синтаксис	`fastcgi_limit_rate` *скорость*;
По умолчанию	`fastcgi_limit_rate 0;`
Контекст	http, server, location

Ограничивает скорость чтения ответа от проксируемого сервера. *Скорость* задается в байтах в секунду; можно использовать переменные.

0	отключает ограничение скорости

Примечание

Ограничение устанавливается на запрос, поэтому, если Angie PRO одновременно откроет два соединения к FastCGI-серверу, суммарная скорость будет вдвое выше заданного ограничения. Ограничение работает только в случае, если включена *буферизация* ответов FastCGI-сервера.

fastcgi_max_temp_file_size

Синтаксис	`fastcgi_max_temp_file_size` *размер*;
По умолчанию	`fastcgi_max_temp_file_size 1024m;`
Контекст	http, server, location

Если включена *буферизация* ответов FastCGI-сервера, и ответ не вмещается целиком в буферы, заданные директивами *fastcgi_buffer_size* и *fastcgi_buffers*, часть ответа может быть записана во временный файл. Эта директива задает максимальный размер временного файла. Размер данных, сбрасываемых во временный файл за один раз, задается директивой *fastcgi_temp_file_write_size*.

0	отключает возможность буферизации ответов во временные файлы

Примечание

Данное ограничение не распространяется на ответы, которые будут *кэшированы* или сохранены *на диске*.

fastcgi_next_upstream

Синтаксис	`fastcgi_next_upstream` error | timeout | invalid_header | http_500 | http_503 | http_403 | http_404 | http_429 | non_idempotent | off ...;
По умолчанию	`fastcgi_next_upstream error timeout;`
Контекст	http, server, location

Определяет, в каких случаях запрос будет передан следующему серверу:

`error`	произошла ошибка соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`timeout`	произошел таймаут во время соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`invalid_header`	сервер вернул пустой или неверный ответ;
`http_500`	сервер вернул ответ с кодом 500;
`http_503`	сервер вернул ответ с кодом 503;
`http_403`	сервер вернул ответ с кодом 403;
`http_404`	сервер вернул ответ с кодом 404;
`http_429`	сервер вернул ответ с кодом 429;
`non_idempotent`	обычно запросы с неидемпотентным методом (*POST*, *LOCK*, *PATCH*) не передаются на другой сервер, если запрос серверу группы уже был отправлен; включение параметра явно разрешает повторять подобные запросы;
`off`	запрещает передачу запроса следующему серверу.

Примечание

Необходимо понимать, что передача запроса следующему серверу возможна только при условии, что клиенту еще ничего не передавалось. То есть, если ошибка или таймаут возникли в середине передачи ответа, то исправить это уже невозможно.

Директива также определяет, что считается *неудачной попыткой* работы с сервером.

`error timeout invalid_header`	всегда считаются неудачными попытками, даже если они не указаны в директиве
`http_500 http_503 http_429`	считаются неудачными попытками, только если они указаны в директиве
`http_403 http_404`	никогда не считаются неудачными попытками

Передача запроса следующему серверу может быть ограничена по *количеству попыток* и по *времени*.

fastcgi_next_upstream_timeout

Синтаксис	`fastcgi_next_upstream_timeout` *время*;
По умолчанию	`fastcgi_next_upstream_timeout 0;`
Контекст	http, server, location

Ограничивает время, в течение которого возможна передача запроса *следующему серверу*.

`0`	отключает это ограничение

fastcgi_next_upstream_tries

Синтаксис	`fastcgi_next_upstream_tries` *число*;
По умолчанию	`fastcgi_next_upstream_tries 0;`
Контекст	http, server, location

Ограничивает число допустимых попыток для передачи запроса *следующему серверу*.

`0`	отключает это ограничение

fastcgi_no_cache

Синтаксис	`fastcgi_no_cache` *строка* ...;
По умолчанию	—
Контекст	http, server, location

Задает условия, при которых ответ не будет сохраняться в кэш. Если значение хотя бы одного из строковых параметров непустое и не равно «0», то ответ не будет сохранен:

```
fastcgi_no_cache $cookie_nocache $arg_nocache$arg_comment;
fastcgi_no_cache $http_pragma    $http_authorization;
```

Можно использовать совместно с директивой *fastcgi_cache_bypass*.

fastcgi_param

Синтаксис	`fastcgi_param` *параметр значение* [if_not_empty];
По умолчанию	—
Контекст	http, server, location

Задает параметр, который будет передаваться FastCGI-серверу. В качестве значения можно использовать текст, переменные и их комбинации. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *fastcgi_param*.

Ниже приведен пример минимально необходимых параметров для PHP:

```
fastcgi_param SCRIPT_FILENAME /home/www/scripts/php$fastcgi_script_name;
fastcgi_param QUERY_STRING    $query_string;
```

Параметр SCRIPT_FILENAME используется в PHP для определения имени скрипта, а в параметре QUERY_STRING передаются параметры запроса.

Если скрипты обрабатывают запросы POST, то нужны еще три параметра:

```
fastcgi_param REQUEST_METHOD  $request_method;
fastcgi_param CONTENT_TYPE    $content_type;
fastcgi_param CONTENT_LENGTH  $content_length;
```

Если PHP был собран с параметром конфигурации *–enable-force-cgi-redirect*, то нужно передавать параметр REDIRECT_STATUS со значением «200»:

```
fastcgi_param REDIRECT_STATUS 200;
```

Если директива указана с `if_not_empty`, такой параметр с пустым значением передаваться на сервер не будет:

```
fastcgi_param HTTPS           $https if_not_empty;
```

fastcgi_pass

Синтаксис	`fastcgi_pass` *адрес*;
По умолчанию	—
Контекст	location, if в location

Задает адрес FastCGI-сервера. Адрес может быть указан в виде доменного имени или IP-адреса, и порта:

```
fastcgi_pass localhost:9000;
```

или в виде пути UNIX-сокета:

```
fastcgi_pass unix:/tmp/fastcgi.socket;
```

Если доменному имени соответствует несколько адресов, то все они будут использоваться по очереди (round-robin). И, кроме того, адрес может быть *группой серверов*. Если используется группа, указать порт невозможно; вместо этого укажите порт для каждого сервера внутри группы отдельно.

В значении параметра можно использовать переменные. В этом случае, если адрес указан в виде доменного имени, имя ищется среди описанных *групп серверов* и если не найдено, то определяется с помощью *resolver*'а.

fastcgi_pass_header

Синтаксис	`fastcgi_pass_header` *поле*;
По умолчанию	—
Контекст	http, server, location

Разрешает передавать от FastCGI-сервера клиенту *запрещенные для передачи* поля заголовка.

fastcgi_pass_request_body

Синтаксис	`fastcgi_pass_request_body` on | off;
По умолчанию	—
Контекст	http, server, location

Позволяет запретить передачу исходного тела запроса на FastCGI-сервер. См. также директиву *fastcgi_pass_request_headers*.

fastcgi_pass_request_headers

Синтаксис	`fastcgi_pass_request_headers` on | off;
По умолчанию	—
Контекст	http, server, location

Позволяет запретить передачу полей заголовка исходного запроса на FastCGI-сервер. См. также директиву *fastcgi_pass_request_body*.

fastcgi_read_timeout

Синтаксис	`fastcgi_read_timeout` *время*;
По умолчанию	`fastcgi_read_timeout 60s;`
Контекст	http, server, location

Задает таймаут при чтении ответа FastCGI-сервера. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями чтения. Если по истечении этого времени FastCGI-сервер ничего не передаст, соединение закрывается.

fastcgi_request_buffering

Синтаксис	`fastcgi_request_buffering` on | off;
По умолчанию	`fastcgi_request_buffering on;`
Контекст	http, server, location

Разрешает или запрещает использовать буферизацию тела запроса клиента.

`on`	тело запроса полностью *читается* от клиента перед отправкой запроса на FastCGI-сервер.
`off`	тело запроса отправляется на FastCGI-сервер сразу же по мере его поступления. В этом случае запрос не может быть передан *следующему серверу*, если Angie PRO уже начал отправку тела запроса.

fastcgi_send_lowat

Синтаксис	`fastcgi_send_lowat` *размер*;
По умолчанию	`fastcgi_send_lowat 0;`
Контекст	http, server, location

При установке директивы в ненулевое значение Angie PRO будет пытаться минимизировать число операций отправки на исходящих соединениях с FastCGI-сервером либо при помощи флага `NOTE_LOWAT` метода *kqueue*, либо при помощи параметра сокета `SO_SNDLOWAT`, с указанным размером.

Примечание

Эта директива игнорируется на Linux, Solaris и Windows.

fastcgi_send_timeout

Синтаксис	`fastcgi_send_timeout` *время*;
По умолчанию	`fastcgi_send_timeout 60s;`
Контекст	http, server, location

Задает таймаут при передаче запроса FastCGI-серверу. Таймаут устанавливается не на всю передачу запроса, а только между двумя операциями записи. Если по истечении этого времени FastCGI-сервер не примет новых данных, соединение закрывается.

fastcgi_socket_keepalive

Синтаксис	`fastcgi_socket_keepalive` on | off;
По умолчанию	`fastcgi_socket_keepalive off;`
Контекст	http, server, location

Конфигурирует поведение «TCP keepalive» для исходящих соединений к FastCGI-серверу.

`""`	По умолчанию для сокета действуют настройки операционной системы.
`on`	для сокета включается параметр *SO_KEEPALIVE*

fastcgi_split_path_info

Синтаксис	`fastcgi_split_path_info` *regex*;
По умолчанию	—
Контекст	location

Задает регулярное выражение, выделяющее значение для переменной *$fastcgi_path_info*. Регулярное выражение должно иметь два выделения, из которых первое становится значением переменной *$fastcgi_script_name*, а второе - значением переменной *$fastcgi_path_info*. Например, при таких настройках

```
location ~ ^(.+\.php)(.*)$ {
    fastcgi_split_path_info       ^(.+\.php)(.*)$;
    fastcgi_param SCRIPT_FILENAME /path/to/php$fastcgi_script_name;
    fastcgi_param PATH_INFO       $fastcgi_path_info;
```

и запросе `/show.php/article/0001` параметр SCRIPT_FILENAME будет равен `/path/to/php/show.php`,

а параметр PATH_INFO - `/article/0001`.

fastcgi_store

Синтаксис	`fastcgi_store` on | off | *строка*;
По умолчанию	`fastcgi_store off;`
Контекст	http, server, location

Разрешает сохранение на диск файлов.

`on`	сохраняет файлы в соответствии с путями, указанными в директивах *alias* или *root*
`off`	запрещает сохранение файлов

Кроме того, имя файла можно задать явно с помощью строки с переменными:

```
fastcgi_store /data/www$original_uri;
```

Время изменения файлов выставляется согласно полученному полю «Last-Modified» в заголовке ответа. Ответ сначала записывается во временный файл, а потом этот файл переименовывается. Временный файл и постоянное место хранения ответа могут располагаться на разных файловых системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если сохраняемые файлы будут находиться на той же файловой системе, что и каталог с временными файлами, задаваемый директивой *fastcgi_temp_path* для данного *location*.

Директиву можно использовать для создания локальных копий статических неизменяемых файлов, например:

```
location /images/ {
    root                  /data/www;
    error_page            404 = /fetch$uri;
}
```

```
location /fetch/ {
    internal;

    fastcgi_pass         backend:9000;
    ...

    fastcgi_store        on;
    fastcgi_store_access user:rw group:rw all:r;
    fastcgi_temp_path    /data/temp;

    alias                /data/www/;
}
```

fastcgi_store_access

Синтаксис	`fastcgi_store_access` пользователи:права ...;
По умолчанию	`fastcgi_store_access user:rw;`
Контекст	http, server, location

Задает права доступа для создаваемых файлов и каталогов, например,

```
fastcgi_store_access user:rw group:rw all:r;
```

Если заданы какие-либо права для group или all, то права для user указывать необязательно:

```
fastcgi_store_access group:rw all:r;
```

fastcgi_temp_file_write_size

Синтаксис	`fastcgi_temp_file_write_size` *размер*;
По умолчанию	`fastcgi_temp_file_write_size 8k|16k;`
Контекст	http, server, location

Ограничивает размер данных, сбрасываемых во временный файл за один раз, при включенной буферизации ответов FastCGI-сервера во временные файлы. По умолчанию размер ограничен двумя буферами, заданными директивами *fastcgi_buffer_size* и *fastcgi_buffers*. Максимальный размер временного файла задается директивой *fastcgi_max_temp_file_size*.

fastcgi_temp_path

Синтаксис	`fastcgi_temp_path` *путь* [*уровень1* [*уровень2* [*уровень3*]]]`;
По умолчанию	`fastcgi_temp_path fastcgi_temp;`
Контекст	http, server, location

Задает имя каталога для хранения временных файлов с данными, полученными от FastCGI-серверов. В каталоге может использоваться иерархия подкаталогов до трех уровней. Например, при такой конфигурации

```
fastcgi_temp_path /spool/angie/fastcgi_temp 1 2;
```

временный файл будет следующего вида:

```
/spool/angie/fastcgi_temp/7/45/00000123457
```

См. также параметр *use_temp_path* директивы *fastcgi_cache_path*.

Параметры, передаваемые FastCGI-серверу

Поля заголовка HTTP-запроса передаются FastCGI-серверу в виде параметров. В приложениях и скриптах, запущенных в виде FastCGI-сервера, эти параметры обычно доступны в виде переменных среды. Например, поле заголовка «User-Agent» передается как параметр HTTP_USER_AGENT. Кроме полей заголовка HTTP-запроса можно передавать произвольные параметры с помощью директивы *fastcgi_param*.

Встроенные переменные

В модуле *http_fastcgi* есть встроенные переменные, которые можно использовать для формирования параметров с помощью директивы *fastcgi_param*:

`$fastcgi_script_name`

URI запроса или же, если URI заканчивается косой чертой, то URI запроса, дополненное именем индексного файла, задаваемого директивой *fastcgi_index*. Эту переменную можно использовать для задания параметров SCRIPT_FILENAME и PATH_TRANSLATED, используемых, в частности, для определения имени скрипта в PHP. Например, для запроса `/info/` и при использовании директив

```
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME /home/www/scripts/php$fastcgi_script_name;
```

параметр SCRIPT_FILENAME будет равен `/home/www/scripts/php/info/index.php`.

При использовании директивы *fastcgi_split_path_info* переменная *$fastcgi_script_name* равна значению первого выделения, задаваемого этой директивой.

`$fastcgi_path_info`

значение второго выделения, задаваемого директивой *fastcgi_split_path_info*. Эту переменную можно использовать для задания параметра PATH_INFO.

FLV

Обеспечивает серверную поддержку псевдо-стриминга для файлов Flash Video (FLV).

Он специальным образом обрабатывает запросы с аргументом *start* в строке запроса, посылая в ответ содержимое файла с запрошенного смещения в байтах, добавив перед ним FLV-заголовок.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_flv_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
location ~ \.flv$ {
    flv;
}
```

Директивы

flv

Синтаксис	`flv;`
По умолчанию	—
Контекст	location

Включает в содержащем location обработку этим модулем.

Geo

Создает переменные, значения которых зависят от IP-адреса клиента.

Пример конфигурации

```
geo $geo {
    default        0;

    127.0.0.1      2;
    192.168.1.0/24 1;
    10.1.0.0/16    1;

    ::1            2;
    2001:0db8::/32 1;
}
```

Директивы

geo

Синтаксис	`geo` [*$адрес*] *$переменная* { ... }
По умолчанию	—
Контекст	http

Описывает для указанной переменной зависимость значения от IP-адреса клиента. По умолчанию адрес берется из переменной *$remote_addr*, но его также можно получить из другой переменной, например:

```
geo $arg_remote_addr $geo {
    ...;
}
```

Примечание

Поскольку переменные вычисляются только в момент использования, само по себе наличие даже большого числа объявлений переменных `geo` не влечет за собой никаких дополнительных расходов на обработку запросов.

Если значение переменной не представляет из себя правильный IP-адрес, то используется адрес «255.255.255.255».

Адреса задаются либо префиксами в формате CIDR (включая одиночные адреса), либо в виде диапазонов.

Также поддерживаются следующие специальные параметры:

`delete`	удаляет описанную сеть
`default`	значение переменной, если адрес клиента не соответствует ни одному из заданных адресов. При задании адресов в формате CIDR вместо *default* можно использовать «*0.0.0.0/0*» и «*::/0*». Если параметр *default* не указан, значением по умолчанию будет пустая строка.
`include`	включает файл с адресами и значениями. Включений может быть несколько.
`proxy`	задает доверенные адреса, при запросе с которых будет использоваться адрес в переданном поле заголовка запроса «*X-Forwarded-For*». В отличие от обычных адресов, доверенные адреса проверяются последовательно.
`proxy_recursive`	включает рекурсивный поиск адреса. При выключенном рекурсивном поиске вместо исходного адреса клиента, совпадающего с одним из доверенных адресов, будет использоваться последний адрес, переданный в «*X-Forwarded-For*». При включенном рекурсивном поиске вместо исходного адреса клиента, совпадающего с одним из доверенных адресов, будет использоваться последний не доверенный адрес, переданный в «*X-Forwarded-For*».
`ranges`	указывает, что адреса задаются в виде диапазонов. Этот параметр должен быть первым. Для ускорения загрузки гео-базы нужно располагать адреса в порядке возрастания.

Пример:

```
geo $country {
    default         ZZ;
    include         conf/geo.conf;
```

```
    delete          127.0.0.0/16;
    proxy           192.168.100.0/24;
    proxy           2001:0db8::/32;

    127.0.0.0/24    US;
    127.0.0.1/32    RU;
    10.1.0.0/16     RU;
    192.168.1.0/24 UK;
}
```

В файле *conf/geo.conf* могут быть такие строки:

```
10.2.0.0/16    RU;
192.168.2.0/24 RU;
```

В качестве значения выбирается максимальное совпадение, например, для адреса *127.0.0.1* будет выбрано значение `RU`, а не `US`.

Пример описания диапазонов:

```
geo $country {
    ranges;
    default                    ZZ;
    127.0.0.0-127.0.0.0        US;
    127.0.0.1-127.0.0.1        RU;
    127.0.0.2-127.0.0.255      US;
    10.1.0.0-10.1.255.255      RU;
    192.168.1.0-192.168.1.255 UK;
}
```

GeoIP

Создает переменные, значения которых зависят от IP-адреса клиента, используя готовые базы данных MaxMind или их аналоги.

При использовании баз данных с поддержкой IPv6 IPv4-адреса ищутся отображенными на IPv6.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_geoip_module`.

Важно

Для этого модуля нужна база данных MaxMind MaxMind GeoIP или ее аналог, например MaxMind GeoLite2 или ЦМУ ССОП.

Пример конфигурации

```
http {
    geoip_country         GeoIP.dat;
    geoip_city            GeoLiteCity.dat;
    geoip_proxy           192.168.100.0/24;
    geoip_proxy           2001:0db8::/32;
    geoip_proxy_recursive on;
    ...
```

Директивы

geoip_country

Синтаксис	`geoip_country` *файл*;
По умолчанию	—
Контекст	http

Задает базу данных для определения страны в зависимости от значения IP-адреса клиента. При использовании этой базы данных доступны следующие переменные:

`$geoip_country_c`	двухбуквенный код страны, например, «RU», «US».
`$geoip_country_c`	трехбуквенный код страны, например, «RUS», «USA».
`$geoip_country_n`	название страны, например, «Russian Federation», «United States».

geoip_city

Синтаксис	`geoip_city` *файл*;
По умолчанию	—
Контекст	http

Задает базу данных для определения страны, региона и города в зависимости от значения IP-адреса клиента. При использовании этой базы данных доступны следующие переменные:

`$geoip_city_cont`	двухбуквенный код континента, например, «EU», «NA».
`$geoip_city_coun`	двухбуквенный код страны, например, «RU», «US».
`$geoip_city_coun`	трехбуквенный код страны, например, «RUS», «USA».
`$geoip_city_coun`	название страны, например, «Russian Federation», «United States».
`$geoip_dma_code`	DMA-код региона в США (также известный как «код агломерации»), согласно геотаргетингу Google AdWords API.
`$geoip_latitude`	широта.
`$geoip_longitude`	долгота.
`$geoip_region`	двухсимвольный код региона страны (область, край, штат, провинция, федеральная земля и тому подобное), например, «48», «DC».
`$geoip_region_na`	название региона страны (область, край, штат, провинция, федеральная земля и тому подобное), например, «Moscow City», «District of Columbia».
`$geoip_city`	название города, например, «Moscow», «Washington».
`$geoip_postal_co`	почтовый индекс.

geoip_org

Синтаксис	`geoip_org` *файл*;
По умолчанию	—
Контекст	http

Задает базу данных для определения названия организации в зависимости от значения IP-адреса клиента. При использовании этой базы данных доступна следующая переменная:

`$geoip_org`	название организации, например, «The University of Melbourne».

geoip_proxy

Синтаксис	`geoip_proxy` *файл*;
По умолчанию	—
Контекст	http

Задает доверенные адреса, при запросе с которых будет использоваться адрес в переданном поле заголовка запроса «*X-Forwarded-For*».

geoip_proxy_recursive

Синтаксис	`geoip_proxy_recursive` on | off;
По умолчанию	`geoip_proxy_recursive off;`
Контекст	http

При выключенном рекурсивном поиске вместо исходного адреса клиента, совпадающего с одним из доверенных адресов, будет использоваться последний адрес, переданный в «*X-Forwarded-For*». При включенном рекурсивном поиске вместо исходного адреса клиента, совпадающего с одним из доверенных адресов, будет использоваться последний не доверенный адрес, переданный в «*X-Forwarded-For*».

gRPC

Позволяет передавать запросы gRPC-серверу.

Важно

Для работы этого модуля необходим модуль *HTTP2*.

Пример конфигурации

```
server {
    listen 9000;

    http2 on;

    location / {
        grpc_pass 127.0.0.1:9000;
    }
}
```

Директивы

grpc_bind

Синтаксис	`grpc_bind` *адрес* [transparent] | off;
По умолчанию	—
Контекст	http, server, location

Задает локальный IP-адрес с необязательным портом, который будет использоваться в исходящих соединениях с gRPC-сервером. В значении параметра допустимо использование переменных. Специальное значение `off` отменяет действие унаследованной с предыдущего уровня конфигурации директивы *grpc_bind*, позволяя системе самостоятельно выбирать локальный IP-адрес и порт.

Параметр `transparent` позволяет задать нелокальный IP-адрес, который будет использоваться в исходящих соединениях с gRPC-сервером, например, реальный IP-адрес клиента:

```
grpc_bind $remote_addr transparent;
```

Для работы параметра обычно требуется запустить рабочие процессы Angie PRO с привилегиями *суперпользователя*. В Linux это не требуется, так как если указан параметр *transparent*, то рабочие процессы наследуют *capability CAP_NET_RAW* из главного процесса.

Важно

Необходимо настроить таблицу маршрутизации ядра для перехвата сетевого трафика с gRPC-сервера.

grpc_buffer_size

Синтаксис	`grpc_buffer_size` *размер*;
По умолчанию	`grpc_buffer_size 4k|8k;`
Контекст	http, server, location

Задает размер буфера, в который будет читаться первая часть ответа, получаемого от gRPC-сервера. Ответ синхронно передается клиенту сразу же по мере его поступления.

grpc_connect_timeout

Синтаксис	`grpc_connect_timeout` *время*;
По умолчанию	`grpc_connect_timeout 60s;`
Контекст	http, server, location

Задает таймаут для установления соединения с gRPC-сервером. Необходимо иметь в виду, что этот таймаут обычно не может превышать 75 секунд.

grpc_connection_drop

Синтаксис	`grpc_connection_drop` *время* | on | off;
По умолчанию	`grpc_connection_drop off;`
Контекст	http, server, location

Настраивает завершение всех соединений с проксируемым сервером, если он был удален из группы или помечен как постоянно недоступный в результате процесса *reresolve* или *команды API* `DELETE`.

Соединение завершается, когда обрабатывается следующее событие чтения или записи для клиента или проксируемого сервера.

Установка *времени* включает *таймаут* до завершения соединения; при выборе значения `on` соединения завершаются немедленно.

grpc_hide_header

Синтаксис	`grpc_hide_header` *поле*;
По умолчанию	—
Контекст	http, server, location

По умолчанию Angie PRO не передает клиенту поля заголовка «Date», «Server» и «X-Accel-...» из ответа gRPC-сервера. Директива *grpc_hide_header* задает дополнительные поля, которые не будут передаваться. Если же передачу полей нужно разрешить, можно воспользоваться директивой *grpc_pass_header*.

grpc_ignore_headers

Синтаксис	`grpc_ignore_headers` *поле* ...;
По умолчанию	—
Контекст	http, server, location

Запрещает обработку некоторых полей заголовка из ответа gRPC-сервера. В директиве можно указать поля «X-Accel-Redirect» и «X-Accel-Charset».

Если не запрещено, обработка этих полей заголовка заключается в следующем:

- «X-Accel-Redirect» производит *внутреннее перенаправление* на указанный URI;

- «X-Accel-Charset» задает желаемую *кодировку* ответа.

grpc_intercept_errors

Синтаксис	`grpc_intercept_errors` on | off;
По умолчанию	`grpc_intercept_errors off;`
Контекст	http, server, location

Определяет, передавать ли клиенту ответы gRPC-сервера с кодом больше либо равным 300, или же перехватывать их и перенаправлять на обработку Angie PRO с помощью директивы *error_page*.

grpc_next_upstream

Синтаксис	`grpc_next_upstream` error | timeout | invalid_header | http_500 | http_502 | http_503 | http_504 | http_403 | http_404 | http_429 | non_idempotent | off ...;
По умолчанию	`grpc_next_upstream error timeout;`
Контекст	http, server, location

Определяет, в каких случаях запрос будет передан следующему в группе *upstream* серверу:

`error`	произошла ошибка соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`timeout`	произошел таймаут во время соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`invalid_header`	сервер вернул пустой или неверный ответ;
`http_500`	сервер вернул ответ с кодом 500;
`http_502`	сервер вернул ответ с кодом 502;
`http_503`	сервер вернул ответ с кодом 503;
`http_504`	сервер вернул ответ с кодом 504;
`http_403`	сервер вернул ответ с кодом 403;
`http_404`	сервер вернул ответ с кодом 404;
`http_429`	сервер вернул ответ с кодом 429;
`non_idempotent`	обычно запросы с неидемпотентным методом (*POST*, *LOCK*, *PATCH*) не передаются на другой сервер, если запрос серверу группы уже был отправлен; включение параметра явно разрешает повторять подобные запросы;
`off`	запрещает передачу запроса следующему серверу.

Примечание

Необходимо понимать, что передача запроса следующему серверу возможна только при условии, что клиенту еще ничего не передавалось. То есть, если ошибка или таймаут возникли в середине передачи ответа клиенту, то действие директивы на такой запрос не распространяется.

Директива также определяет, что считается *неудачной попыткой* работы с сервером.

`error timeout invalid_header`	всегда считаются неудачными попытками, даже если они не указаны в директиве
`http_500 http_502 http_503 http_504 http_429`	считаются неудачными попытками, только если они указаны в директиве
`http_403 http_404`	никогда не считаются неудачными попытками

Передача запроса следующему серверу может быть ограничена по *количеству попыток* и по *времени*.

grpc_next_upstream_timeout

Синтаксис	`grpc_next_upstream_timeout` *время*;
По умолчанию	`grpc_next_upstream_timeout 0;`
Контекст	http, server, location

Ограничивает время, в течение которого возможна передача запроса *следующему* серверу.

`0`	отключает это ограничение

grpc_next_upstream_tries

Синтаксис	`grpc_next_upstream_tries` *число*;
По умолчанию	`grpc_next_upstream_tries 0;`
Контекст	http, server, location

Ограничивает число допустимых попыток для передачи запроса *следующему* серверу.

`0`	отключает это ограничение

grpc_pass

Синтаксис	`grpc_pass` *адрес*;
По умолчанию	—
Контекст	location, if в location

Задает адрес gRPC-сервера. Адрес может быть указан в виде доменного имени или IP-адреса, и порта:

```
grpc_pass localhost:9000;
```

или в виде пути UNIX-сокета:

```
grpc_pass unix:/tmp/grpc.socket;
```

Также может использоваться схема «*grpc://*»:

```
grpc_pass grpc://127.0.0.1:9000;
```

Для использования gRPC по SSL необходимо использовать схему «*grpcs://*»:

```
grpc_pass grpcs://127.0.0.1:443;
```

Если доменному имени соответствует несколько адресов, то все они будут использоваться по очереди (round-robin). Кроме того, в качестве адреса можно указать *группу серверов*. Если используется группа, указать порт невозможно; вместо этого укажите порт для каждого сервера внутри группы отдельно.

В значении параметра можно использовать переменные. В этом случае, если адрес указан в виде доменного имени, имя ищется среди описанных групп серверов и если не найдено, то определяется с помощью *resolver*'а.

grpc_pass_header

Синтаксис	`grpc_pass_header` *поле*;
По умолчанию	—
Контекст	http, server, location

Разрешает передавать от gRPC-сервера клиенту *запрещенные для передачи* поля заголовка.

grpc_read_timeout

Синтаксис	`grpc_read_timeout` *время*;
По умолчанию	`grpc_read_timeout 60s;`
Контекст	http, server, location

Задает таймаут при чтении ответа gRPC-сервера. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями чтения. Если по истечении этого времени gRPC-сервер ничего не передаст, соединение закрывается.

grpc_send_timeout

Синтаксис	`grpc_send_timeout` *время*;
По умолчанию	`grpc_send_timeout 60s;`
Контекст	http, server, location

Задает таймаут при передаче запроса gRPC-серверу. Таймаут устанавливается не на всю передачу запроса, а только между двумя операциями записи. Если по истечении этого времени gRPC-сервер не примет новых данных, соединение закрывается.

grpc_set_header

Синтаксис	`grpc_set_header` *поле значение*;
По умолчанию	`grpc_set_header Content-Length $content_length;`
Контекст	http, server, location

Позволяет переопределять или добавлять поля заголовка запроса, *передаваемые* проксируемому серверу. В качестве *значения* можно использовать текст, переменные и их комбинации. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *grpc_set_header*.

Если значение поля заголовка — пустая строка, то поле вообще не будет передаваться gRPC-серверу:

```
grpc_set_header Accept-Encoding "";
```

grpc_socket_keepalive

Синтаксис	`grpc_socket_keepalive` on | off;
По умолчанию	`grpc_socket_keepalive off;`
Контекст	http, server, location

Конфигурирует поведение «TCP keepalive» для исходящих соединений к проксируемому серверу.

`""`	По умолчанию для сокета действуют настройки операционной системы.
`on`	для сокета включается параметр *SO_KEEPALIVE*

grpc_ssl_certificate

Синтаксис	`grpc_ssl_certificate` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с сертификатом в формате PEM для аутентификации на gRPC SSL-сервере. В имени файла можно использовать переменные.

grpc_ssl_certificate_key

Синтаксис	`grpc_ssl_certificate_key` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с секретным ключом в формате PEM для аутентификации на gRPC SSL-сервере.

Вместо файла можно указать значение «engine:*имя*:id», которое загружает ключ с указанным *id* из OpenSSL engine с заданным именем.

В имени файла можно использовать переменные.

grpc_ssl_ciphers

Синтаксис	`grpc_ssl_ciphers` *шифры*;
По умолчанию	`grpc_ssl_ciphers DEFAULT;`
Контекст	http, server, location

Описывает разрешенные шифры для запросов к gRPC SSL-серверу. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL.

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

grpc_ssl_conf_command

Синтаксис	`grpc_ssl_conf_command` *имя значение*;
По умолчанию	—
Контекст	http, server, location

Задает произвольные конфигурационные команды OpenSSL при установлении соединения с gRPC SSL-сервером.

Важно

Директива поддерживается при использовании OpenSSL 1.0.2 и выше.

На одном уровне может быть указано несколько директив *grpc_ssl_conf_command*. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *grpc_ssl_conf_command*.

Осторожно

Следует учитывать, что изменение настроек OpenSSL напрямую может привести к неожиданному поведению.

grpc_ssl_crl

Синтаксис	`grpc_ssl_crl` *файл*;
По умолчанию	—
Контекст	http, server, location

Указывает файл с отозванными сертификатами (CRL) в формате PEM, используемыми при *проверке* сертификата gRPC SSL-сервера.

grpc_ssl_name

Синтаксис	`grpc_ssl_name` *имя*;
По умолчанию	`grpc_ssl_name` `имя хоста` из grpc_pass;`
Контекст	http, server, location

Позволяет переопределить имя сервера, используемое при *проверке* сертификата gRPC SSl-сервера, а также для *передачи его через SNI* при установлении соединения с gRPC SSL-сервером.

По умолчанию используется имя хоста из *grpc_pass*.

grpc_ssl_password_file

Синтаксис	`grpc_ssl_password_file` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с паролями от *секретных ключей*, где каждый пароль указан на отдельной строке. Пароли применяются по очереди в момент загрузки ключа.

grpc_ssl_protocols

Синтаксис	`grpc_ssl_protocols` [SSLv2] [SSLv3] [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`grpc_ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;`
Контекст	http, server, location

Изменено в версии 1.2.0: Параметр `TLSv1.3` добавлен к используемым по умолчанию.

Разрешает указанные протоколы для запросов к gRPC SSL-серверу.

grpc_ssl_server_name

Синтаксис	`grpc_ssl_server_name` on | off;
По умолчанию	`grpc_ssl_server_name off;`
Контекст	http, server, location

Разрешает или запрещает передачу имени сервера, заданного директивой *grpc_ssl_name*, через расширение Server Name Indication протокола TLS (SNI, RFC 6066) при установлении соединения с SSL-сервером gRPC.

grpc_ssl_session_reuse

Синтаксис	`grpc_ssl_session_reuse` on | off;
По умолчанию	`grpc_ssl_session_reuse on;`
Контекст	http, server, location

Определяет, использовать ли повторно SSL-сессии при работе с gRPC-сервером. Если в логах появляются ошибки «*SSL3_GET_FINISHED:digest check failed*», то можно попробовать выключить повторное использование сессий.

grpc_ssl_trusted_certificate

Синтаксис	`grpc_ssl_trusted_certificate` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с доверенными сертификатами CA в формате PEM, используемыми при *проверке* сертификата gRPC SSL-сервера.

grpc_ssl_verify

Синтаксис	`grpc_ssl_verify` on | off;
По умолчанию	`grpc_ssl_verify off;`
Контекст	http, server, location

Разрешает или запрещает проверку сертификата gRPC SSL-сервера.

grpc_ssl_verify_depth

Синтаксис	`grpc_ssl_verify_depth` *число*;
По умолчанию	`grpc_ssl_verify_depth 1;`
Контекст	http, server, location

Устанавливает глубину проверки в цепочке сертификатов gRPC SSL-сервера.

GunZIP

Фильтр, распаковывающий ответы с «Content-Encoding: gzip» для тех клиентов, которые не поддерживают метод сжатия «gzip». Модуль будет полезен, когда данные желательно хранить сжатыми для экономии места и сокращения затрат на ввод-вывод.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_gunzip_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
location /storage/ {
    gunzip on;
#    ...
}
```

Директивы

gunzip

Синтаксис	`gunzip` on | off;
По умолчанию	`gunzip off;`
Контекст	http, server, location

Разрешает или запрещает распаковку ответов, сжатых методом gzip, для тех клиентов, которые его не поддерживают. Если разрешено, то для определения, поддерживает ли клиент gzip, также учитываются следующие директивы: *gzip_http_version*, *gzip_proxied* и *gzip_disable*. См. также директиву *gzip_vary*.

gunzip_buffers

Синтаксис	`gunzip_buffers` *число размер*;
По умолчанию	`gunzip_buffers 32 4k|16 8k;`
Контекст	http, server, location

Задает число и размер буферов, в которые будет разжиматься ответ. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

GZip

Фильтр, сжимающий ответ методом gzip, что позволяет уменьшить размер передаваемых данных в 2 и более раз.

Осторожно

При использовании протокола SSL/TLS сжатые ответы могут быть подвержены атакам BREACH.

Пример конфигурации

```
gzip            on;
gzip_min_length 1000;
gzip_proxied    expired no-cache no-store private auth;
gzip_types      text/plain application/xml;
```

Для записи в лог достигнутого коэффициента сжатия можно использовать переменную *$gzip_ratio*.

Директивы

gzip

Синтаксис	`gzip` on | off;
По умолчанию	`gzip off;`
Контекст	http, server, location, if в location

Разрешает или запрещает сжатие ответа методом gzip.

gzip_buffers

Синтаксис	`gzip_buffers` *число размер*;
По умолчанию	`gzip_buffers 32 4k|16 8k;`
Контекст	http, server, location

Задает число и размер буферов, в которые будет сжиматься ответ. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

gzip_comp_level

Синтаксис	`gzip_comp_level` *степень*;
По умолчанию	`gzip_comp_level 1;`
Контекст	http, server, location

Устанавливает степень сжатия ответа методом gzip. Допустимые значения находятся в диапазоне от 1 до 9.

gzip_disable

Синтаксис	`gzip_disable` *regex ...*;
По умолчанию	—
Контекст	http, server, location

Запрещает сжатие ответа методом gzip для запросов с полями заголовка «User-Agent», совпадающими с заданными регулярными выражениями.

Специальная маска `msie6` соответствует регулярному выражению «*MSIE [4-6].*», но работает быстрее. Из этой маски исключается «*MSIE 6.0; ... SV1*».

gzip_http_version

Синтаксис	`gzip_http_version` 1.0 | 1.1;
По умолчанию	`gzip_http_version 1.1;`
Контекст	http, server, location

Устанавливает минимальную HTTP-версию запроса, необходимую для сжатия ответа.

gzip_min_length

Синтаксис	`gzip_min_length` *длина*;
По умолчанию	`gzip_min_length 20;`
Контекст	http, server, location

Устанавливает минимальную длину ответа, который будет сжиматься методом gzip. Длина определяется только из поля «Content-Length» заголовка ответа.

gzip_proxied

Синтаксис	`gzip_proxied` off | expired | no-cache | no-store | private | no_last_modified | no_etag | auth | any ...;
По умолчанию	`gzip_proxied off;`
Контекст	http, server, location

Разрешает или запрещает сжатие ответа методом gzip для проксированных запросов в зависимости от запроса и ответа. То, что запрос проксированный, определяется на основании наличия поля «Via» в заголовке запроса. В директиве можно указать одновременно несколько параметров:

`off`	запрещает сжатие для всех проксированных запросов, игнорируя остальные параметры;
`expired`	разрешает сжатие, если в заголовке ответа есть поле «Expires» со значением, запрещающим кэширование;
`no-cache`	разрешает сжатие, если в заголовке ответа есть поле «Cache-Control» с параметром «no-cache»;
`no-store`	разрешает сжатие, если в заголовке ответа есть поле «Cache-Control» с параметром «no-store»;
`private`	разрешает сжатие, если в заголовке ответа есть поле «Cache-Control» с параметром «private»;
`no_last_modified`	разрешает сжатие, если в заголовке ответа нет поля «Last-Modified»;
`no_etag`	разрешает сжатие, если в заголовке ответа нет поля «ETag»;
`auth`	разрешает сжатие, если в заголовке запроса есть поле «Authorization»;
`any`	разрешает сжатие для всех проксированных запросов.

gzip_types

Синтаксис	`gzip_types` mime-*тип* ...;
По умолчанию	`gzip_types text/html;`
Контекст	http, server, location

Разрешает сжатие ответа методом gzip для указанных MIME-типов в дополнение к «*text/html*». Специальное значение «*» соответствует любому MIME-типу. Ответы с типом «*text/html*» сжимаются всегда.

gzip_vary

Синтаксис	`gzip_vary` on | off;
По умолчанию	`gzip_vary off;`
Контекст	http, server, location

Разрешает или запрещает выдавать в ответе поле заголовка «Vary: Accept-Encoding», если активны директивы *gzip*, *gzip_static* или *gunzip*.

Встроенные переменные

`$gzip_ratio`

достигнутый коэффициент сжатия — отношение размера исходного ответа к размеру сжатого.

GZip Static

Позволяет отдавать вместо обычного файла предварительно сжатый файл с таким же именем и с расширением «.gz».

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_gzip_static_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
gzip_static  on;
gzip_proxied expired no-cache no-store private auth;
```

Директивы

gzip_static

Синтаксис	`gzip_static` on | off | always;
По умолчанию	`gzip_static off;`
Контекст	http, server, location

Разрешает (`on`) или запрещает (`off`) проверку готового сжатого файла. При использовании также учитываются директивы *gzip_http_version*, *gzip_proxied*, *gzip_disable* и *gzip_vary*.

Со значением `always` во всех случаях будет использоваться сжатый файл, без проверки поддержки на стороне клиента. Это полезно, если на диске все равно нет несжатых файлов, или используется модуль *GunZIP*.

Сжимать файлы можно с помощью программы gzip или совместимой с ней. Желательно, чтобы дата и время модификации исходного и сжатого файлов совпадали.

Headers

Позволяет выдавать поля заголовка «Expires» и «Cache-Control», а также добавлять произвольные поля в заголовок ответа.

Пример конфигурации

```
expires    24h;
expires    modified +24h;
expires    @24h;
expires    0;
expires    -1;
expires    epoch;
expires    $expires;
add_header Cache-Control private;
```

Директивы

add_header

Синтаксис	`add_header` *имя значение* [always];
По умолчанию	—
Контекст	http, server, location, if в location

Добавляет указанное поле в заголовок ответа при условии, что код ответа равен 200, 201 (1.3.10), 204, 206, 301, 302, 303, 304, 307 или 308. В значении параметра можно использовать переменные.

Директив *add_header* может быть несколько. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *add_header*.

Если указан параметр `always`, то поле заголовка будет добавлено независимо от кода ответа.

add_trailer

Синтаксис	`add_trailer` *имя значение* [always];
По умолчанию	—
Контекст	http, server, location, if в location

Добавляет указанное поле в конец ответа при условии, что код ответа равен 200, 201, 206, 301, 302, 303, 307 или 308. В значении можно использовать переменные.

Директив *add_trailer* может быть несколько. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *add_trailer*.

Если указан параметр `always`, то указанное поле будет добавлено независимо от кода ответа.

expires

Синтаксис	`expires` [modified] *время*; `expires` epoch | max | off;
По умолчанию	`expires off;`
Контекст	http, server, location, if в location

Разрешает или запрещает добавлять или менять поля «Expires» и «Cache-Control» в заголовке ответа при условии, что код ответа равен 200, 201, 204, 206, 301, 302, 303, 304, 307 или 308. В качестве параметра можно задать положительное или отрицательное *время*.

Время в поле «Expires» получается как сумма текущего времени и времени, заданного в директиве. Если используется параметр `modified`, то время получается как сумма времени модификации файла и времени, заданного в директиве.

Кроме того, с помощью префикса «@» можно задать время суток:

```
expires @15h30m;
```

Содержимое поля «Cache-Control» зависит от знака заданного времени:

- отрицательное время — «Cache-Control: no-cache».
- положительное или равное нулю время — «Cache-Control: max-age=`t`», где t это время в секундах, заданное в директиве.

`epoch`	задает время «Thu, 01 Jan 1970 00:00:01 GMT» (1 января 1970 00:00:01 GMT) для поля «Expires» и «no-cache» для поля «Cache-Control».
`max`	задает время «Thu, 31 Dec 2037 23:55:55 GMT» (31 декабря 2037 23:55:55 GMT) для поля «Expires» и 10 лет для поля «Cache-Control».
`off`	запрещает добавлять или менять поля «Expires» и «Cache-Control» в заголовке ответа.

В значении последнего параметра можно использовать переменные:

```
map $sent_http_content_type $expires {
    default          off;
    application/pdf 42d;
    ~image/          max;
}

expires $expires;
```

Image Filter

Фильтр для преобразования изображений в форматах JPEG, GIF, PNG и WebP.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_image_filter_module`.

В наших репозиториях модуль собран динамически и доступен отдельным пакетом *angie-pro-module-image-filter*.

Важно

Для этого модуля необходима библиотека libgd. Рекомендуется использовать самую последнюю версию библиотеки.

Для преобразования изображений в формате WebP библиотека *libgd* должна быть собрана с поддержкой WebP.

Пример конфигурации

```
location /img/ {
    proxy_pass   http://backend;
    image_filter resize 150 100;
    image_filter rotate 90;
    error_page   415 = /empty;
}

location = /empty {
    empty_gif;
}
```

Директивы

image_filter

Синтаксис	`image_filter` **off;** `image_filter` test; `image_filter` size; `image_filter` rotate 90 | 180 | 270; `image_filter` resize *ширина высота*; `image_filter` crop *ширина высота*;
По умолчанию	`image_filter off;`
Контекст	location

Задает тип преобразования изображения:

`off`	отключает обработку данным модулем во вложенном location.
`test`	проверяет, что ответ действительно является изображением в формате JPEG, GIF, PNG или WebP. В противном случае возвращается ошибка 415 (Unsupported Media Type).
`size`	**выдает информацию об изображении в формате JSON, например:** { «img» : { «width»: 100, «height»: 100, «type»: «gif» } } **В случае ошибки выдается** {}
`rotate 90|180|270`	поворачивает изображение против часовой стрелки на указанное число градусов. В значении параметра допустимо использование переменных. Можно использовать как отдельно, так и совместно с преобразованиями *resize* и *crop*.
`resize` *ширина высота*	пропорционально уменьшает изображение до указанных размеров. Если требуется уменьшить только по одному измерению, то в качестве второго можно указать «-». В случае ошибки сервер возвращает код 415 (Unsupported Media Type). В значениях параметров допустимо использование переменных. При использовании совместно с *rotate*, поворот изображения происходит **после** уменьшения размеров изображения.
`crop` *ширина высота*	пропорционально уменьшает изображение до размера большей стороны и обрезает лишние края по другой стороне. Если требуется уменьшить только по одному измерению, то в качестве второго можно указать «-». В случае ошибки сервер возвращает код 415 (Unsupported Media Type). В значениях параметров допустимо использование переменных. При использовании совместно с rotate, поворот изображения происходит **до** уменьшения размеров изображения.

image_filter_buffer

Синтаксис	`image_filter_buffer` *размер*;
По умолчанию	`image_filter_buffer 1M;`
Контекст	http, server, location

Задает максимальный размер буфера для чтения изображения. При превышении размера сервер вернет ошибку 415 (Unsupported Media Type).

image_filter_interlace

Синтаксис	`image_filter_interlace` on | off;
По умолчанию	`image_filter_interlace off;`
Контекст	http, server, location

Если включено, то итоговые изображения будут с чересстрочностью. В случае JPEG итоговые изображения будут в формате «progressive JPEG».

image_filter_jpeg_quality

Синтаксис	`image_filter_jpeg_quality` *качество*;
По умолчанию	`image_filter_jpeg_quality 75;`
Контекст	http, server, location

Задает желаемое качество преобразованного изображения в формате JPEG. Допустимые значения находятся в диапазоне от 1 до 100. Меньшим значениям обычно соответствует худшее качество изображения и меньший объем передаваемых данных. Максимальное рекомендуемое значение — 95. В значении параметра допустимо использование переменных.

image_filter_sharpen

Синтаксис	`image_filter_sharpen` *процент*;
По умолчанию	`image_filter_sharpen 0;`
Контекст	http, server, location

Повышает резкость итогового изображения. Процент резкости может быть больше 100. Значение `0` отключает повышение резкости. В значении параметра допустимо использование переменных.

image_filter_transparency

Синтаксис	`image_filter_transparency` on | off;
По умолчанию	`image_filter_transparency on;`
Контекст	http, server, location

Определяет, сохранять ли прозрачность при обработке изображений в формате GIF и в формате PNG с цветами, заданными палитрой. Потеря прозрачности позволяет получить более качественное изображение. Прозрачность альфа-канала в формате PNG сохраняется всегда.

image_filter_webp_quality

Синтаксис	`image_filter_webp_quality` *качество*;
По умолчанию	`image_filter_webp_quality 80;`
Контекст	http, server, location

Задает желаемое качество преобразованного изображения в формате WebP. Допустимые значения находятся в диапазоне от 1 до 100. Меньшим значениям обычно соответствует худшее качество изображения и меньший объем передаваемых данных. В значении параметра допустимо использование переменных.

Index

Обслуживает запросы, оканчивающиеся косой чертой (/). Такие запросы также могут обслуживаться модулями *AutoIndex* и *Random Index*.

Пример конфигурации

```
location / {
    index index.$geo.html index.html;
}
```

Директивы

index

Синтаксис	`index` *файл* ...;
По умолчанию	`index index.html;`
Контекст	http, server, location

Определяет файлы, которые будут использоваться в качестве индекса. В имени файла можно использовать переменные. Наличие файлов проверяется в порядке их перечисления. В конце списка может стоять файл с абсолютным путем. Пример:

```
index index.$geo.html index.0.html /index.html;
```

Необходимо иметь в виду, что при использовании индексного файла делается внутреннее перенаправление и запрос может быть обработан уже в другом location'е. Например, в такой конфигурации:

```
location = / {
    index index.html;
}

location / {
#    ...
}
```

запрос "/" будет фактически обработан во втором location'е как "*/index.html*".

JS

Позволяет задавать обработчики на njs — подмножестве языка JavaScript.

В наших репозиториях модуль собран динамически и доступен отдельным пакетом *angie-pro-module-njs*; подключить его можно с помощью директивы *load_module*.

Пример конфигурации

```
http {
    js_import http.js;

    js_set $foo     http.foo;
    js_set $summary http.summary;
    js_set $hash    http.hash;

    resolver 127.0.0.53;

    server {
        listen 8000;

        location / {
            add_header X-Foo $foo;
            js_content http.baz;
        }

        location = /summary {
            return 200 $summary;
        }

        location = /hello {
            js_content http.hello;
        }

        location = /fetch {
            js_content                    http.fetch;
            js_fetch_trusted_certificate /path/to/ISRG_Root_X1.pem;
        }

        location = /crypto {
            add_header Hash $hash;
            return     200;
        }
    }
}
```

Файл `http.js`:

```
function foo(r) {
    r.log("hello from foo() handler");
    return "foo";
}

function summary(r) {
    var a, s, h;

    s = "JS summary\n\n";

    s += "Method: " + r.method + "\n";
    s += "HTTP version: " + r.httpVersion + "\n";
    s += "Host: " + r.headersIn.host + "\n";
    s += "Remote Address: " + r.remoteAddress + "\n";
    s += "URI: " + r.uri + "\n";

    s += "Headers:\n";
```

```
    for (h in r.headersIn) {
        s += "  header '" + h + "' is '" + r.headersIn[h] + "'\n";
    }

    s += "Args:\n";
    for (a in r.args) {
        s += "  arg '" + a + "' is '" + r.args[a] + "'\n";
    }

    return s;
}

function baz(r) {
    r.status = 200;
    r.headersOut.foo = 1234;
    r.headersOut['Content-Type'] = "text/plain; charset=utf-8";
    r.headersOut['Content-Length'] = 15;
    r.sendHeader();
    r.send("nginx");
    r.send("java");
    r.send("script");

    r.finish();
}

function hello(r) {
    r.return(200, "Hello world!");
}

async function fetch(r) {
    let results = await Promise.all([ngx.fetch('https://google.com/'),
                                     ngx.fetch('https://google.ru/')]);

    r.return(200, JSON.stringify(results, undefined, 4));
}

async function hash(r) {
    let hash = await crypto.subtle.digest('SHA-512', r.headersIn.host);
    r.setReturnValue(Buffer.from(hash).toString('hex'));
}

export default {foo, summary, baz, hello, fetch, hash};
```

Директивы

js_body_filter

Синтаксис	`js_body_filter` *функция* | *модуль.функция* [buffer_type=*строка* | *буфер*];
По умолчанию	—
Контекст	location, if in location, limit_except

Задает функцию njs в качестве фильтра тела ответа. Функция фильтра вызывается для каждого блока данных тела ответа со следующими аргументами:

`r`	объект HTTP request
`data`	входящий блок данных может быть строкой или буфером в зависимости от значения *buffer_type*, по умолчанию является строкой.
`flags`	объект со следующими свойствами: `last` — логическое значение `true` — если данные являются последним буфером.

Функция фильтра может передавать свою модифицированную версию входящего блока данных следующему фильтру тела ответа при помощи вызова r.sendBuffer(). Пример преобразования букв в нижний регистр в теле ответа:

```
function filter(r, data, flags) {
    r.sendBuffer(data.toLowerCase(), flags);
}
```

Для отмены фильтра (блоки данных будут передаваться клиенту без вызова *js_body_filter*), можно использовать r.done().

Если функция фильтра изменяет длину тела ответа, то необходимо очистить заголовок ответа «Content-Length» (если присутствует) в *js_header_filter*, чтобы применить поблочное кодирование.

Примечание

Так как обработчик *js_body_filter* должен сразу возвращать результат, то поддерживаются только синхронные операции, Таким образом, асинхронные операции, например r.subrequest() или setTimeout(), не поддерживаются.

js_content

Синтаксис	`js_content` *функция* | *модуль.функция*;
По умолчанию	—
Контекст	location, if in location, limit_except

Задает функцию njs в качестве обработчика содержимого location. Можно ссылаться на функцию модуля.

js_fetch_buffer_size

Синтаксис	`js_fetch_buffer_size` *размер*;
По умолчанию	`js_fetch_buffer_size 16k;`
Контекст	http, server, location

Задает размер буфера, который будет использоваться для чтения и записи для Fetch API.

js_fetch_ciphers

Синтаксис	`js_fetch_ciphers` *шифры*;
По умолчанию	`js_fetch_ciphers HIGH:!aNULL:!MD5;`
Контекст	http, server, location

Описывает разрешенные шифры для HTTPS-соединений при помощи Fetch API. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL.

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

js_fetch_max_response_buffer_size

Синтаксис	`js_fetch_max_response_buffer_size` *размер*;
По умолчанию	`js_fetch_max_response_buffer_size 1m;`
Контекст	http, server, location

Задает максимальный размер ответа, полученного при помощи Fetch API.

js_fetch_protocols

Синтаксис	`js_fetch_protocols` [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`js_fetch_protocols TLSv1 TLSv1.1 TLSv1.2;`
Контекст	http, server, location

Разрешает указанные протоколы для HTTPS-соединений при помощи Fetch API.

js_fetch_timeout

Синтаксис	`js_fetch_timeout` *время*;
По умолчанию	`js_fetch_timeout 60s;`
Контекст	http, server, location

Задает таймаут при чтении и записи при помощи Fetch API. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями чтения. Если по истечении этого времени данные не передавались, соединение закрывается.

js_fetch_trusted_certificate

Синтаксис	`js_fetch_trusted_certificate` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с доверенными сертификатами CA в формате PEM, используемыми при проверке HTTPS-сертификата при помощи Fetch API.

js_fetch_verify

Синтаксис	`js_fetch_verify` on | off;
По умолчанию	`js_fetch_verify on;`
Контекст	http, server, location

Разрешает или запрещает проверку сертификата HTTPS-сервера при помощи Fetch API.

js_fetch_verify_depth

Синтаксис	`js_fetch_verify_depth` *число*;
По умолчанию	`js_fetch_verify_depth 100;`
Контекст	http, server, location

Устанавливает глубину проверки в цепочке HTTPS-сертификатов при помощи Fetch API.

js_header_filter

Синтаксис	`js_header_filter` *функция* | *модуль.функция*;
По умолчанию	—
Контекст	location, if in location, limit_except

Задает функцию njs в качестве фильтра заголовка ответа. Директива позволяет менять произвольные поля заголовка ответа.

Примечание

Так как обработчик *js_header_filter* должен сразу возвращать результат, то поддерживаются только синхронные операции. Таким образом, асинхронные операции, например r.subrequest() или setTimeout(), не поддерживаются.

js_import

Синтаксис	`js_import` *модуль.js* | *имя_экспорта from модуль.js*;
По умолчанию	—
Контекст	http, server, location

Импортирует модуль, позволяющий задавать обработчики location и переменных на njs. *Имя_экспорта* является пространством имен при доступе к функциям модуля. Если *имя_экспорта* не задано, то пространством имен будет являться имя модуля.

```
js_import http.js;
```

В примере при доступе к экспорту в качестве пространства имен используется имя модуля *http*. Если импортируемый модуль экспортирует *foo()*, то для доступа используется *http.foo*.

Директив *js_import* может быть несколько.

js_path

Синтаксис	`js_path` *путь*;
По умолчанию	—
Контекст	http, server, location

Задает дополнительный путь для модулей njs.

js_preload_object

Синтаксис	`js_preload_object` *имя.json* | *имя from файл.json*;
По умолчанию	—
Контекст	http, server, location

Предварительно загружает неизменяемый объект во время конфигурации. *Имя* используется в качестве имени глобальной переменной, через которую объект доступен в коде njs. Если *имя* не указано, то будет использоваться имя файла.

```
js_preload_object map.json;
```

В примере *map* используется в качестве имени во время доступа к предварительно загруженному объекту.

Директив *js_preload_object* может быть несколько.

js_set

Синтаксис	`js_set` *$переменная функция* | *модуль.функция*;
По умолчанию	—
Контекст	http, server, location

Задает функцию njs для указанной переменной. Можно ссылаться на функцию модуля.

Функция вызывается в момент первого обращения к переменной для данного запроса. Точный момент вызова функции зависит от *фазы*, в которой происходит обращение к переменной. Это можно использовать для реализации дополнительной логики, не относящейся к вычислению переменной. Например, если переменная указана в директиве *log_format*, то ее обработчик не будет выполняться до фазы записи в лог. Этот обработчик также может использоваться для выполнения процедур непосредственно перед освобождением запроса.

Примечание

Так как обработчик *js_set* должен сразу возвращать результат, то поддерживаются только синхронные операции. Таким образом, асинхронные операции, например r.subrequest() или setTimeout(), не поддерживаются.

js_shared_dict_zone

Синтаксис	`js_shared_dict_zone` zone=*имя:размер* [timeout=*время*] [type=string | number] [evict];
По умолчанию	—
Контекст	http

Задает *имя* и *размер* зоны разделяемой памяти, в которой хранится словарь ключей и значений, разделяемый между рабочими процессами.

`type`	необязательный параметр, позволяет изменить тип значения на числовой (`number`), по умолчанию в качестве ключа и значения используется строка (`string`).
`timeout`	необязательный параметр, задает время, по завершении которого все записи в словаре удаляются из зоны
`evict`	необязательный параметр, удаляет самую старую пару ключ-значение при переполнении зоны

Пример:

```
example.conf:
    # Создается словарь размером 1Мб со строковыми значениями,
    # пары ключ-значение удаляются при отсутствии активности в течение 60 секунд:
    js_shared_dict_zone zone=foo:1M timeout=60s;

    # Создается словарь размером 512Кб со строковыми значениями,
    # удаляется самая старая пара ключ-значение при переполнении зоны:
    js_shared_dict_zone zone=bar:512K timeout=30s evict;
```

```
    # Создается постоянный словарь размером 32Кб с числовыми значениями:
    js_shared_dict_zone zone=num:32k type=number;
```

```
example.js:
    function get(r) {
        r.return(200, ngx.shared.foo.get(r.args.key));
    }

    function set(r) {
        r.return(200, ngx.shared.foo.set(r.args.key, r.args.value));
    }

    function delete(r) {
        r.return(200, ngx.shared.bar.delete(r.args.key));
    }

    function increment(r) {
        r.return(200, ngx.shared.num.incr(r.args.key, 2));
    }
```

js_var

Синтаксис	`js_var` *$переменная* [*значение*];
По умолчанию	—
Контекст	http, server, location

Объявляет перезаписываемую переменную. В качестве значения можно использовать текст, переменные и их комбинации. Переменная не перезаписывается после перенаправления, в отличие от переменных, созданных при помощи директивы set.

Аргумент запроса

Каждый HTTP-обработчик njs получает один аргумент, объект запроса.

Limit Conn

Позволяет ограничить число соединений по заданному ключу, в частности, число соединений с одного IP-адреса.

Учитываются не все соединения, а лишь те, в которых имеются запросы, обрабатываемые сервером, и заголовок запроса уже прочитан.

Пример конфигурации

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

    ...

    server {

        ...

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

Директивы

limit_conn

Синтаксис	`limit_conn` *зона число*;
По умолчанию	—
Контекст	http, server, location

Задает зону разделяемой памяти и максимально допустимое число соединений для одного значения ключа. При превышении этого числа в ответ на запрос сервер вернет *ошибку*. Например, директивы

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

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

разрешают одновременно обрабатывать не более одного соединения с одного IP-адреса.

> **Примечание**
>
> В HTTP/2 и SPDY каждый параллельный запрос считается отдельным соединением.

Директив *limit_conn* может быть несколько. Например, следующая конфигурация ограничивает число соединений с сервером с одного клиентского IP-адреса и в то же время ограничивает общее число соединений с виртуальным сервером:

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

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

Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *limit_ conn*.

limit_conn_dry_run

Синтаксис	`limit_conn_dry_run` on | off;
По умолчанию	`limit_conn_dry_run off;`
Контекст	http, server, location

Включает режим пробного запуска. В данном режиме число соединений не ограничивается, однако в *зоне разделяемой памяти* текущее число избыточных соединений учитывается как обычно.

limit_conn_log_level

Синтаксис	`limit_conn_log_level` info | notice | warn | error;
По умолчанию	`limit_conn_log_level error;`
Контекст	http, server, location

Задает желаемый уровень записи в лог случаев ограничения числа соединений.

limit_conn_status

Синтаксис	`limit_conn_status` *код*;
По умолчанию	`limit_conn_status 503;`
Контекст	http, server, location

Позволяет переопределить код ответа, используемый при отклонении запросов.

limit_conn_zone

Синтаксис	`limit_conn_zone` *ключ* zone = *название:размер*;
По умолчанию	—
Контекст	http

Задает параметры зоны разделяемой памяти, которая хранит состояние для разных значений ключа. Состояние в частности содержит текущее число соединений. В качестве ключа можно использовать текст, переменные и их комбинации. Запросы с пустым значением ключа не учитываются.

Пример использования:

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

Здесь в качестве ключа используется IP-адрес клиента. Обратите внимание, что вместо переменной `$remote_addr` использована переменная `$binary_remote_addr`.

Длина значения переменной *$remote_addr* может колебаться от 7 до 15 байт, при этом размер хранимого состояния составляет либо 32, либо 64 байта на 32-битных платформах и всегда 64 байта на 64-битных.

Длина значения переменной *$binary_remote_addr* всегда равна 4 байтам для IPv4-адресов или 16 байтам для IPv6-адресов. При этом размер состояния всегда равен 32 или 64 байтам на 32-битных платформах и 64 байтам на 64-битных.

В зоне размером 1 мегабайт может разместиться около 32 тысяч состояний размером 32 байта или 16 тысяч состояний размером 64 байта. При переполнении зоны в ответ на последующие запросы сервер будет возвращать *ошибку*.

Встроенные переменные

`$limit_conn_status`

хранит результат ограничения числа соединений: *PASSED*, *REJECTED* или *REJECTED_DRY_RUN*

Limit Req

Позволяет ограничить скорость обработки запросов по заданному ключу или, как частный случай, скорость обработки запросов, поступающих с одного IP-адреса. Ограничение обеспечивается с помощью метода «leaky bucket».

Пример конфигурации

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

    ...

    server {

        ...

        location /search/ {
            limit_req zone=one burst=5;
        }
```

Директивы

limit_req

Синтаксис	`limit_req` zone=*название* [burst=*число*] [nodelay | delay=*число*];
По умолчанию	—
Контекст	http, server, location

Задает зону разделяемой памяти (`zone`) и максимальный размер всплеска запросов (`burst`). Если скорость поступления запросов превышает описанную в зоне, то их обработка задерживается так, чтобы запросы обрабатывались с заданной скоростью. Избыточные запросы задерживаются

до тех пор, пока их число не превысит максимальный размер всплеска. При превышении запрос завершается с ошибкой. По умолчанию максимальный размер всплеска равен нулю. Например, директивы

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

server {
    location /search/ {
        limit_req zone=one burst=5;
    }
```

позволяют в среднем не более 1 запроса в секунду со всплесками не более 5 запросов.

Если же избыточные запросы в пределах лимита всплесков задерживать не требуется, то следует использовать параметр `nodelay`:

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

Параметр `delay` задает лимит, по достижении которого избыточные запросы задерживаются. Значение по умолчанию равно нулю и означает, что задерживаются все избыточные запросы.

Директив *limit_ req* может быть несколько. Например, следующая конфигурация ограничивает скорость обработки запросов, поступающих с одного IP-адреса, и в то же время ограничивает скорость обработки запросов одним виртуальным сервером:

```
limit_req_zone $binary_remote_addr zone=perip:10m rate=1r/s;
limit_req_zone $server_name zone=perserver:10m rate=10r/s;

server {
    ...
    limit_req zone=perip burst=5 nodelay;
    limit_req zone=perserver burst=10;
}
```

Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *limit_ req*.

limit_req_dry_run

Синтаксис	`limit_req_dry_run` on | off;
По умолчанию	`limit_req_dry_run off;`
Контекст	http, server, location

Включает режим пробного запуска. В данном режиме скорость обработки запросов не ограничивается, однако в *зоне разделяемой памяти* текущее число избыточных запросов учитывается как обычно.

limit_req_log_level

Синтаксис	`limit_req_log_level` info | notice | warn | error;
По умолчанию	`limit_req_log_level error;`
Контекст	http, server, location

Задает желаемый уровень записи в лог случаев отказа в обработке запросов при превышении скорости и случаев задержек при обработке запроса. Задержки записываются в лог с уровнем на единицу меньшим, чем отказы, например, если указано *limit_req_log_level notice;*, то задержки будут записываться в лог на уровне *info*.

limit_req_status

Синтаксис	`limit_req_status` *код*;
По умолчанию	`limit_req_status 503;`
Контекст	http, server, location

Позволяет переопределить код ответа, используемый при отклонении запросов.

limit_req_zone

Синтаксис	`limit_req_zone` *ключ* zone=*название:размер* rate=*скорость*;
По умолчанию	—
Контекст	http

Задает параметры зоны разделяемой памяти, которая хранит состояние для разных значений ключа. Состояние в частности хранит текущее число избыточных запросов. В качестве ключа можно использовать текст, переменные и их комбинации. Запросы с пустым значением ключа не учитываются.

Пример использования:

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

В данном случае состояния хранятся в зоне `one` размером 10 мегабайт, и средняя скорость обработки запросов для этой зоны не может превышать 1 запроса в секунду.

В качестве ключа используется IP-адрес клиента. Обратите внимание, что вместо переменной `$remote_addr` используется переменная `$binary_remote_addr`.

Длина значения переменной *$binary_remote_addr* всегда равна 4 байтам для IPv4-адресов или 16 байтам для IPv6-адресов. При этом размер состояния всегда равен 64 байтам на 32-битных платформах и 128 байтам на 64-битных платформах.

В зоне размером 1 мегабайт может разместиться около 16 тысяч состояний размером 64 байта или около 8 тысяч состояний размером 128 байт.

При переполнении зоны удаляется наименее востребованное состояние. Если и это не позволяет создать новое состояние, запрос завершается с *ошибкой*.

Скорость `rate` задается в запросах в секунду (r/s). Если же нужна скорость меньше одного запроса в секунду, то она задается в запросах в минуту (r/m), например, ползапроса в секунду — это 30r/m.

Встроенные переменные

`$limit_req_status`

хранит результат ограничения скорости поступления запросов: *PASSED*, *DELAYED*, *REJECTED*, *DELAYED_DRY_RUN* или *REJECTED_DRY_RUN*

Log

Модуль записывает логи запросов в указанном формате.

Логи записываются в контексте *location*'а, где заканчивается обработка. Это может быть *location*, отличный от первоначального, если в процессе обработки запроса происходит *внутреннее перенаправление*.

Пример конфигурации

```
log_format compression '$remote_addr - $remote_user [$time_local] '
                       '"$request" $status $bytes_sent '
                       '"$http_referer" "$http_user_agent" "$gzip_ratio"';

access_log /spool/logs/angie-access.log compression buffer=32k;
```

Директивы

access_log

Синтаксис	`access_log` *путь* [*формат* [buffer=*размер*] [gzip[=*степень*]] [flush=*время*] [if=*условие*]]; `access_log` off;
По умолчанию	`access_log logs/access.log combined;`
Контекст	http, server, location, if в location, limit_except

Задает *путь*, *формат* и настройки буферизованной записи в лог. На одном уровне конфигурации может использоваться несколько логов. Запись в *syslog* настраивается указанием префикса *«syslog:»* в первом параметре. Специальное значение *off* отменяет все директивы *access_log* для текущего уровня. Если формат не указан, то используется предопределенный формат *«combined»*.

Если задан размер буфера с помощью параметра *buffer* или указан параметр *gzip*, то запись будет буферизованной.

> **Осторожно**
>
> Размер буфера должен быть не больше размера атомарной записи в дисковый файл. Для FreeBSD этот размер неограничен.

При включенной буферизации данные записываются в файл:

- если очередная строка лога не помещается в буфер;
- если данные в буфере находятся дольше интервала времени, заданного параметром *flush*;

- при *переоткрытии лог-файла* или завершении рабочего процесса.

Если задан параметр *gzip*, то буфер будет сжиматься перед записью в файл. Степень сжатия может быть задана в диапазоне от *1* (быстрее, но хуже сжатие) до *9* (медленнее, но лучше сжатие). По умолчанию используются буфер размером *64K* байт и степень сжатия *1*. Данные сжимаются атомарными блоками, и в любой момент времени лог-файл может быть распакован или прочитан с помощью утилиты *«zcat»*.

Пример:

```
access_log /path/to/log.gz combined gzip flush=5m;
```

Важно

Для поддержки gzip-сжатия логов Angie PRO должен быть собран с библиотекой *zlib*.

В пути файла можно использовать переменные, но такие логи имеют некоторые ограничения:

- *пользователь*, с правами которого работают рабочие процессы, должен иметь права на создание файлов в каталоге с такими логами;
- не работает буферизация;
- файл открывается для каждой записи в лог и сразу же после записи закрывается. Следует однако иметь в виду, что поскольку дескрипторы часто используемых файлов могут храниться в кэше, то при ротации логов в течение времени, заданного параметром *valid* директивы *open_log_file_cache*, запись может продолжаться в старый файл.
- при каждой записи в лог проверяется существование корневого каталога для запроса — если этот каталог не существует, то лог не создается. Поэтому *root* и *access_log* нужно описывать на одном уровне конфигурации:

```
server {
    root       /spool/vhost/data/$host;
    access_log /spool/vhost/logs/$host;
    ...
```

Параметр *if* включает условную запись в лог. Запрос не будет записываться в лог, если результатом вычисления условия является *«0»* или пустая строка. В следующем примере запросы с кодами ответа 2xx и 3xx не будут записываться в лог:

```
map $status $loggable {
    ~^[23]  0;
    default 1;
}

access_log /path/to/access.log combined if=$loggable;
```

log_format

Синтаксис	`log_format` *имя* [escape=default | json | none] *строка* ...;
По умолчанию	`log_format combined "...";`
Контекст	http

Задает формат лога.

Параметр *escape* позволяет задать экранирование символов *json* или *default* в переменных, по умолчанию используется *default*. Значение *none* отключает экранирование символов.

При использовании *default* символы «"», «\», а также символы со значениями меньше 32 или больше 126 экранируются как «\xXX». Если значение переменной не найдено, то в качестве значения в лог будет записываться дефис «-«.

При использовании *json* экранируются все символы, недопустимые в JSON строках: символы «"» и «\» экранируются как «\"» и «\\», символы со значениями меньше 32 экранируются как «\n», «\r», «\t», «\b», «\f» или «\u00XX».

Строки заголовка, переданные клиенту, начинаются с префикса *sent_http_*, например, *$sent_http_content_range*.

В конфигурации всегда существует предопределенный формат *combined*:

```
log_format combined '$remote_addr - $remote_user [$time_local] '
                    '"$request" $status $body_bytes_sent '
                    '"$http_referer" "$http_user_agent"';
```

open_log_file_cache

Синтаксис	`open_log_file_cache` max=*N* [inactive=*время*] [min_uses=*N*] [valid=*время*]; `open_log_file_cache` off;
По умолчанию	`open_log_file_cache off;`
Контекст	http, server, location

Задает кэш, в котором хранятся дескрипторы файлов часто используемых логов, имена которых заданы с использованием переменных. Параметры:

`max`	задает максимальное число дескрипторов в кэше; при переполнении кэша наименее востребованные (LRU) дескрипторы закрываются
`inactive`	задает время, после которого кэшированный дескриптор закрывается, если к нему не было обращений в течение этого времени; по умолчанию 10 секунд
`min_uses`	задает минимальное число использований файла в течение времени, заданного параметром *inactive*, после которого дескриптор файла будет оставаться открытым в кэше; по умолчанию 1
`valid`	задает, через какое время нужно проверять, что файл еще существует под тем же именем; по умолчанию 60 секунд
`off`	запрещает кэш

Пример использования:

```
open_log_file_cache max=1000 inactive=20s valid=1m min_uses=2;
```

Map

Создает переменные, значения которых зависят от значений других переменных.

Пример конфигурации

```
map $http_host $name {
    hostnames;

    default       0;

    example.com   1;
    *.example.com 1;
    example.org   2;
    *.example.org 2;
    .example.net  3;
    wap.*         4;
}

map $http_user_agent $mobile {
    default       0;
    "~Opera Mini" 1;
}
```

Директивы

map

Синтаксис	`map` *строка* *$переменная* { ... };
По умолчанию	—
Контекст	http

Создает новую переменную. Ее значение зависит от первого параметра, заданного строкой с переменными, например:

```
set $var1 "foo";
set $var2 "bar";

map $var1$var2 $new_variable {
    default "foobar_value";
}
```

Здесь переменная `$new_variable` будет иметь значение, составленное из двух переменных `$var1` и `$var2`, или значение по умолчанию, если эти переменные не определены.

Примечание

Поскольку переменные вычисляются только в момент использования, само по себе наличие даже большого числа объявлений переменных «map» не влечет за собой никаких дополнительных расходов на обработку запросов.

Параметры внутри блока *map* задают соответствие между исходными и результирующими значениями.

Исходные значения задаются строками или регулярными выражениями.

Строки проверяются без учета регистра.

Перед регулярным выражением ставится символ «~», если при сравнении следует учитывать регистр символов, либо символы «~*», если регистр символов учитывать не нужно. Регулярное выражение может содержать именованные и позиционные выделения, которые могут затем использоваться в других директивах совместно с результирующей переменной.

Если исходное значение совпадает с именем одного из специальных параметров, описанных ниже, перед ним следует поставить символ «\".

В качестве результирующего значения можно указать текст, переменную и их комбинации.

Также поддерживаются следующие специальные параметры:

`default` *значение*	задает результирующее значение, если исходное значение не совпадает ни с одним из перечисленных. Если параметр *default* не указан, результирующим значением по умолчанию будет пустая строка.
`hostnames`	указывает, что в качестве исходных значений можно использовать маску для первой или последней части имени хоста. Этот параметр следует указывать перед списком значений.

Например,

```
*.example.com 1;
example.*     1;
```

Вместо двух записей

```
example.com   1;
*.example.com 1;
```

можно использовать одну:

```
.example.com  1;
```

`include` *файл*	включает файл со значениями. Включений может быть несколько.
`volatile`	указывает, что переменная не кэшируется.

Если исходному значению соответствует несколько из указанных вариантов, например, одновременно подходят и маска, и регулярное выражение, будет выбран первый подходящий вариант в следующем порядке приоритета:

1. строковое значение без маски
2. самое длинное строковое значение с маской в начале, например «**.example.com*»
3. самое длинное строковое значение с маской в конце, например «*mail.**»
4. первое подходящее регулярное выражение (в порядке следования в конфигурационном файле)
5. значение по умолчанию (*default*)

map_hash_bucket_size

Синтаксис	`map_hash_bucket_size` *размер*;
По умолчанию	`map_hash_bucket_size 32|64|128;`
Контекст	http

Задает размер корзины в хэш-таблицах для переменных *map*. Значение по умолчанию зависит от размера строки кэша процессора. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

map_hash_max_size

Синтаксис	`map_hash_max_size` *размер*;
По умолчанию	`map_hash_max_size 2048;`
Контекст	http

Задает максимальный размер хэш-таблиц для переменных *map*. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

Memcached

Позволяет получать ответ из сервера memcached. Ключ задается в переменной *$memcached_key*. Ответ в memcached должен быть предварительно помещен внешним по отношению к Angie PRO способом.

Пример конфигурации

```
server {
    location / {
        set             $memcached_key "$uri?$args";
        memcached_pass host:11211;
        error_page      404 502 504 = @fallback;
    }

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

Директивы

memcached_bind

Синтаксис	`memcached_bind` *адрес* [transparent] | off;
По умолчанию	—
Контекст	http, server, location

Задает локальный IP-адрес с необязательным портом, который будет использоваться в исходящих соединениях с сервером memcached. В значении параметра допустимо использование переменных. Специальное значение `off` отменяет действие унаследованной с предыдущего уровня конфигурации директивы *memcached_bind*, позволяя системе самостоятельно выбирать локальный IP-адрес и порт.

Параметр `transparent` позволяет задать нелокальный IP-адрес, который будет использоваться в исходящих соединениях с проксируемым сервером, например, реальный IP-адрес клиента:

```
memcached_bind $remote_addr transparent;
```

Для работы параметра обычно требуется запустить рабочие процессы Angie PRO с привилегиями *суперпользователя*. В Linux это не требуется, так как если указан параметр *transparent*, то рабочие процессы наследуют *capability CAP_NET_RAW* из главного процесса.

Важно

Необходимо настроить таблицу маршрутизации ядра для перехвата сетевого трафика с сервера memcached.

memcached_buffer_size

Синтаксис	`memcached_buffer_size` *размер*;
По умолчанию	`memcached_buffer_size 4k|8k;`
Контекст	http, server, location

Задает размер буфера, в который будет читаться первая часть ответа, получаемого от сервера memcached. Ответ синхронно передается клиенту сразу же по мере его поступления.

memcached_connect_timeout

Синтаксис	`memcached_connect_timeout` *время*;
По умолчанию	`memcached_connect_timeout 60s;`
Контекст	http, server, location

Задает таймаут для установления соединения с сервером memcached. Необходимо иметь в виду, что этот таймаут обычно не может превышать 75 секунд.

memcached_gzip_flag

Синтаксис	`memcached_gzip_flag` *флаг*;
По умолчанию	—
Контекст	http, server, location

Включает проверку указанного флага в ответе сервера memcached и установку поля «Content-Encoding» заголовка ответа в «gzip», если этот флаг установлен.

memcached_next_upstream

Синтаксис	`memcached_next_upstream` error | timeout | invalid_response | not_found | off . . . ;
По умолчанию	`memcached_next_upstream error timeout;`
Контекст	http, server, location

Определяет, в каких случаях запрос будет передан следующему в группе *upstream* серверу:

`error`	произошла ошибка соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`timeout`	произошел таймаут во время соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`invalid_response`	сервер вернул пустой или неверный ответ;
`not_found`	сервер не нашел ответ;
`off`	запрещает передачу запроса следующему серверу.

Примечание

Необходимо понимать, что передача запроса следующему серверу возможна только при условии, что клиенту еще ничего не передавалось. То есть, если ошибка или таймаут возникли в середине передачи ответа клиенту, то действие директивы на такой запрос не распространяется.

Директива также определяет, что считается *неудачной попыткой* работы с сервером.

`error timeout invalid_response`	всегда считаются неудачными попытками, даже если они не указаны в директиве
`not_found`	никогда не считается неудачными попытками

Передача запроса следующему серверу может быть ограничена по *количеству попыток* и по *времени*.

memcached_next_upstream_timeout

Синтаксис	`memcached_next_upstream_timeout` *время*;
По умолчанию	`memcached_next_upstream_timeout 0;`
Контекст	http, server, location

Ограничивает время, в течение которого возможна передача запроса *следующему* серверу.

`0`	отключает это ограничение

memcached_next_upstream_tries

Синтаксис	`memcached_next_upstream_tries` *число*;
По умолчанию	`memcached_next_upstream_tries 0;`
Контекст	http, server, location

Ограничивает число допустимых попыток для передачи запроса *следующему* серверу.

`0`	отключает это ограничение

memcached_pass

Синтаксис	`memcached_pass` *адрес*;
По умолчанию	—
Контекст	location, if в location

Задает адрес сервера memcached. Адрес может быть указан в виде доменного имени или IP-адреса, и порта:

```
memcached_pass localhost:11211;
```

или в виде пути UNIX-сокета:

```
memcached_pass unix:/tmp/memcached.socket;
```

Если доменному имени соответствует несколько адресов, то все они будут использоваться по очереди (round-robin). Кроме того, в качестве адреса можно указать *группу серверов*. Если используется группа, указать порт невозможно; вместо этого укажите порт для каждого сервера внутри группы отдельно.

memcached_read_timeout

Синтаксис	`memcached_read_timeout` *время*;
По умолчанию	`memcached_read_timeout 60s;`
Контекст	http, server, location

Задает таймаут при чтении ответа сервера memcached. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями чтения. Если по истечении этого времени сервер memcached ничего не передаст, соединение закрывается.

memcached_send_timeout

Синтаксис	`memcached_send_timeout` *время*;
По умолчанию	`memcached_send_timeout 60s;`
Контекст	http, server, location

Задает таймаут при передаче запроса серверу memcached. Таймаут устанавливается не на всю передачу запроса, а только между двумя операциями записи. Если по истечении этого времени сервер memcached не примет новых данных, соединение закрывается.

memcached_socket_keepalive

Синтаксис	`memcached_socket_keepalive` on | off;
По умолчанию	`memcached_socket_keepalive off;`
Контекст	http, server, location

Конфигурирует поведение «TCP keepalive» для исходящих соединений к проксируемому серверу.

`""`	По умолчанию для сокета действуют настройки операционной системы.
`on`	для сокета включается параметр *SO_KEEPALIVE*

Встроенные переменные

`$memcached_key`

Задает ключ для получения ответа из сервера memcached.

Mirror

Позволяет зеркалировать исходный запрос при помощи создания фоновых зеркалирующих подзапросов. Ответы на зеркалирующие подзапросы игнорируются.

Пример конфигурации

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

location = /mirror {
    internal;
    proxy_pass http://test_backend$request_uri;
}
```

Директивы

mirror

Синтаксис	`mirror` *uri* | off;
По умолчанию	`mirror off;`
Контекст	http, server, location

Задает URI, на который будет зеркалироваться исходный запрос. На одном уровне конфигурации может быть задано несколько зеркал.

mirror_request_body

Синтаксис	`mirror_request_body` on | off;
По умолчанию	`mirror_request_body on;`
Контекст	http, server, location

Определяет, зеркалировать ли тело запроса клиента. Если включено, то тело запроса клиента будет прочитано перед созданием зеркалирующих подзапросов. В этом случае небуферизованное проксирование тела запроса клиента, задаваемое директивами *proxy_request_buffering*, *fastcgi_request_buffering*, *scgi_request_buffering* и *uwsgi_request_buffering*, будет отключено.

```
location / {
    mirror /mirror;
    mirror_request_body off;
    proxy_pass http://backend;
}

location = /mirror {
    internal;
    proxy_pass http://log_backend;
    proxy_pass_request_body off;
    proxy_set_header Content-Length "";
    proxy_set_header X-Original-URI $request_uri;
}
```

MP4

Обеспечивает серверную поддержку псевдо-стриминга для файлов в формате MP4. Такие файлы обычно имеют расширения .mp4, .m4v и .m4a.

Псевдо-стриминг работает в паре с совместимым медиаплеером. Плеер посылает серверу HTTP-запрос с указанием точки времени старта в аргументе start строки запроса (время задается в секундах), а сервер в ответ посылает поток, у которого начальная позиция соответствует запрошенному времени, например:

http://example.com/elephants_dream.mp4?start=238.88

Это позволяет в любой момент времени выполнить произвольное позиционирование, а также начать воспроизведение с середины временной шкалы.

В форматах, основанных на H.264, метаданные, необходимые для поддержки позиционирования, хранятся в так называемом «moov-атоме». Это часть файла, которая содержит индексную информацию для всего файла.

До начала воспроизведения плееру необходимо прочитать метаданные. Для этого он отсылает специальный запрос с аргументом *start=0*. Многие кодирующие программы добавляют метаданные в конец файла. Это неоптимально для псевдо-стриминга, поскольку плееру потребуется загрузить файл целиком прежде чем начать воспроизведение. Если метаданные находятся в начале файла, Angie PRO достаточно начать отправлять в ответ содержимое файла. Если же метаданные находятся в конце файла, потребуется прочитать весь файл и подготовить новый поток, в котором метаданные предшествуют медийным данным. Это требует дополнительного процессорного времени, памяти и дискового ввода/вывода, поэтому лучше заранее подготовить исходный файл для псевдо-стриминга, нежели делать это для каждого запроса.

Модуль также поддерживает аргумент *end* HTTP-запроса, задающий время окончания воспроизведения потока. Аргумент *end* задается совместно с аргументом *start* или самостоятельно:

http://example.com/elephants_dream.mp4?start=238.88&end=555.55

Для запроса с ненулевыми аргументами *start* или *end* Angie PRO считывает из файла метаданные, готовит поток с запрошенным диапазоном и отправляет его клиенту. Это тоже требует дополнительных ресурсов, как указано выше.

Если аргумент *start* указывает на видеокадр, не являющийся ключевым, то начало такого видео может воспроизводиться с ошибками. В этом случае к запрашиваемому видео *могут* быть добавлены ближайший к точке *start* ключевой кадр и все промежуточные кадры между ними. При воспроизведении эти кадры будут скрыты при помощи edit-листа.

Если запрос, обрабатываемый этим модулем, не содержит аргументов *start* и *end*, дополнительные ресурсы не тратятся, а файл отсылается непосредственно как статический ресурс. Некоторые плееры также поддерживают запросы с указанием диапазона запрашиваемых байт (byte-range requests), для них этот модуль не требуется.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_mp4_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Осторожно

Если ранее использовался сторонний модуль mp4, следует его отключить.

Схожая поддержка псевдо-стриминга для FLV-файлов обеспечивается модулем *FLV*.

Пример конфигурации

```
location /video/ {
    mp4;
    mp4_buffer_size     1m;
    mp4_max_buffer_size 5m;
}
```

Директивы

mp4

Синтаксис	`mp4;`
По умолчанию	—
Контекст	location

Включает в содержащем location обработку этим модулем.

mp4_buffer_size

Синтаксис	`mp4_buffer_size` *размер*;
По умолчанию	`mp4_buffer_size 512K;`
Контекст	http, server, location

Задает начальный размер буфера, используемого при обработке MP4-файлов.

mp4_max_buffer_size

Синтаксис	`mp4_max_buffer_size` *размер*;
По умолчанию	`mp4_max_buffer_size 10M;`
Контекст	http, server, location

В ходе обработки метаданных может понадобиться буфер большего размера. Его размер не может превышать указанного, иначе Angie PRO вернет серверную ошибку 500 (Internal Server Error) и запишет в лог следующее сообщение:

> «/some/movie/file.mp4» mp4 moov atom is too large: 12583268, you may want to increase mp4_max_buffer_size

mp4_limit_rate

Синтаксис	`mp4_limit_rate` on | off | *коэффициент*;
По умолчанию	`mp4_limit_rate off;`
Контекст	http, server, location

Ограничивает скорость передачи запрошенного MP4-файла клиенту. Предельное значение вычисляется умножением заданного *коэффициента* на средний битрейт файла.

- Специальное значение `off` отключает ограничение скорости.
- Специальное значение `on` соответствует *коэффициенту* `1.1`.
- Начало действия ограничения регулируется значением *mp4_limit_rate_after*.

Запросы ограничиваются индивидуально: если клиент открыл два соединения, общая скорость удваивается. В связи с этим обратите внимание на *limit_conn* и сопутствующие директивы.

mp4_limit_rate_after

Синтаксис	`mp4_limit_rate_after` *время*;
По умолчанию	`mp4_limit_rate_after 60s;`
Контекст	http, server, location

Задает (в пересчете на *время воспроизведения*) объем медиаданных, после передачи которого скорость будет ограничена директивой *mp4_limit_rate*.

mp4_start_key_frame

Синтаксис	`mp4_start_key_frame` on | off;
По умолчанию	`mp4_start_key_frame off;`
Контекст	http, server, location

Включает режим, в котором видео всегда начинается с ключевого видеокадра. Если аргумент start не указывает на ключевой кадр, то первоначальные кадры будут скрыты при помощи mp4 edit-листа. Edit-листы поддерживаются большинством плееров и браузеров включая Chrome, Safari, QuickTime и ffmpeg, частично поддерживаются в Firefox.

Perl

Модуль позволяет писать обработчики location и переменных на Perl, а также вставлять вызовы Perl в SSI.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_perl_module`.

В наших репозиториях модуль собран динамически и доступен отдельным пакетом *angie-pro-module-perl*; подключить его можно с помощью директивы *load_module*.

Важно

Для сборки этого модуля необходим Perl версии 5.6.1 и выше. Компилятор C должен быть совместим с тем, которым был собран Perl.

Известные проблемы

Модуль экспериментальный, поэтому возможно все.

Для того чтобы во время переконфигурации Perl перекомпилировал измененные модули, его нужно собрать с параметрами *-Dusemultiplicity=yes* или *-Dusethreads=yes*. Кроме того, чтобы во время работы Perl терял меньше памяти, его нужно собрать с параметром *-Dusemymalloc=no*. Узнать значения этих параметров у уже собранного Perl можно так (в примере приведены желаемые значения параметров):

```
$ perl -V:usemultiplicity -V:usemymalloc |br|
usemultiplicity='define'; |br|
usemymalloc='n';
```

Необходимо учитывать, что после пересборки Perl с новыми параметрами *-Dusemultiplicity=yes* или *-Dusethreads=yes* придется также пересобрать и все бинарные модули Perl, так как они просто перестанут работать с новым Perl.

Возможно, главный процесс, а вслед за ним и рабочие процессы, будут увеличиваться в размерах при каждой переконфигурации. Когда главный процесс вырастет до неприемлемых размеров, можно воспользоваться процедурой *обновления сервера на лету*, не меняя при этом сам исполняемый файл.

Если модуль Perl выполняет длительную операцию, например, определяет адрес по имени, соединяется с другим сервером, делает запрос к базе данных, то на это время все остальные запросы, обслуживаемые данным рабочим процессом, не будут обрабатываться. Поэтому рекомендуется ограничиться операциями, время исполнения которых короткое и предсказуемое, например, обращение к локальной файловой системе.

Пример конфигурации

```
http {

    perl_modules perl/lib;
    perl_require hello.pm;

    perl_set $msie6 '

        sub {
            my $r = shift;
            my $ua = $r->header_in("User-Agent");

            return "" if $ua =~ /Opera/;
            return "1" if $ua =~ / MSIE [6-9]\.\d+/;
            return "";
        }

    ';

    server {
        location / {
```

```
            perl hello::handler;
        }
    }
```

Модуль *perl/lib/hello.pm*:

```
package hello;

use nginx;

sub handler {
    my $r = shift;

    $r->send_http_header("text/html");
    return OK if $r->header_only;

    $r->print("hello!\n<br/>");

    if (-f $r->filename or -d _) {
        $r->print($r->uri, " exists!\n");
    }

    return OK;
}

1;
__END__
```

Директивы

perl

Синтаксис	`perl` *модуль* :: *функция* | 'sub { ... }';
По умолчанию	—
Контекст	location, limit_except

Устанавливает обработчик Perl для данного location.

perl_modules

Синтаксис	`perl_modules` *путь*;
По умолчанию	—
Контекст	http

Задает дополнительный путь для модулей Perl.

perl_require

Синтаксис	`perl_require` *модуль*;
По умолчанию	—
Контекст	http

Задает имя модуля, который будет подгружаться при каждой переконфигурации. Директив *perl_ require* может быть несколько.

perl_set

Синтаксис	`perl_set` *$переменная модуль* :: *функция* | 'sub { ... }';
По умолчанию	—
Контекст	http

Устанавливает обработчик Perl для указанной переменной.

Вызов Perl из SSI

Формат команды SSI с вызовом Perl следующий:

```
<!--# perl sub="модуль::функция" arg="параметр1" arg="параметр2" ...
-->
```

Методы объекта запроса $r

`$r->args`

возвращает аргументы запроса.

`$r->filename`

возвращает имя файла, соответствующее URI запроса.

`$r->has_request_body` (***обработчик***)

возвращает 0, если в запросе нет тела. Если же в запросе есть тело, то устанавливается указанный обработчик и возвращается 1. По окончании чтения тела запроса Angie PRO вызовет установленный обработчик. Обратите внимание, что нужно передавать ссылку на функцию обработчика. Пример:

```
package hello;

use nginx;

sub handler {
    my $r = shift;
```

```
    if ($r->request_method ne "POST") {
        return DECLINED;
    }

    if ($r->has_request_body(\&post)) {
        return OK;
    }

    return HTTP_BAD_REQUEST;
}

sub post {
    my $r = shift;

    $r->send_http_header;

    $r->print("request_body: \"", $r->request_body, "\"<br/>");
    $r->print("request_body_file: \"", $r->request_body_file, "\"<br/>\n");

    return OK;
}

1;

__END__
```

`$r->allow_ranges`

разрешает использовать диапазоны байт (byte ranges) при передаче ответа.

`$r->discard_request_body`

указывает Angie PRO игнорировать тело запроса.

`$r->header_in` (***поле***)

возвращает значение заданного поля в заголовке запроса клиента.

`$r->header_only`

определяет, нужно ли передавать клиенту только заголовок ответа или весь ответ.

`$r->header_out` (***поле, значение***)

устанавливает значение для заданного поля в заголовке ответа.

`$r->internal_redirect` (***uri***)

делает внутреннее перенаправление на указанный uri. Перенаправление происходит уже после завершения обработчика Perl. Метод принимает экранированные URI и поддерживает перенаправления в *именованные location*.

`$r->log_error` (***код_ошибки, сообщение***)

записывает указанное сообщение в *error_log*. Если *код_ошибки* ненулевой, то к сообщению будет добавлен код ошибки и ее описание.

`$r->print` (***текст, ...***)

метод передает клиенту данные.

`$r->request_body`

возвращает тело запроса клиента при условии, что тело не записано во временный файл. Для того чтобы тело запроса клиента гарантированно находилось в памяти, нужно ограничить его размер с помощью *client_max_body_size* и задать достаточной размер для буфера *client_body_buffer_size*.

`$r->request_body_file`

возвращает имя файла, в котором хранится тело запроса клиента. По завершению обработки файл необходимо удалить. Для того чтобы тело запроса клиента всегда записывалось в файл, следует включить *client_body_in_file_only*.

`$r->request_method`

возвращает HTTP-метод запроса клиента.

`$r->remote_addr`

возвращает IP-адрес клиента.

`$r->flush`

немедленно передает данные клиенту.

`$r->sendfile` (***имя*** [, ***смещение*** [, ***длина***]])

передает клиенту содержимое указанного файла. Необязательные параметры задают начальное смещение и длину передаваемых данных. Непосредственно передача данных происходит уже после завершения обработчика Perl.

`$r->send_http_header` ([***тип***])

передает клиенту заголовок ответа. Необязательный параметр тип устанавливает значение поля «Content-Type» в заголовке ответа. Пустая строка в качестве типа запрещает передачу поля «Content-Type».

`$r->status` (***код***)

устанавливает код ответа.

`$r->sleep` (***миллисекунды, обработчик***)

устанавливает указанный обработчик и останавливает обработку запроса на заданное время. Angie PRO в это время продолжает обрабатывать другие запросы. По истечении указанного времени Angie PRO вызовет установленный обработчик. Обратите внимание, что нужно передавать ссылку на функцию обработчика. Для передачи данных между обработчиками следует использовать *$r->variable()*. Пример:

```
package hello;

use nginx;

sub handler {
    my $r = shift;

    $r->discard_request_body;
    $r->variable("var", "OK");
    $r->sleep(1000, \&next);

    return OK;
}

sub next {
    my $r = shift;

    $r->send_http_header;
    $r->print($r->variable("var"));

    return OK;
}

1;

__END__
```

`$r->unescape` (***текст***)

декодирует текст, заданный в виде «%XX».

`$r->uri`

возвращает URI запроса.

`$r->variable` (***имя*** [, ***значение***])

возвращает или устанавливает значение указанной переменной. Переменные локальны для каждого запроса.

Prometheus

Собирает *статистику* Angie PRO, исходя из определенных в конфигурации шаблонов, и возвращает сформированные на основании этих шаблонов метрики в формате Prometheus.

> **Внимание**
>
> Чтобы собирать статистику, включите в нужных контекстах зону разделяемой памяти с помощью:
>
> - директивы `zone` в *http_ upstream* или *stream_ upstream*;
> - директивы *status_ zone*;
> - параметра `status_zone` в директиве *resolver*.

Пример конфигурации

Три метрики для сбора статистики запросов к серверным зонам разделяемой памяти, объединенные в шаблон `custom` и опубликованные по пути `/p8s`:

```
http {

    prometheus_template custom {
        'angie_http_server_zones_requests_total{zone="$1"}' $p8s_value
            path=~^/http/server_zones/([^/]+)/requests/total$
            type=counter;

        'angie_http_server_zones_requests_processing{zone="$1"}' $p8s_value
            path=~^/http/server_zones/([^/]+)/requests/processing$
            type=gauge;

        'angie_http_server_zones_requests_discarded{zone="$1"}' $p8s_value
            path=~^/http/server_zones/([^/]+)/requests/discarded$
            type=counter;
    }

    # ...

    server {
```

```
        listen 80;

        location =/p8s {
            prometheus custom;
        }

        # ...

    }
}
```

В состав Angie PRO входит вспомогательный файл `prometheus_all.conf`, куда включен набор общеупотребимых метрик, сведенных в шаблон `all`:

Содержимое файла (Angie)

```
prometheus_template all {

angie_connections_accepted $p8s_value
    path=/connections/accepted
    type=counter
    'help=The total number of accepted client connections.';

angie_connections_dropped $p8s_value
    path=/connections/dropped
    type=counter
    'help=The total number of dropped client connections.';

angie_connections_active $p8s_value
    path=/connections/active
    type=gauge
    'help=The current number of active client connections.';

angie_connections_idle $p8s_value
    path=/connections/idle
    type=gauge
    'help=The current number of idle client connections.';


'angie_slabs_pages_used{zone="$1"}' $p8s_value
    path=~^/slabs/([^/]+)/pages/used$
    type=gauge
    'help=The number of currently used memory pages in a slab zone.';

'angie_slabs_pages_free{zone="$1"}' $p8s_value
    path=~^/slabs/([^/]+)/pages/free$
    type=gauge
    'help=The number of currently free memory pages in a slab zone.';


'angie_slabs_pages_slots_used{zone="$1",size="$2"}' $p8s_value
    path=~^/slabs/([^/]+)/slots/([^/]+)/used$
    type=gauge
    'help=The number of currently used memory slots of a specific size in a slab zone.
↪';
```

```
'angie_slabs_pages_slots_free{zone="$1",size="$2"}' $p8s_value
    path=~^/slabs/([^/]+)/slots/([^/]+)/free$
    type=gauge
    'help=The number of currently free memory slots of a specific size in a slab zone.
↪';

'angie_slabs_pages_slots_reqs{zone="$1",size="$2"}' $p8s_value
    path=~^/slabs/([^/]+)/slots/([^/]+)/reqs$
    type=counter
    'help=The total number of attempts to allocate a memory slot of a specific size␣
↪in a slab zone.';

'angie_slabs_pages_slots_fails{zone="$1",size="$2"}' $p8s_value
    path=~^/slabs/([^/]+)/slots/([^/]+)/fails$
    type=counter
    'help=The number of unsuccessful attempts to allocate a memory slot of a specific␣
↪size in a slab zone.';


'angie_resolvers_queries{zone="$1",type="$2"}' $p8s_value
    path=~^/resolvers/([^/]+)/queries/([^/]+)$
    type=counter
    'help=The number of queries of a specific type to resolve in a resolver zone.';

'angie_resolvers_sent{zone="$1",type="$2"}' $p8s_value
    path=~^/resolvers/([^/]+)/sent/([^/]+)$
    type=counter
    'help=The number of sent DNS queries of a specific type to resolve in a resolver␣
↪zone.';

'angie_resolvers_responses{zone="$1",status="$2"}' $p8s_value
    path=~^/resolvers/([^/]+)/responses/([^/]+)$
    type=counter
    'help=The number of resolution results with a specific status in a resolver zone.
↪';


'angie_http_server_zones_ssl_handshaked{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/ssl/handshaked$
    type=counter
    'help=The total number of successful SSL handshakes in an HTTP server zone.';

'angie_http_server_zones_ssl_reuses{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/ssl/reuses$
    type=counter
    'help=The total number of session reuses during SSL handshakes in an HTTP server␣
↪zone.';

'angie_http_server_zones_ssl_timedout{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/ssl/timedout$
    type=counter
    'help=The total number of timed-out SSL handshakes in an HTTP server zone.';

'angie_http_server_zones_ssl_failed{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/ssl/failed$
    type=counter
    'help=The total number of failed SSL handshakes in an HTTP server zone.';
```

```
'angie_http_server_zones_requests_total{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/requests/total$
    type=counter
    'help=The total number of client requests received in an HTTP server zone.';

'angie_http_server_zones_requests_processing{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/requests/processing$
    type=gauge
    'help=The number of client requests currently being processed in an HTTP server␣
↪zone.';

'angie_http_server_zones_requests_discarded{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/requests/discarded$
    type=counter
    'help=The total number of client requests completed in an HTTP server zone␣
↪without sending a response.';


'angie_http_server_zones_responses{zone="$1",code="$2"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/responses/([^/]+)$
    type=counter
    'help=The number of responses with a specific status in an HTTP server zone.';


'angie_http_server_zones_data_received{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes received from clients in an HTTP server zone.';

'angie_http_server_zones_data_sent{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes sent to clients in an HTTP server zone.';


'angie_http_location_zones_requests_total{zone="$1"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/requests/total$
    type=counter
    'help=The total number of client requests in an HTTP location zone.';

'angie_http_location_zones_requests_discarded{zone="$1"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/requests/discarded$
    type=counter
    'help=The total number of client requests completed in an HTTP location zone␣
↪without sending a response.';


'angie_http_location_zones_responses{zone="$1",code="$2"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/responses/([^/]+)$
    type=counter
    'help=The number of responses with a specific status in an HTTP location zone.';


'angie_http_location_zones_data_received{zone="$1"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/data/received$
```

```
    type=counter
    'help=The total number of bytes received from clients in an HTTP location zone.';

'angie_http_location_zones_data_sent{zone="$1"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes sent to clients in an HTTP location zone.';


'angie_http_upstreams_peers_state{upstream="$1",peer="$2"}' $p8st_all_ups_state
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/state$
    type=gauge
    'help=The current state of an upstream peer in "HTTP": 1 - up, 2 - down, 3 -␣
↪unavailable, or 4 - recovering.';


'angie_http_upstreams_peers_selected_current{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/selected/current$
    type=gauge
    'help=The number of requests currently being processed by an upstream peer in
↪"HTTP".';

'angie_http_upstreams_peers_selected_total{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/selected/total$
    type=counter
    'help=The total number of attempts to use an upstream peer in "HTTP".';


'angie_http_upstreams_peers_responses{upstream="$1",peer="$2",code="$3"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/responses/([^/]+)$
    type=counter
    'help=The number of responses with a specific status received from an upstream␣
↪peer in "HTTP".';


'angie_http_upstreams_peers_data_sent{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes sent to an upstream peer in "HTTP".';

'angie_http_upstreams_peers_data_received{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes received from an upstream peer in "HTTP".';


'angie_http_upstreams_peers_health_fails{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/fails$
    type=counter
    'help=The total number of unsuccessful attempts to communicate with an upstream␣
↪peer in "HTTP".';

'angie_http_upstreams_peers_health_unavailable{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/unavailable$
    type=counter
    'help=The number of times when an upstream peer in "HTTP" became "unavailable"␣
↪due to reaching the max_fails limit.';
```

```
'angie_http_upstreams_peers_health_downtime{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/downtime$
    type=counter
    'help=The total time (in milliseconds) that an upstream peer in "HTTP" was
↪"unavailable".';


'angie_http_upstreams_keepalive{upstream="$1"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/keepalive$
    type=gauge
    'help=The number of currently cached keepalive connections for an HTTP upstream.';


'angie_http_caches_responses{zone="$1",status="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/([^/]+)/responses$
    type=counter
    'help=The total number of responses processed in an HTTP cache zone with a␣
↪specific cache status.';

'angie_http_caches_bytes{zone="$1",status="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/([^/]+)/bytes$
    type=counter
    'help=The total number of bytes processed in an HTTP cache zone with a specific␣
↪cache status.';

'angie_http_caches_responses_written{zone="$1",status="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/([^/]+)/responses_written$
    type=counter
    'help=The total number of responses written to an HTTP cache zone with a specific␣
↪cache status.';

'angie_http_caches_bytes_written{zone="$1",status="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/([^/]+)/bytes_written$
    type=counter
    'help=The total number of bytes written to an HTTP cache zone with a specific␣
↪cache status.';


'angie_http_caches_size{zone="$1"}' $p8s_value
    path=~^/http/caches/([^/]+)/size$
    type=gauge
    'help=The current size (in bytes) of cached responses in an HTTP cache zone.';


'angie_http_caches_shards_size{zone="$1",path="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/shards/([^/]+)/size$
    type=gauge
    'help=The current size (in bytes) of cached responses in a shard path of an HTTP␣
↪cache zone.';


'angie_http_limit_conns{zone="$1",status="$2"}' $p8s_value
    path=~^/http/limit_conns/([^/]+)/([^/]+)$
    type=counter
    'help=The number of requests processed by an HTTP limit_conn zone with a specific␣
↪result.';
```

```
'angie_http_limit_reqs{zone="$1",status="$2"}' $p8s_value
    path=~^/http/limit_reqs/([^/]+)/([^/]+)$
    type=counter
    'help=The number of requests processed by an HTTP limit_reqs zone with a specific␣
↪result.';


'angie_stream_server_zones_ssl_handshaked{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/ssl/handshaked$
    type=counter
    'help=The total number of successful SSL handshakes in a stream server zone.';

'angie_stream_server_zones_ssl_reuses{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/ssl/reuses$
    type=counter
    'help=The total number of session reuses during SSL handshakes in a stream server␣
↪zone.';

'angie_stream_server_zones_ssl_timedout{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/ssl/timedout$
    type=counter
    'help=The total number of timed-out SSL handshakes in a stream server zone.';

'angie_stream_server_zones_ssl_failed{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/ssl/failed$
    type=counter
    'help=The total number of failed SSL handshakes in a stream server zone.';


'angie_stream_server_zones_connections_total{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/connections/total$
    type=counter
    'help=The total number of client connections received in a stream server zone.';

'angie_stream_server_zones_connections_processing{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/connections/processing$
    type=gauge
    'help=The number of client connections currently being processed in a stream␣
↪server zone.';

'angie_stream_server_zones_connections_discarded{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/connections/discarded$
    type=counter
    'help=The total number of client connections completed in a stream server zone␣
↪without establishing a session.';

'angie_stream_server_zones_connections_passed{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/connections/passed$
    type=counter
    'help=The total number of client connections in a stream server zone passed for␣
↪handling to a different listening socket.';


'angie_stream_server_zones_sessions{zone="$1",status="$2"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/sessions/([^/]+)$
    type=counter
```

```
    'help=The number of sessions finished with a specific status in a stream server␣
↪zone.';


'angie_stream_server_zones_data_received{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes received from clients in a stream server zone.';

'angie_stream_server_zones_data_sent{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes sent to clients in a stream server zone.';


'angie_stream_upstreams_peers_state{upstream="$1",peer="$2"}' $p8st_all_ups_state
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/state$
    type=gauge
    'help=The current state of an upstream peer in "stream": 1 - up, 2 - down, 3 -␣
↪unavailable, or 4 - recovering.';


'angie_stream_upstreams_peers_selected_current{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/selected/current$
    type=gauge
    'help=The number of sessions currently being processed by an upstream peer in
↪"stream".';

'angie_stream_upstreams_peers_selected_total{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/selected/total$
    type=counter
    'help=The total number of attempts to use an upstream peer in "stream".';


'angie_stream_upstreams_peers_data_sent{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes sent to an upstream peer in "stream".';

'angie_stream_upstreams_peers_data_received{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes received from an upstream peer in "stream".';


'angie_stream_upstreams_peers_health_fails{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/fails$
    type=counter
    'help=The total number of unsuccessful attempts to communicate with an upstream␣
↪peer in "stream".';

'angie_stream_upstreams_peers_health_unavailable{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/unavailable$
    type=counter
    'help=The number of times when an upstream peer in "stream" became "unavailable"␣
↪due to reaching the max_fails limit.';
```

```
'angie_stream_upstreams_peers_health_downtime{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/downtime$
    type=counter
    'help=The total time (in milliseconds) that an upstream peer in "stream" was
↪"unavailable".';
}

map $p8s_value $p8st_all_ups_state {
    volatile;
    "up"           1;
    "down"         2;
    "unavailable"  3;
    "recovering"   4;
    default        0;
}
```

Содержимое файла (Angie PRO)

```
prometheus_template all {

angie_connections_accepted $p8s_value
    path=/connections/accepted
    type=counter
    'help=The total number of accepted client connections.';

angie_connections_dropped $p8s_value
    path=/connections/dropped
    type=counter
    'help=The total number of dropped client connections.';

angie_connections_active $p8s_value
    path=/connections/active
    type=gauge
    'help=The current number of active client connections.';

angie_connections_idle $p8s_value
    path=/connections/idle
    type=gauge
    'help=The current number of idle client connections.';


'angie_slabs_pages_used{zone="$1"}' $p8s_value
    path=~^/slabs/([^/]+)/pages/used$
    type=gauge
    'help=The number of currently used memory pages in a slab zone.';

'angie_slabs_pages_free{zone="$1"}' $p8s_value
    path=~^/slabs/([^/]+)/pages/free$
    type=gauge
    'help=The number of currently free memory pages in a slab zone.';


'angie_slabs_pages_slots_used{zone="$1",size="$2"}' $p8s_value
    path=~^/slabs/([^/]+)/slots/([^/]+)/used$
    type=gauge
    'help=The number of currently used memory slots of a specific size in a slab zone.
```

```
↪';

'angie_slabs_pages_slots_free{zone="$1",size="$2"}' $p8s_value
    path=~^/slabs/([^/]+)/slots/([^/]+)/free$
    type=gauge
    'help=The number of currently free memory slots of a specific size in a slab zone.
↪';

'angie_slabs_pages_slots_reqs{zone="$1",size="$2"}' $p8s_value
    path=~^/slabs/([^/]+)/slots/([^/]+)/reqs$
    type=counter
    'help=The total number of attempts to allocate a memory slot of a specific size␣
↪in a slab zone.';

'angie_slabs_pages_slots_fails{zone="$1",size="$2"}' $p8s_value
    path=~^/slabs/([^/]+)/slots/([^/]+)/fails$
    type=counter
    'help=The number of unsuccessful attempts to allocate a memory slot of a specific␣
↪size in a slab zone.';


'angie_resolvers_queries{zone="$1",type="$2"}' $p8s_value
    path=~^/resolvers/([^/]+)/queries/([^/]+)$
    type=counter
    'help=The number of queries of a specific type to resolve in a resolver zone.';

'angie_resolvers_sent{zone="$1",type="$2"}' $p8s_value
    path=~^/resolvers/([^/]+)/sent/([^/]+)$
    type=counter
    'help=The number of sent DNS queries of a specific type to resolve in a resolver␣
↪zone.';

'angie_resolvers_responses{zone="$1",status="$2"}' $p8s_value
    path=~^/resolvers/([^/]+)/responses/([^/]+)$
    type=counter
    'help=The number of resolution results with a specific status in a resolver zone.
↪';


'angie_http_server_zones_ssl_handshaked{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/ssl/handshaked$
    type=counter
    'help=The total number of successful SSL handshakes in an HTTP server zone.';

'angie_http_server_zones_ssl_reuses{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/ssl/reuses$
    type=counter
    'help=The total number of session reuses during SSL handshakes in an HTTP server␣
↪zone.';

'angie_http_server_zones_ssl_timedout{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/ssl/timedout$
    type=counter
    'help=The total number of timed-out SSL handshakes in an HTTP server zone.';

'angie_http_server_zones_ssl_failed{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/ssl/failed$
```

```
    type=counter
    'help=The total number of failed SSL handshakes in an HTTP server zone.';


'angie_http_server_zones_requests_total{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/requests/total$
    type=counter
    'help=The total number of client requests received in an HTTP server zone.';

'angie_http_server_zones_requests_processing{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/requests/processing$
    type=gauge
    'help=The number of client requests currently being processed in an HTTP server␣
↪zone.';

'angie_http_server_zones_requests_discarded{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/requests/discarded$
    type=counter
    'help=The total number of client requests completed in an HTTP server zone␣
↪without sending a response.';


'angie_http_server_zones_responses{zone="$1",code="$2"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/responses/([^/]+)$
    type=counter
    'help=The number of responses with a specific status in an HTTP server zone.';


'angie_http_server_zones_data_received{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes received from clients in an HTTP server zone.';

'angie_http_server_zones_data_sent{zone="$1"}' $p8s_value
    path=~^/http/server_zones/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes sent to clients in an HTTP server zone.';


'angie_http_location_zones_requests_total{zone="$1"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/requests/total$
    type=counter
    'help=The total number of client requests in an HTTP location zone.';

'angie_http_location_zones_requests_discarded{zone="$1"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/requests/discarded$
    type=counter
    'help=The total number of client requests completed in an HTTP location zone␣
↪without sending a response.';


'angie_http_location_zones_responses{zone="$1",code="$2"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/responses/([^/]+)$
    type=counter
    'help=The number of responses with a specific status in an HTTP location zone.';
```

```
'angie_http_location_zones_data_received{zone="$1"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes received from clients in an HTTP location zone.';

'angie_http_location_zones_data_sent{zone="$1"}' $p8s_value
    path=~^/http/location_zones/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes sent to clients in an HTTP location zone.';


'angie_http_upstreams_peers_state{upstream="$1",peer="$2"}' $p8st_all_ups_state
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/state$
    type=gauge
    'help=The current state of an upstream peer in "HTTP": 1 - up, 2 - down, 3 -␣
↪unavailable, 4 - recovering, 5 - unhealthy, 6 - checking, or 7 - draining.';


'angie_http_upstreams_peers_selected_current{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/selected/current$
    type=gauge
    'help=The number of requests currently being processed by an upstream peer in
↪"HTTP".';

'angie_http_upstreams_peers_selected_total{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/selected/total$
    type=counter
    'help=The total number of attempts to use an upstream peer in "HTTP".';


'angie_http_upstreams_peers_responses{upstream="$1",peer="$2",code="$3"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/responses/([^/]+)$
    type=counter
    'help=The number of responses with a specific status received from an upstream␣
↪peer in "HTTP".';


'angie_http_upstreams_peers_data_sent{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes received from an upstream peer in "HTTP".';

'angie_http_upstreams_peers_data_received{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes sent to an upstream peer in "HTTP".';


'angie_http_upstreams_peers_health_fails{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/fails$
    type=counter
    'help=The total number of unsuccessful attempts to communicate with an upstream␣
↪peer in "HTTP".';

'angie_http_upstreams_peers_health_unavailable{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/unavailable$
    type=counter
```

```
    'help=The number of times when an upstream peer in "HTTP" became "unavailable"␣
↪due to reaching the max_fails limit.';

'angie_http_upstreams_peers_health_downtime{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/downtime$
    type=counter
    'help=The total time (in milliseconds) that an upstream peer in "HTTP" was
↪"unavailable".';

'angie_http_upstreams_peers_health_header_time{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/header_time$
    type=gauge
    'help=Average time (in milliseconds) to receive the response headers from an␣
↪upstream peer in "HTTP".';

'angie_http_upstreams_peers_health_response_time{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/response_time$
    type=gauge
    'help=Average time (in milliseconds) to receive the complete response from an␣
↪upstream peer in "HTTP".';

'angie_http_upstreams_peers_health_probes_count{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/probes/count$
    type=counter
    'help=The total number of probes for this peer.';

'angie_http_upstreams_peers_health_probes_fails{upstream="$1",peer="$2"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/peers/([^/]+)/health/probes/fails$
    type=counter
    'help=The total number of failed probes for this peer.';


'angie_http_upstreams_keepalive{upstream="$1"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/keepalive$
    type=gauge
    'help=The number of currently cached keepalive connections for an HTTP upstream.';


'angie_http_upstreams_queue_queued{upstream="$1"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/queue/queued$
    type=counter
    'help=The total number of queued requests for an HTTP upstream.';

'angie_http_upstreams_queue_waiting{upstream="$1"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/queue/waiting$
    type=gauge
    'help=The number of requests currently waiting in an HTTP upstream queue.';

'angie_http_upstreams_queue_dropped{upstream="$1"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/queue/dropped$
    type=counter
    'help=The total number of requests dropped from an HTTP upstream queue because␣
↪the client had prematurely closed the connection.';

'angie_http_upstreams_queue_timedout{upstream="$1"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/queue/timedout$
    type=counter
```

```
    'help=The total number of requests timed out from an HTTP upstream queue.';

'angie_http_upstreams_queue_overflows{upstream="$1"}' $p8s_value
    path=~^/http/upstreams/([^/]+)/queue/overflows$
    type=counter
    'help=The total number of requests rejected by an HTTP upstream queue because the␣
↪size limit had been reached.';


'angie_http_caches_responses{zone="$1",status="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/([^/]+)/responses$
    type=counter
    'help=The total number of responses processed in an HTTP cache zone with a␣
↪specific cache status.';

'angie_http_caches_bytes{zone="$1",status="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/([^/]+)/bytes$
    type=counter
    'help=The total number of bytes processed in an HTTP cache zone with a specific␣
↪cache status.';

'angie_http_caches_responses_written{zone="$1",status="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/([^/]+)/responses_written$
    type=counter
    'help=The total number of responses written to an HTTP cache zone with a specific␣
↪cache status.';

'angie_http_caches_bytes_written{zone="$1",status="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/([^/]+)/bytes_written$
    type=counter
    'help=The total number of bytes written to an HTTP cache zone with a specific␣
↪cache status.';


'angie_http_caches_size{zone="$1"}' $p8s_value
    path=~^/http/caches/([^/]+)/size$
    type=gauge
    'help=The current size (in bytes) of cached responses in an HTTP cache zone.';


'angie_http_caches_shards_size{zone="$1",path="$2"}' $p8s_value
    path=~^/http/caches/([^/]+)/shards/([^/]+)/size$
    type=gauge
    'help=The current size (in bytes) of cached responses in a shard path of an HTTP␣
↪cache zone.';


'angie_http_limit_conns{zone="$1",status="$2"}' $p8s_value
    path=~^/http/limit_conns/([^/]+)/([^/]+)$
    type=counter
    'help=The number of requests processed by an HTTP limit_conn zone with a specific␣
↪result.';

'angie_http_limit_reqs{zone="$1",status="$2"}' $p8s_value
    path=~^/http/limit_reqs/([^/]+)/([^/]+)$
    type=counter
    'help=The number of requests processed by an HTTP limit_reqs zone with a specific␣
```

```
↪result.';


'angie_stream_server_zones_ssl_handshaked{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/ssl/handshaked$
    type=counter
    'help=The total number of successful SSL handshakes in a stream server zone.';

'angie_stream_server_zones_ssl_reuses{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/ssl/reuses$
    type=counter
    'help=The total number of session reuses during SSL handshakes in a stream server␣
↪zone.';

'angie_stream_server_zones_ssl_timedout{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/ssl/timedout$
    type=counter
    'help=The total number of timed-out SSL handshakes in a stream server zone.';

'angie_stream_server_zones_ssl_failed{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/ssl/failed$
    type=counter
    'help=The total number of failed SSL handshakes in a stream server zone.';


'angie_stream_server_zones_connections_total{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/connections/total$
    type=counter
    'help=The total number of client connections received in a stream server zone.';

'angie_stream_server_zones_connections_processing{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/connections/processing$
    type=gauge
    'help=The number of client connections currently being processed in a stream␣
↪server zone.';

'angie_stream_server_zones_connections_discarded{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/connections/discarded$
    type=counter
    'help=The total number of client connections completed in a stream server zone␣
↪without establishing a session.';


'angie_stream_server_zones_sessions{zone="$1",status="$2"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/sessions/([^/]+)$
    type=counter
    'help=The number of sessions finished with a specific status in a stream server␣
↪zone.';


'angie_stream_server_zones_data_received{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes received from clients in a stream server zone.';

'angie_stream_server_zones_data_sent{zone="$1"}' $p8s_value
    path=~^/stream/server_zones/([^/]+)/data/sent$
```

```
    type=counter
    'help=The total number of bytes sent to clients in a stream server zone.';


'angie_stream_upstreams_peers_state{upstream="$1",peer="$2"}' $p8st_all_ups_state
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/state$
    type=gauge
    'help=The current state of an upstream peer in "stream": 1 - up, 2 - down, 3 -␣
↪unavailable, 4 - recovering, 5 - unhealthy, 6 - checking, or 7 - draining.';


'angie_stream_upstreams_peers_selected_current{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/selected/current$
    type=gauge
    'help=The number of sessions currently being processed by an upstream peer in
↪"stream".';

'angie_stream_upstreams_peers_selected_total{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/selected/total$
    type=counter
    'help=The total number of attempts to use an upstream peer in "stream".';


'angie_stream_upstreams_peers_data_sent{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/data/sent$
    type=counter
    'help=The total number of bytes received from an upstream peer in "stream".';

'angie_stream_upstreams_peers_data_received{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/data/received$
    type=counter
    'help=The total number of bytes sent to an upstream peer in "stream".';


'angie_stream_upstreams_peers_health_fails{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/fails$
    type=counter
    'help=The total number of unsuccessful attempts to communicate with an upstream␣
↪peer in "stream".';

'angie_stream_upstreams_peers_health_unavailable{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/unavailable$
    type=counter
    'help=The number of times when an upstream peer in "stream" became "unavailable"␣
↪due to reaching the max_fails limit.';

'angie_stream_upstreams_peers_health_downtime{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/downtime$
    type=counter
    'help=The total time (in milliseconds) that an upstream peer in "stream" was
↪"unavailable".';

'angie_stream_upstreams_peers_health_connect_time{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/connect_time$
    type=gauge
    'help=Average time (in milliseconds) to connect to an upstream peer in "stream".';
```

```
'angie_stream_upstreams_peers_health_first_byte_time{upstream="$1",peer="$2"}' $p8s_
↪value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/first_byte_time$
    type=gauge
    'help=Average time (in milliseconds) to receive the first byte from an upstream␣
↪peer in "stream".';

'angie_stream_upstreams_peers_health_last_byte_time{upstream="$1",peer="$2"}' $p8s_
↪value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/last_byte_time$
    type=gauge
    'help=Average time (in milliseconds) of the whole communication session with an␣
↪upstream peer in "stream".';


'angie_stream_upstreams_peers_health_probes_count{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/probes/count$
    type=counter
    'help=The total number of probes for this peer.';

'angie_stream_upstreams_peers_health_probes_fails{upstream="$1",peer="$2"}' $p8s_value
    path=~^/stream/upstreams/([^/]+)/peers/([^/]+)/health/probes/fails$
    type=counter
    'help=The total number of failed probes for this peer.';
}

map $p8s_value $p8st_all_ups_state {
    volatile;
    "up"           1;
    "down"         2;
    "unavailable"  3;
    "recovering"   4;
    "unhealthy"    5;
    "checking"     6;
    "draining"     7;
    default        0;
}
```

Его использование:

```
http {

    include prometheus_all.conf;

    # ...

    server {

        listen 80;

        location =/p8s {
            prometheus all;
        }

        # ...

    }
}
```

```
$ curl localhost/p8s

    # Angie PRO Prometheus template "all"
    ...
```

Директивы

prometheus

Синтаксис	`prometheus` *имя_шаблона*;
По умолчанию	—
Контекст	location

Указывает для контекста `location` шаблон-обработчик, заданный директивой *prometheus_template*. При запросе этот `location` вычисляет и возвращает метрики шаблона в формате Prometheus.

```
location =/p8s {
    prometheus custom;
}
```

```
$ curl localhost/p8s

    # Angie PRO Prometheus template "custom"
    ...
```

prometheus_template

Синтаксис	`prometheus_template` *имя_шаблона* { ... }
По умолчанию	—
Контекст	http

Определяет именованный шаблон метрик, собираемых и экспортируемых Angie PRO, для использования с директивой *prometheus*.

Примечание

В состав Angie PRO также входит готовый шаблон *all*, куда включен набор наиболее общеупотребимых метрик.

Может содержать произвольное число определений метрик, каждая из которых имеет следующую структуру: <*имя_метрики*> <*переменная*> [`path=`<*строка_сопоставления*>] [`type=`<*тип*>] [`help=`<*справка*>];

`имя_метрики`	Задает имя метрики, под которым она будет добавлена в формате Prometheus в ответ на запрос. Может содержать необязательную часть с метками (`...`), например: `http_requests_total{method="$1",code="$2"}` В значениях меток можно использовать переменные Angie PRO; если *строка_сопоставления* задана регулярным выражением, то можно также использовать определенные в этом выражении группы захвата. Такие переменные и группы вычисляются при получении значения метрики, которое задает *переменная*.
`переменная`	Задает имя переменной, которая будет вычислена и добавлена как значение метрики в ответ на запрос. Если переменной нет или результат вычисления пуст (`""`), метрика не добавляется.

Метрика вычисляется со значением, которое задает *переменная*; при успехе вычисления метрика добавляется в ответ, например:

```
'angie_time{version="$angie_version"}' $msec;
```

```
$ curl localhost/p8s

   angie_time{version="1.7.0"} 1695119820.562
```

`path=строка_сопо`	Сопоставляется со всеми конечными путями метрик в поддереве */status* API-интерфейса Angie PRO, позволяя добавить в ответ сразу несколько экземпляров метрики.

При сопоставлении пути берутся с начальной косой чертой, но без конечной, например `/angie/generation`; при этом регистр символов не учитывается. Есть два способа сопоставления:

`path=точное_соот`	Проверяется посимвольным сравнением.
`path=~регулярное`	Проверяется при помощи библиотеки PCRE; может задавать группы захвата для использования в метках поля *имя метрики*.

Если *строка_сопоставления* соответствует какому-либо пути, то значение метрики Angie PRO по нему заносится в переменную *$p8s_value*, которую при заданном `path=` можно использовать в поле *переменная*.

В случае регулярного выражения совпадающих путей может быть несколько; метрика добавляется в ответ для *каждого* совпадения. В сочетании с группами захвата это позволяет получить ряд метрик с одним именем и разными метками, например:

```
'angie_slabs_slots_free{zone="$1",size="$2"}' $p8s_value
   path=~^/slabs/([^/]+)/slots/([^/]+)/free$;
```

Это определение добавляет метрики для всех зон и всех размеров, которые есть сейчас в конфигурации:

```
angie_slabs_slots_free{zone="one",size="8"} 502
angie_slabs_slots_free{zone="one",size="16"} 249
angie_slabs_slots_free{zone="one",size="32"} 122
angie_slabs_slots_free{zone="one",size="128"} 22
angie_slabs_slots_free{zone="one",size="512"} 4
angie_slabs_slots_free{zone="two",size="8"} 311
...
```

Если совпадений нет (при любом способе сопоставления), то метрика не добавляется.

> **Примечание**
>
> Параметр `path=` доступен только при сборке Angie PRO с модулем *API*.

`type=тип`, `help=справка`	Задают соответственно тип и справочную строку метрики в формате Prometheus, которые добавляются с ней в ответ без изменений и проверок.

Встроенные переменные

В модуле `http_prometheus` есть встроенная переменная, получающая значение при сопоставлении путей метрик из раздела */status* API-интерфейса Angie PRO с параметром *строка_сопоставления* метрик, заданных директивой *prometheus_template*.

`$p8s_value`

Если *строка_сопоставления* метрики, заданной в *prometheus_template*, соответствует какому-либо пути, то значение метрики Angie PRO, находящееся по этому пути, заносится в переменную `$p8s_value`. Она предназначена для использования в поле *переменная* в определениях метрик, которые вычисляются на основе параметра `path=`.

Значения метрик Angie PRO, заносимые в переменную `$p8s_value`, не всегда отвечают потребностям формата Prometheus. Тогда можно воспользоваться директивой *map*, например для преобразования строк в числа:

```
map $p8s_value $ups_state_n {
    up           0;
    unavailable  1;
    down         2;
    default      3;
}

prometheus_template main {
    'angie_http_upstreams_state{upstream="$1",peer="$2"}' $ups_state_n
        path=~^/http/upstreams/([^/]+)/peers/([^/]+)/state$;
}
```

Если у метрики Angie PRO логическое значение, то есть `true` или `false`, переменная получает значение `"1"` или `"0"` соответственно; если значение метрики — `null`, то переменная будет равна `"(null)"`. Для дат используется целочисленный формат эпохи UNIX.

Proxy

Позволяет передавать запросы другому (проксируемому) серверу.

Пример конфигурации

```
location / {
    proxy_pass       http://localhost:8000;
    proxy_set_header Host      $host;
    proxy_set_header X-Real-IP $remote_addr;
}
```

Директивы

proxy_bind

Синтаксис	`proxy_bind` *адрес* [transparent] | off;
По умолчанию	—
Контекст	http, server, location

Задает локальный IP-адрес с необязательным портом, который будет использоваться в исходящих соединениях с проксируемым сервером. В значении параметра допустимо использование переменных. Специальное значение `off` отменяет действие унаследованной с предыдущего уровня конфигурации директивы *proxy_bind*, позволяя системе самостоятельно выбирать локальный IP-адрес и порт.

Параметр `transparent` позволяет задать нелокальный IP-адрес, который будет использоваться в исходящих соединениях с проксируемым сервером, например, реальный IP-адрес клиента:

```
proxy_bind $remote_addr transparent;
```

Для работы параметра обычно требуется запустить рабочие процессы Angie PRO с привилегиями *суперпользователя*. В Linux это не требуется, так как если указан параметр *transparent*, то рабочие процессы наследуют *capability CAP_NET_RAW* из главного процесса.

Важно

Необходимо настроить таблицу маршрутизации ядра для перехвата сетевого трафика с проксируемого сервера.

proxy_buffer_size

Синтаксис	`proxy_buffer_size` *размер*;
По умолчанию	`proxy_buffer_size 4k|8k;`
Контекст	http, server, location

Задает размер буфера, в который будет читаться первая часть ответа, получаемого от проксируемого сервера. В этой части ответа обычно находится небольшой заголовок ответа. По умолчанию размер одного буфера равен размеру страницы памяти. В зависимости от платформы это или 4K, или 8K, однако его можно сделать меньше.

proxy_buffering

Синтаксис	`proxy_buffering` *размер*;
По умолчанию	`proxy_buffering on;`
Контекст	http, server, location

`on`	Angie PRO принимает ответ проксируемого сервера как можно быстрее, сохраняя его в буферы, заданные директивами *proxy_buffer_size* и *proxy_buffers*. Если ответ не вмещается целиком в память, то его часть может быть записана на диск во *временный файл*. Запись во временные файлы контролируется директивами *proxy_max_temp_file_size* и *proxy_temp_file_write_size*.
`off`	Ответ синхронно передается клиенту сразу же по мере его поступления. Angie PRO не пытается считать весь ответ проксируемого сервера. Максимальный размер данных, который Angie PRO может принять от сервера за один раз, задается директивой *proxy_buffer_size*.

Буферизация может быть также включена или выключена путем передачи значения «yes» или «no» в поле «X-Accel-Buffering» заголовка ответа. Эту возможность можно запретить с помощью директивы *proxy_ignore_headers*.

proxy_buffers

Синтаксис	`proxy_buffers` *число размер*;
По умолчанию	`proxy_buffers 8 4k|8k;`
Контекст	http, server, location

Задает число и размер буферов для одного соединения, в которые будет читаться ответ, получаемый от проксируемого сервера. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

proxy_busy_buffers_size

Синтаксис	`proxy_busy_buffers_size` *размер*;
По умолчанию	`proxy_buffers 8k|16k;`
Контекст	http, server, location

При включенной *буферизации* ответов проксируемого сервера, ограничивает суммарный размер буферов, которые могут быть заняты для отправки ответа клиенту, пока ответ еще не прочитан целиком. Оставшиеся буферы тем временем могут использоваться для чтения ответа и, при необходимости, буферизации части ответа во временный файл. По умолчанию размер ограничен величиной двух буферов, заданных директивами *proxy_buffer_size* и *proxy_buffers*.

proxy_cache

Синтаксис	`proxy_cache` *зона* | off [path=*путь*];
По умолчанию	`proxy_cache off;`
Контекст	http, server, location

Задает зону разделяемой памяти для кэширования. Одну и ту же зону можно использовать в нескольких местах конфигурации. В значении параметра допускаются переменные.

`off`	запрещает кэширование, унаследованное с предыдущего уровня конфигурации.

Добавлено в версии 1.2.0: PRO

В Angie PRO можно указать несколько директив *proxy_cache_path*, использующих одно и то же значение `keys_zone`, чтобы включить *шардинг кэша*. При этом следует задать параметр `path` директивы *proxy_cache*, использующей это значение `keys_zone`:

`path=`*путь*	Значение вычисляется в момент *кэширования* ответа от бэкенда и предполагает использование переменных, в том числе содержащих информацию из ответа. Если ответ берется из кэша, то *путь* не вычисляется заново; таким образом, кэшированный ответ сохраняет изначальный *путь*, пока не будет удален из кэша.

Это позволяет выбирать нужный путь кэша, применяя директивы *map* или скрипты к ответам от бэкенда. Пример для `Content-Type`:

```
proxy_cache_path /cache/one keys_zone=zone:10m;
proxy_cache_path /cache/two keys_zone=zone;

map $upstream_http_content_type $cache {
   ~^text/  one;
   default  two;
}

server {
   ...
   location / {
       proxy_pass http://backend;
       proxy_cache zone path=/cache/$cache;
   }
}
```

Здесь есть два пути кэша и отображение переменной, чтобы их различать. Если `Content-Type` начинается с `text/`, будет выбран первый путь, иначе — второй.

proxy_cache_background_update

Синтаксис	`proxy_cache_background_update` on | off;
По умолчанию	`proxy_cache_background_update off;`
Контекст	http, server, location

Позволяет запустить фоновый подзапрос для обновления просроченного элемента кэша, в то время как клиенту возвращается устаревший кэшированный ответ.

Внимание

Использование устаревшего кэшированного ответа в момент его обновления должно быть *разрешено*.

proxy_cache_bypass

Синтаксис	`proxy_cache_bypass` ...;
По умолчанию	—
Контекст	http, server, location

Задает условия, при которых ответ не будет браться из кэша. Если значение хотя бы одного из строковых параметров непустое и не равно «0», то ответ не берется из кэша:

```
proxy_cache_bypass $cookie_nocache $arg_nocache$arg_comment;
proxy_cache_bypass $http_pragma    $http_authorization;
```

Можно использовать совместно с директивой *proxy_no_cache*.

proxy_cache_convert_head

Синтаксис	`proxy_cache_convert_head` on | off;
По умолчанию	`proxy_cache_convert_head on;`
Контекст	http, server, location

Разрешает или запрещает преобразование метода «HEAD» в «GET» для кэширования. Если преобразование выключено, то необходимо, чтобы *ключ кэширования* включал в себя *$request_method*.

proxy_cache_key

Синтаксис	`proxy_cache_key` *строка*;
По умолчанию	`proxy_cache_key $scheme$proxy_host$request_uri;`
Контекст	http, server, location

Задает ключ для кэширования, например,

```
proxy_cache_key "$host$request_uri $cookie_user";
```

По умолчанию значение директивы близко к строке

```
proxy_cache_key $scheme$proxy_host$uri$is_args$args;
```

proxy_cache_lock

Синтаксис	`proxy_cache_lock` on | off;
По умолчанию	`proxy_cache_lock off;`
Контекст	http, server, location

Если включено, одновременно только одному запросу будет позволено заполнить новый элемент кэша, идентифицируемый согласно директиве *proxy_cache_key*, передав запрос на проксируемый сервер. Остальные запросы этого же элемента будут либо ожидать появления ответа в кэше, либо освобождения блокировки этого элемента, в течение времени, заданного директивой *proxy_cache_lock_timeout*.

proxy_cache_lock_age

Синтаксис	`proxy_cache_lock_age` *время*;
По умолчанию	`proxy_cache_lock_age 5s;`
Контекст	http, server, location

Если последний запрос, переданный на проксируемый сервер для заполнения нового элемента кэша, не завершился за указанное время, на проксируемый сервер может быть передан еще один запрос.

proxy_cache_lock_timeout

Синтаксис	`proxy_cache_lock_timeout` *время*;
По умолчанию	`proxy_cache_lock_timeout 5s;`
Контекст	http, server, location

Задает таймаут для *proxy_cache_lock*. По истечении указанного времени запрос будет передан на проксируемый сервер, однако ответ не будет кэширован.

proxy_cache_max_range_offset

Синтаксис	`proxy_cache_max_range_offset` *число*;
По умолчанию	—
Контекст	http, server, location

Задает смещение в байтах для запросов с указанием диапазона запрашиваемых байт (byte-range requests). Если диапазон находится за указанным смещением, range-запрос будет передан на проксируемый сервер и ответ не будет кэширован.

proxy_cache_methods

Синтаксис	`proxy_cache_methods` GET | HEAD | POST ...;
По умолчанию	`proxy_cache_methods GET HEAD;`
Контекст	http, server, location

Если метод запроса клиента указан в этой директиве, то ответ будет кэширован. Методы «GET» и «HEAD» всегда добавляются в список, но тем не менее рекомендуется перечислять их явно. См. также директиву *proxy_no_cache*.

proxy_cache_min_uses

Синтаксис	`proxy_cache_min_uses` *число*;
По умолчанию	`proxy_cache_min_uses 1;`
Контекст	http, server, location

Задает число запросов, после которого ответ будет кэширован.

proxy_cache_path

Синтаксис	`proxy_cache_path` *путь* [levels=*уровни*] [use_temp_path=on|off] keys_zone=*имя:размер* [inactive=*время*] [max_size=*размер*] [min_free=*размер*] [manager_files=*число*] [manager_sleep=*время*] [manager_threshold=*время*] [loader_files=*число*] [loader_sleep=*время*] [loader_threshold=*время*];
По умолчанию	—
Контекст	http

Задает *путь* и другие параметры кэша. Данные кэша хранятся в файлах. Именем файла в кэше является результат функции MD5 от *ключа кэширования*.

`levels`	задает уровни иерархии кэша: можно задать от 1 до 3 уровней, на каждом уровне допускаются значения 1 или 2.

Например, при использовании

```
proxy_cache_path /data/angie/cache levels=1:2 keys_zone=one:10m;
```

имена файлов в кэше будут такого вида:

```
/data/angie/cache/c/29/b7f54b2df7773722d382f4809d65029c
```

Кэшируемый ответ сначала записывается во временный файл, а потом этот файл переименовывается. Временные файлы и кэш могут располагаться на разных файловых системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если кэш будет находиться на той же файловой системе, что и каталог с временными файлами.

`use_temp_path=on`	определяет каталог, который будет использоваться для временных файлов
`on`	Если параметр не задан или установлен в значение `on`, будет использоваться каталог, задаваемый директивой *proxy_ temp_ path* для данного *location*
`off`	временные файлы будут располагаться непосредственно в каталоге кэша
`keys_zone`	Задает имя и размер зоны разделяемой памяти для хранения всех активных ключей и информации о данных. Зоны размером в 1 мегабайт достаточно для хранения около 8 тысяч ключей.
`inactive`	Если к данным кэша не обращаются в течение времени, заданного этим параметром, то данные удаляются, независимо от их свежести. По умолчанию *inactive* равен 10 минутам.

Примечание

Добавлено в версии 1.2.0: PRO

В Angie PRO можно задавать несколько директив *proxy_ cache_ path* с одним и тем же значением `keys_zone`. Размер зоны разделяемой памяти можно указывать только в первой из них. Выбор между директивами будет производиться на основе параметра `path` соответствующей директивы *proxy_ cache*.

Специальный процесс **cache manager** следит за максимальным размером кэша, а также за минимальным объемом свободного места на файловой системе с кэшем, и удаляет наименее востребованные данные при превышении максимального размера кэша или недостаточном объеме свободного места. Удаление данных происходит итерациями.

`max_size`	максимальное пороговое значение размера кэша
`min_free`	минимальное пороговое значение объема свободного места на файловой системе с кэшем
`manager_files`	максимальное количество удаляемых элементов кэша за одну итерацию По умолчанию *100*
`manager_threshol`	ограничивает время работы одной итерации По умолчанию *200* миллисекунд
`manager_sleep`	время, в течение которого выдерживается пауза между итерациями По умолчанию *50* миллисекунд

Через минуту после старта Angie PRO активируется специальный процесс **cache loader**, который загружает в зону кэша информацию о ранее кэшированных данных, хранящихся на файловой системе. Загрузка также происходит итерациями.

`loader_files`	максимальное количество элементов кэша к загрузке в одну итерацию По умолчанию *100*
`loader_threshold`	ограничивает время работы одной итерации По умолчанию *200* миллисекунд
`loader_sleep`	время, в течение которого выдерживается пауза между итерациями По умолчанию *50* миллисекунд

proxy_cache_revalidate

Синтаксис	`proxy_cache_revalidate` on | off;
По умолчанию	`proxy_cache_revalidate off;`
Контекст	http, server, location

Разрешает ревалидацию просроченных элементов кэша при помощи условных запросов с полями заголовка «If-Modified-Since» и «If-None-Match».

proxy_cache_use_stale

Синтаксис	`proxy_cache_use_stale` error | timeout | invalid_header | updating | http_500 | http_502 | http_503 | http_504 | http_403 | http_404 | http_429 | off ...;
По умолчанию	`proxy_cache_use_stale off;`
Контекст	http, server, location

Определяет, в каких случаях можно использовать устаревший кэшированный ответ. Параметры директивы совпадают с параметрами директивы *proxy_next_upstream*.

`error`	Позволяет использовать устаревший кэшированный ответ при невозможности выбора проксированного сервера для обработки запроса.
`updating`	Дополнительный параметр, разрешает использовать устаревший кэшированный ответ, если на данный момент он уже обновляется. Это позволяет минимизировать число обращений к проксированным серверам при обновлении кэшированных данных.

Использование устаревшего кэшированного ответа может также быть разрешено непосредственно в заголовке ответа на определенное количество секунд после того, как ответ устарел:

- Расширение stale-while-revalidate поля заголовка «Cache-Control» разрешает использовать устаревший кэшированный ответ, если на данный момент он уже обновляется.
- Расширение stale-if-error поля заголовка «Cache-Control» разрешает использовать устаревший кэшированный ответ в случае ошибки.

Примечание

Такой способ менее приоритетен, чем задание параметров директивы.

Чтобы минимизировать число обращений к проксированным серверам при заполнении нового элемента кэша, можно воспользоваться директивой *proxy_cache_lock*.

proxy_cache_valid

Синтаксис	`proxy_cache_valid` [*код* ...] *время*;
По умолчанию	—
Контекст	http, server, location

Задает время кэширования для разных кодов ответа. Например, директивы

```
proxy_cache_valid 200 302 10m;
proxy_cache_valid 404      1m;
```

задают время кэширования 10 минут для ответов с кодами 200 и 302 и 1 минуту для ответов с кодом 404.

Если указано только время кэширования,

```
proxy_cache_valid 5m;
```

то кэшируются только ответы 200, 301 и 302.

Кроме того, можно кэшировать любые ответы с помощью параметра `any`:

```
proxy_cache_valid 200 302 10m;
proxy_cache_valid 301      1h;
proxy_cache_valid any      1m;
```

Примечание

Параметры кэширования могут также быть заданы непосредственно в заголовке ответа. Такой способ приоритетнее, чем задание времени кэширования с помощью директивы.

- Поле заголовка «X-Accel-Expires» задает время кэширования ответа в секундах. Значение *0* запрещает кэшировать ответ. Если значение начинается с префикса *@*, оно задает абсолютное время в секундах с начала эпохи, до которого ответ может быть кэширован.
- Если в заголовке нет поля «X-Accel-Expires», параметры кэширования определяются по полям заголовка «Expires» или «Cache-Control».
- Ответ, в заголовке которого есть поле «Set-Cookie», не будет кэшироваться.
- Ответ, в заголовке которого есть поле «Vary» со специальным значением «*», не будет кэшироваться. Ответ, в заголовке которого есть поле «Vary» с другим значением, будет кэширован с учетом соответствующих полей заголовка запроса.

Обработка одного или более из этих полей заголовка может быть отключена при помощи директивы *proxy_ignore_headers*.

proxy_connect_timeout

Синтаксис	`proxy_connect_timeout` *время*;
По умолчанию	`proxy_connect_timeout 60s;`
Контекст	http, server, location

Задает таймаут для установления соединения с проксированным сервером. Необходимо иметь в виду, что этот таймаут обычно не может превышать 75 секунд.

proxy_connection_drop

Синтаксис	`proxy_connection_drop` *время* | on | off;
По умолчанию	`proxy_connection_drop off;`
Контекст	http, server, location

Настраивает завершение всех соединений с проксируемым сервером, если он был удален из группы или помечен как постоянно недоступный в результате процесса *reresolve* или *команды API* `DELETE`.

Соединение завершается, когда обрабатывается следующее событие чтения или записи для клиента или проксируемого сервера.

Установка *времени* включает *таймаут* до завершения соединения; при выборе значения `on` соединения завершаются немедленно.

proxy_cookie_domain

Синтаксис	`proxy_cookie_domain` off; `proxy_cookie_domain` *домен замена*;
По умолчанию	`proxy_cookie_domain off;`
Контекст	http, server, location

Задает текст, который нужно изменить в атрибуте domain полей «Set-Cookie» заголовка ответа проксируемого сервера. Предположим, проксируемый сервер вернул поле заголовка «Set-Cookie» с атрибутом «domain=localhost». Директива

```
proxy_cookie_domain localhost example.org;
```

перепишет данный атрибут в виде «domain=example.org».

Точка в начале строк *домен* и *замена*, а равно как и в атрибуте *domain* игнорируется. Регистр значения не имеет.

В строках *домен* и *замена* можно использовать переменные:

```
proxy_cookie_domain www.$host $host;
```

Директиву также можно задать при помощи регулярных выражений. При этом *домен* должен начинаться с символа «~». Регулярное выражение может содержать именованные и позиционные выделения, а *замена* ссылаться на них:

```
proxy_cookie_domain ~\.(?P<sl_domain>[-0-9a-z]+\.[a-z]+)$ $sl_domain;
```

На одном уровне может быть указано несколько директив *proxy_ cookie_ domain*:

```
proxy_cookie_domain localhost example.org;
proxy_cookie_domain ~\.([a-z]+\.[a-z]+)$ $1;
```

Если к cookie могут быть применены несколько директив, будет выбрана первая из них.

Параметр `off` отменяет действие унаследованных с предыдущего уровня конфигурации директив *proxy_ cookie_ domain*.

proxy_cookie_flags

Синтаксис	`proxy_cookie_flags` off | *cookie* [*флаг* ...];
По умолчанию	`proxy_cookie_flags off;`
Контекст	http, server, location

Задает один или несколько флагов для cookie. В качестве cookie можно использовать текст, переменные и их комбинации. В качестве флага можно использовать текст, переменные и их комбинации.

Параметры *secure*, *httponly*, *samesite=strict*, *samesite=lax*, *samesite=none* добавляют соответствующие флаги.

Параметры *nosecure*, *nohttponly*, *nosamesite* удаляют соответствующие флаги.

Cookie также можно задать при помощи регулярных выражений. При этом cookie должен начинаться с символа «~».

На одном уровне конфигурации может быть указано несколько директив *proxy_ cookie_ flags*:

```
proxy_cookie_flags one httponly;
proxy_cookie_flags ~ nosecure samesite=strict;
```

Если к cookie могут быть применены несколько директив, будет выбрана первая из них. В данном примере флаг *httponly* добавляется к cookie *one*, для остальных cookie добавляется флаг *samesite=strict* и удаляется флаг *secure*.

Параметр `off` отменяет действие всех директив *proxy_ cookie_ flags* на данном уровне.

proxy_cookie_path

Синтаксис	`proxy_cookie_path` off; `proxy_cookie_path` *путь замена*;
По умолчанию	`proxy_cookie_path off;`
Контекст	http, server, location

Задает текст, который нужно изменить в атрибуте path полей «Set-Cookie» заголовка ответа проксируемого сервера. Предположим, проксируемый сервер вернул поле заголовка «Set-Cookie» с атрибутом «path=/two/some/uri/». Директива

```
proxy_cookie_path /two/ /;
```

перепишет данный атрибут в виде «path=/some/uri/».

В строках *путь* и *замена* можно использовать переменные:

```
proxy_cookie_path $uri /some$uri;
```

Директиву также можно задать при помощи регулярных выражений. При этом *путь* должен начинаться либо с символа «~», если при сравнении следует учитывать регистр символов, либо с символов «~*», если регистр символов учитывать не нужно. Регулярное выражение может содержать именованные и позиционные выделения, а *замена* ссылаться на них:

```
proxy_cookie_path ~*^/user/([^/]+) /u/$1;
```

На одном уровне может быть указано несколько директив *proxy_cookie_path*:

```
proxy_cookie_path /one/ /;
proxy_cookie_path / /two/;
```

Если к cookie могут быть применены несколько директив, будет выбрана первая из них.

Параметр `off` отменяет действие унаследованных с предыдущего уровня конфигурации директив *proxy_cookie_path*.

proxy_force_ranges

Синтаксис	`proxy_force_ranges` off;
По умолчанию	`proxy_force_ranges off;`
Контекст	http, server, location

Включает поддержку диапазонов запрашиваемых байт (byte-range) для кэшированных и некэшированных ответов проксируемого сервера вне зависимости от наличия поля «Accept-Ranges» в заголовках этих ответов.

proxy_headers_hash_bucket_size

Синтаксис	`proxy_headers_hash_bucket_size` *размер*;
По умолчанию	`proxy_headers_hash_bucket_size 64;`
Контекст	http, server, location

Задает размер корзины для хэш-таблиц, используемых директивами *proxy_hide_header* и *proxy_set_header*. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

proxy_headers_hash_max_size

Синтаксис	`proxy_headers_hash_max_size` *размер*;
По умолчанию	`proxy_headers_hash_max_size 512;`
Контекст	http, server, location

Задает максимальный размер хэш-таблиц, используемых директивами *proxy_hide_header* и *proxy_set_header*. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

proxy_hide_header

Синтаксис	`proxy_hide_header` *поле*;
По умолчанию	—
Контекст	http, server, location

По умолчанию Angie PRO не передает клиенту поля заголовка «Date», «Server», «X-Pad» и «X-Accel-...» из ответа проксированного сервера. Директива *proxy_hide_header* задает дополнительные поля, которые не будут передаваться. Если же передачу полей нужно разрешить, можно воспользоваться директивой *proxy_pass_header*.

proxy_http_version

Синтаксис	`proxy_http_version` 1.0 | 1.1 | 3;
По умолчанию	`proxy_http_version 1.0;`
Контекст	http, server, location, if в location, limit_except

Задает версию протокола HTTP для проксирования. По умолчанию используется версия 1.0. Для работы *постоянных соединений* рекомендуется версия 1.1 или выше.

proxy_http3_hq

Синтаксис	`proxy_http3_hq` on | off;
По умолчанию	`proxy_http3_hq off;`
Контекст	http, server

Отключает или включает особый режим согласования `hq-interop`, используемый в функциональных тестах *QUIC*, на которые полагается Angie PRO.

proxy_http3_max_concurrent_streams

Синтаксис	`proxy_http3_max_concurrent_streams` *число*;
По умолчанию	`proxy_http3_max_concurrent_streams 128;`
Контекст	http, server

Задает максимальное число параллельных HTTP/3-потоков в *соединении*. Требует включения *постоянных соединений*.

proxy_http3_stream_buffer_size

Синтаксис	`proxy_http3_stream_buffer_size` *размер*;
По умолчанию	`proxy_http3_stream_buffer_size 64k;`
Контекст	http, server

Задает *размер* буфера, используемого для чтения и записи *QUIC-потоков*.

proxy_ignore_client_abort

Синтаксис	`proxy_ignore_client_abort` on | off;
По умолчанию	`proxy_ignore_client_abort off;`
Контекст	http, server, location

Определяет, закрывать ли соединение с проксируемым сервером в случае, если клиент закрыл соединение, не дождавшись ответа.

proxy_ignore_headers

Синтаксис	`proxy_ignore_headers` *поле* ...;
По умолчанию	—
Контекст	http, server, location

Запрещает обработку некоторых полей заголовка из ответа проксированного сервера. В директиве можно указать поля «X-Accel-Redirect», «X-Accel-Expires», «X-Accel-Limit-Rate», «X-Accel-Buffering», «X-Accel-Charset», «Expires», «Cache-Control», «Set-Cookie» и «Vary».

Если не запрещено, обработка этих полей заголовка заключается в следующем:

- «X-Accel-Expires», «Expires», «Cache-Control», «Set-Cookie» и «Vary» задают *параметры кэширования* ответа;
- «X-Accel-Redirect» производит *внутреннее перенаправление* на указанный URI;
- «X-Accel-Limit-Rate» задает *ограничение скорости* передачи ответа клиенту;
- «X-Accel-Buffering» включает или выключает *буферизацию* ответа;
- «X-Accel-Charset» задает желаемую *кодировку* ответа.

proxy_intercept_errors

Синтаксис	`proxy_intercept_errors` on | off;
По умолчанию	`proxy_intercept_errors off;`
Контекст	http, server, location

Определяет, передавать ли клиенту проксированные ответы с кодом больше либо равным 300, или же перехватывать их и перенаправлять на обработку Angie PRO с помощью директивы *error_page*.

proxy_limit_rate

Синтаксис	`proxy_limit_rate` *скорость*;
По умолчанию	`proxy_limit_rate 0;`
Контекст	http, server, location

Ограничивает скорость чтения ответа от проксируемого сервера. *Скорость* задается в байтах в секунду; можно использовать переменные.

0	отключает ограничение скорости

Примечание

Ограничение устанавливается на запрос, поэтому, если Angie PRO одновременно откроет два соединения к проксируемому серверу, суммарная скорость будет вдвое выше заданного ограничения. Ограничение работает только в случае, если включена *буферизация* ответов проксируемого сервера.

proxy_max_temp_file_size

Синтаксис	`proxy_max_temp_file_size` *размер*;
По умолчанию	`proxy_max_temp_file_size 1024m;`
Контекст	http, server, location

Если включена *буферизация* ответов проксируемого сервера, и ответ не вмещается целиком в буферы, заданные директивами *proxy_buffer_size* и *proxy_buffers*, часть ответа может быть записана во временный файл. Эта директива задает максимальный размер временного файла. Размер данных, сбрасываемых во временный файл за один раз, задается директивой *proxy_temp_file_write_size*.

0	отключает возможность буферизации ответов во временные файлы

Примечание

Данное ограничение не распространяется на ответы, которые будут *кэшированы* или сохранены *на диске*.

proxy_method

Синтаксис	`proxy_method` *метод*;
По умолчанию	—
Контекст	http, server, location

Задает HTTP-метод, который будет использоваться в передаваемых на проксируемый сервер запросах вместо метода из клиентского запроса. В значении параметра допустимо использование переменных.

proxy_next_upstream

Синтаксис	`proxy_next_upstream` error | timeout | invalid_header | http_500 | http_502 | http_503 | http_504 | http_403 | http_404 | http_429 | non_idempotent | off . . . ;
По умолчанию	`proxy_next_upstream error timeout;`
Контекст	http, server, location

Определяет, в каких случаях запрос будет передан следующему в группе *upstream* серверу:

`error`	произошла ошибка соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`timeout`	произошел таймаут во время соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`invalid_header`	сервер вернул пустой или неверный ответ;
`http_500`	сервер вернул ответ с кодом 500;
`http_502`	сервер вернул ответ с кодом 502;
`http_503`	сервер вернул ответ с кодом 503;
`http_504`	сервер вернул ответ с кодом 504;
`http_403`	сервер вернул ответ с кодом 403;
`http_404`	сервер вернул ответ с кодом 404;
`http_429`	сервер вернул ответ с кодом 429;
`non_idempotent`	обычно запросы с неидемпотентным методом (*POST*, *LOCK*, *PATCH*) не передаются на другой сервер, если запрос серверу группы уже был отправлен; включение параметра явно разрешает повторять подобные запросы;
`off`	запрещает передачу запроса следующему серверу.

Примечание

Необходимо понимать, что передача запроса следующему серверу возможна только при условии, что клиенту еще ничего не передавалось. То есть, если ошибка или таймаут возникли в середине передачи ответа клиенту, то действие директивы на такой запрос не распространяется.

Директива также определяет, что считается *неудачной попыткой* работы с сервером.

`error timeout invalid_header`	всегда считаются неудачными попытками, даже если они не указаны в директиве
`http_500 http_502 http_503 http_504 http_429`	считаются неудачными попытками, только если они указаны в директиве
`http_403 http_404`	никогда не считаются неудачными попытками

Передача запроса следующему серверу может быть ограничена по *количеству попыток* и по *времени*.

proxy_next_upstream_timeout

Синтаксис	`proxy_next_upstream_timeout` *время*;
По умолчанию	`proxy_next_upstream_timeout 0;`
Контекст	http, server, location

Ограничивает время, в течение которого возможна передача запроса *следующему* серверу.

`0`	отключает это ограничение

proxy_next_upstream_tries

Синтаксис	`proxy_next_upstream_tries` *число*;
По умолчанию	`proxy_next_upstream_tries 0;`
Контекст	http, server, location

Ограничивает число допустимых попыток для передачи запроса *следующему* серверу.

`0`	отключает это ограничение

proxy_no_cache

Синтаксис	`proxy_no_cache` *строка* ...;
По умолчанию	—
Контекст	http, server, location

Задает условия, при которых ответ не будет сохраняться в кэш. Если значение хотя бы одного из строковых параметров непустое и не равно «0», то ответ не будет сохранен:

```
proxy_no_cache $cookie_nocache $arg_nocache$arg_comment;
proxy_no_cache $http_pragma    $http_authorization;
```

Можно использовать совместно с директивой *proxy_ cache_ bypass*.

proxy_pass

Синтаксис	proxy_pass URL;
По умолчанию	—
Контекст	location, if в location, limit_except

Задает протокол и адрес проксируемого сервера, а также необязательный URI, на который должен отображаться location. В качестве протокола можно указать `http` или `https`. Адрес может быть указан в виде доменного имени или IP-адреса, и необязательного порта:

```
proxy_pass http://localhost:8000/uri/;
```

или в виде пути UNIX-сокета, который указывается после слова `unix` и заключается в двоеточия:

```
proxy_pass http://unix:/tmp/backend.socket:/uri/;
```

Если доменному имени соответствует несколько адресов, то все они будут использоваться по очереди (round-robin). Кроме того, в качестве адреса можно указать *группу серверов*. Если используется группа, указать порт невозможно; вместо этого укажите порт для каждого сервера внутри группы отдельно.

В значении параметра можно использовать переменные. В этом случае, если адрес указан в виде доменного имени, имя ищется среди описанных групп серверов и если не найдено, то определяется с помощью *resolver*'а.

URI запроса передается на сервер так:

- Если директива *proxy_ pass* указана **с URI**, то при передаче запроса серверу часть *нормализованного* URI запроса, соответствующая location, заменяется на URI, указанный в директиве:

```
location /name/ {
    proxy_pass http://127.0.0.1/remote/;
}
```

- Если директива proxy_pass указана **без URI**, то при обработке первоначального запроса на сервер передается URI запроса в том же виде, в каком его прислал клиент, а при обработке измененного URI - нормализованный URI запроса целиком:

```
location /some/path/ {
    proxy_pass http://127.0.0.1;
}
```

В ряде случаев часть URI запроса, подлежащую замене, выделить невозможно:

- Если *location* задан регулярным выражением, а также в именованных *location*'ах.

В этих случаях *proxy_ pass* следует указывать без URI.

- Если внутри проксируемого *location* с помощью директивы *rewrite* изменяется URI, и именно с этой конфигурацией будет обрабатываться запрос (*break*):

```
location /name/ {
    rewrite    /name/([^/]+) /users?name=$1 break;
    proxy_pass http://127.0.0.1;
}
```

В этом случае URI, указанный в директиве, игнорируется, и на сервер передается измененный URI запроса целиком.

- При использовании переменных в *proxy_pass*:

```
location /name/ {
    proxy_pass http://127.0.0.1$request_uri;
}
```

В этом случае если в директиве указан URI, он передается на сервер как есть, заменяя URI первоначального запроса.

Проксирование WebSocket требует особой *настройки*.

proxy_pass_header

Синтаксис	`proxy_pass_header` *поле* ...;
По умолчанию	—
Контекст	http, server, location

Разрешает передавать от проксируемого сервера клиенту *запрещенные для передачи* поля заголовка.

proxy_pass_request_body

Синтаксис	`proxy_pass_request_body` on | off;
По умолчанию	`proxy_pass_request_body on;`
Контекст	http, server, location

Позволяет запретить передачу исходного тела запроса на проксируемый сервер.

```
location /x-accel-redirect-here/ {
    proxy_method GET;
    proxy_pass_request_body off;
    proxy_set_header Content-Length "";

    proxy_pass ...;
}
```

См. также директивы *proxy_set_header* и *proxy_pass_request_headers*.

proxy_pass_request_headers

Синтаксис	`proxy_pass_request_headers` on | off;
По умолчанию	`proxy_pass_request_headers on;`
Контекст	http, server, location

Позволяет запретить передачу полей заголовка исходного запроса на проксируемый сервер.

```
location /x-accel-redirect-here/ {
    proxy_method GET;
    proxy_pass_request_headers off;
    proxy_pass_request_body off;

    proxy_pass ...;
}
```

См. также директивы *proxy_set_header* и *proxy_pass_request_body*.

proxy_quic_active_connection_id_limit

Синтаксис	`proxy_quic_active_connection_id_limit` *число*;
По умолчанию	`proxy_quic_active_connection_id_limit 2;`
Контекст	http, server

Задает значение транспортного параметра *QUIC* `active_connection_id_limit`. Это максимальное число активных идентификаторов соединений, поддерживаемых для одного сервера.

proxy_quic_gso

Синтаксис	`proxy_quic_gso` on | off;
По умолчанию	`proxy_quic_gso off;`
Контекст	http, server

Отключает или включает отправку данных в оптимизированном пакетном режиме *QUIC*, использующем программное снижение нагрузки путем сегментации (generic segmentation offload).

proxy_quic_host_key

Синтаксис	`proxy_quic_host_key` *файл*;
По умолчанию	—
Контекст	http, server

Задает *файл* с секретным ключом, применяемым в *QUIC* при шифровании токенов Stateless Reset и Address Validation. По умолчанию случайный ключ создается при каждом перезапуске. Токены, созданные при помощи старых ключей, не принимаются.

proxy_read_timeout

Синтаксис	`proxy_read_timeout` *время*;
По умолчанию	`proxy_read_timeout 60s;`
Контекст	http, server, location

Задает таймаут при чтении ответа проксированного сервера. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями чтения. Если по истечении этого времени проксируемый сервер ничего не передаст, соединение закрывается.

proxy_redirect

Синтаксис	`proxy_redirect` default; `proxy_redirect` off; `proxy_redirect` *перенаправление замена*;
По умолчанию	`proxy_redirect default;`
Контекст	http, server, location

Задает текст, который нужно изменить в полях заголовка «Location» и «Refresh» в ответе проксируемого сервера.

Предположим, проксируемый сервер вернул поле заголовка:

```
Location: http://localhost:8000/two/some/uri/
```

Директива

```
proxy_redirect http://localhost:8000/two/ http://frontend/one/;
```

перепишет эту строку в виде:

```
Location: http://frontend/one/some/uri/
```

В заменяемой строке можно не указывать имя сервера:

```
proxy_redirect http://localhost:8000/two/ /;
```

тогда будут подставлены основное имя сервера и порт, если он отличен от 80.

Стандартная замена, задаваемая параметром `default`, использует параметры директив *location* и *proxy_pass*. Поэтому две нижеприведенные конфигурации одинаковы:

```
location /one/ {
    proxy_pass     http://upstream:port/two/;
    proxy_redirect default;
```

```
location /one/ {
    proxy_pass     http://upstream:port/two/;
    proxy_redirect http://upstream:port/two/ /one/;
```

Осторожно

Параметр `default` недопустим, если в *proxy_pass* используются переменные.

В строке *замена* можно использовать переменные:

```
proxy_redirect http://localhost:8000/ http://$host:$server_port/;
```

В строке *перенаправление* тоже можно использовать переменные:

```
proxy_redirect http://$proxy_host:8000/ /;
```

Директиву также можно задать при помощи регулярных выражений. При этом *перенаправление* должно начинаться либо с символа «~», если при сравнении следует учитывать регистр символов, либо с символов «~*», если регистр символов учитывать не нужно. Регулярное выражение может содержать именованные и позиционные выделения, а *замена* ссылаться на них:

```
proxy_redirect ~^(http://[^:]+):\d+(/.+)$ $1$2;
proxy_redirect ~*/user/([^/]+)/(.+)$      http://$1.example.com/$2;
```

На одном уровне может быть указано несколько директив *proxy_redirect*:

```
proxy_redirect default;
proxy_redirect http://localhost:8000/  /;
proxy_redirect http://www.example.com/ /;
```

Если к полям заголовка в ответе проксируемого сервера могут быть применены несколько директив, будет выбрана первая из них.

Параметр `off` отменяет действие унаследованных с предыдущего уровня конфигурации директив *proxy_redirect*.

С помощью этой директивы можно также добавлять имя хоста к относительным перенаправлениям, выдаваемым проксируемым сервером:

```
proxy_redirect / /;
```

proxy_request_buffering

Синтаксис	`proxy_request_buffering` on | off;
По умолчанию	`proxy_request_buffering on;`
Контекст	http, server, location

Разрешает или запрещает использовать буферизацию тела запроса клиента.

`on`	тело запроса полностью *читается* от клиента перед отправкой запроса на проксируемый сервер.
`off`	тело запроса отправляется на проксируемый сервер сразу же по мере его поступления. В этом случае запрос не может быть передан *следующему серверу*, если Angie PRO уже начал отправку тела запроса.

Если для отправки тела исходного запроса используется HTTP/1.1 и передача данных частями (chunked transfer encoding), то тело запроса буферизуется независимо от значения директивы, если для проксирования также не *включен* HTTP/1.1.

proxy_send_lowat

Синтаксис	`proxy_send_lowat` *размер*;
По умолчанию	`proxy_send_lowat 0;`
Контекст	http, server, location

При установке директивы в ненулевое значение Angie PRO будет пытаться минимизировать число операций отправки на исходящих соединениях с проксируемым сервером либо при помощи флага `NOTE_LOWAT` метода *kqueue*, либо при помощи параметра сокета `SO_SNDLOWAT`, с указанным размером.

Примечание

Эта директива игнорируется на Linux, Solaris и Windows.

proxy_send_timeout

Синтаксис	`proxy_send_timeout` *время*;
По умолчанию	`proxy_send_timeout 60s;`
Контекст	http, server, location

Задает таймаут при передаче запроса проксируемому серверу. Таймаут устанавливается не на всю передачу запроса, а только между двумя операциями записи. Если по истечении этого времени проксируемый сервер не примет новых данных, соединение закрывается.

proxy_set_body

Синтаксис	`proxy_set_body` *значение*;
По умолчанию	—
Контекст	http, server, location

Позволяет переопределить тело запроса, передаваемое на проксируемый сервер. В качестве значения можно использовать текст, переменные и их комбинации.

proxy_set_header

Синтаксис	`proxy_set_header` *поле значение*;
По умолчанию	`proxy_set_header Host $proxy_host;`
Контекст	http, server, location

Позволяет переопределять или добавлять поля заголовка запроса, *передаваемые* проксируемому серверу. В качестве *значения* можно использовать текст, переменные и их комбинации. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *proxy_set_header*. По умолчанию переопределяются только два поля:

```
proxy_set_header Host       $proxy_host;
proxy_set_header Connection close;
```

Если включено кэширование, поля заголовка «If-Modified-Since», «If-Unmodified-Since», «If-None-Match», «If-Match», «Range» и «If-Range» исходного запроса не передаются на проксируемый сервер.

Неизмененное поле заголовка запроса «Host» можно передать так:

```
proxy_set_header Host       $http_host;
```

Однако, если это поле отсутствует в заголовке запроса клиента, то ничего передаваться не будет. В этом случае лучше воспользоваться переменной *$host* - ее значение равно имени сервера в поле «Host» заголовка запроса, или же основному имени сервера, если поля нет:

```
proxy_set_header Host       $host;
```

Кроме того, можно передать имя сервера вместе с портом проксируемого сервера:

```
proxy_set_header Host       $host:$proxy_port;
```

Если значение поля заголовка — пустая строка, то поле вообще не будет передаваться проксируемому серверу:

```
proxy_set_header Accept-Encoding "";
```

proxy_socket_keepalive

Синтаксис	`proxy_socket_keepalive` on | off;
По умолчанию	`proxy_socket_keepalive off;`
Контекст	http, server, location

Конфигурирует поведение «TCP keepalive» для исходящих соединений к проксируемому серверу.

`""`	По умолчанию для сокета действуют настройки операционной системы.
`on`	для сокета включается параметр *SO_KEEPALIVE*

proxy_ssl_certificate

Синтаксис	`proxy_ssl_certificate` *файл* [*файл*];
По умолчанию	—
Контекст	http, server, location

Задает файл с сертификатом в формате PEM для аутентификации на проксируемом HTTPS-сервере. В имени файла можно использовать переменные.

Добавлено в версии 1.2.0.

При включенном *proxy_ssl_ntls* директива принимает два аргумента вместо одного:

```
location /proxy {
    proxy_ssl_ntls  on;

    proxy_ssl_certificate      sign.crt enc.crt;
    proxy_ssl_certificate_key  sign.key enc.key;

    proxy_ssl_ciphers "ECC-SM2-WITH-SM4-SM3:ECDHE-SM2-WITH-SM4-SM3:RSA";

    proxy_pass https://backend:443;
}
```

proxy_ssl_certificate_key

Синтаксис	`proxy_ssl_certificate_key` *файл* [*файл*];
По умолчанию	—
Контекст	http, server, location

Задает файл с секретным ключом в формате PEM для аутентификации на проксируемом HTTPS-сервере.

Вместо файла можно указать значение «engine:*имя*:id», которое загружает ключ с указанным *id* из OpenSSL engine с заданным именем.

В имени файла можно использовать переменные.

Добавлено в версии 1.2.0.

При включенном *proxy_ssl_ntls* директива принимает два аргумента вместо одного:

```
location /proxy {
    proxy_ssl_ntls  on;

    proxy_ssl_certificate      sign.crt enc.crt;
    proxy_ssl_certificate_key  sign.key enc.key;

    proxy_ssl_ciphers "ECC-SM2-WITH-SM4-SM3:ECDHE-SM2-WITH-SM4-SM3:RSA";

    proxy_pass https://backend:443;
}
```

proxy_ssl_ciphers

Синтаксис	`proxy_ssl_ciphers` *шифры*;
По умолчанию	`proxy_ssl_ciphers DEFAULT;`
Контекст	http, server, location

Описывает разрешенные шифры для запросов к проксируемому HTTPS-серверу. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL.

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

proxy_ssl_conf_command

Синтаксис	`proxy_ssl_conf_command` *имя значение*;
По умолчанию	—
Контекст	http, server, location

Задает произвольные конфигурационные команды OpenSSL при установлении соединения с проксируемым HTTPS-сервером.

Важно

Директива поддерживается при использовании OpenSSL 1.0.2 и выше.

На одном уровне может быть указано несколько директив *proxy_ssl_conf_command*. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *proxy_ssl_conf_command*.

Осторожно

Следует учитывать, что изменение настроек OpenSSL напрямую может привести к неожиданному поведению.

proxy_ssl_crl

Синтаксис	`proxy_ssl_crl` *файл*;
По умолчанию	—
Контекст	http, server, location

Указывает файл с отозванными сертификатами (CRL) в формате PEM, используемыми при *проверке* сертификата проксируемого HTTPS-сервера.

proxy_ssl_name

Синтаксис	`proxy_ssl_name` *имя*;
По умолчанию	`proxy_ssl_name $proxy_host;`
Контекст	http, server, location

Позволяет переопределить имя сервера, используемое при *проверке* сертификата проксируемого HTTPS-сервера, а также для *передачи его через SNI* при установлении соединения с проксируемым HTTPS-сервером.

По умолчанию используется имя хоста из URL'а, заданного директивой *proxy_pass*.

proxy_ssl_ntls

Добавлено в версии 1.2.0.

Синтаксис	`proxy_ssl_ntls on | off;`
По умолчанию	`proxy_ssl_ntls off;`
Контекст	http, server

Включает клиентскую поддержку NTLS при использовании TLS библиотеки TongSuo.

```
location /proxy {
    proxy_ssl_ntls  on;

    proxy_ssl_certificate      sign.crt enc.crt;
    proxy_ssl_certificate_key  sign.key enc.key;

    proxy_ssl_ciphers "ECC-SM2-WITH-SM4-SM3:ECDHE-SM2-WITH-SM4-SM3:RSA";

    proxy_pass https://backend:443;
}
```

Важно

Angie PRO необходимо собрать с использованием параметра конфигурации *–with-ntls*, с соответствующей SSL библиотекой с поддержкой NTLS

```
./configure --with-openssl=../Tongsuo-8.3.0 \
            --with-openssl-opt=enable-ntls  \
            --with-ntls
```

proxy_ssl_password_file

Синтаксис	`proxy_ssl_password_file` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с паролями от *секретных ключей*, где каждый пароль указан на отдельной строке. Пароли применяются по очереди в момент загрузки ключа.

proxy_ssl_protocols

Синтаксис	`proxy_ssl_protocols` [SSLv2] [SSLv3] [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`proxy_ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;`
Контекст	http, server, location

Изменено в версии 1.2.0: Параметр `TLSv1.3` добавлен к используемым по умолчанию.

Разрешает указанные протоколы для запросов к проксируемому HTTPS-серверу.

proxy_ssl_server_name

Синтаксис	`proxy_ssl_server_name` on | off;
По умолчанию	`proxy_ssl_server_name off;`
Контекст	http, server, location

Разрешает или запрещает передачу имени сервера, заданного директивой *proxy_ssl_name*, через расширение Server Name Indication протокола TLS (SNI, RFC 6066) при установлении соединения с проксируемым HTTPS-сервером.

proxy_ssl_session_reuse

Синтаксис	`proxy_ssl_session_reuse` on | off;
По умолчанию	`proxy_ssl_session_reuse on;`
Контекст	http, server, location

Определяет, использовать ли повторно SSL-сессии при работе с проксируемым сервером. Если в логах появляются ошибки «*SSL3_GET_FINISHED:digest check failed*», то можно попробовать выключить повторное использование сессий.

proxy_ssl_trusted_certificate

Синтаксис	`proxy_ssl_trusted_certificate` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с доверенными сертификатами CA в формате PEM, используемыми при *проверке* сертификата проксируемого HTTPS-сервера.

proxy_ssl_verify

Синтаксис	`proxy_ssl_verify` on | off;
По умолчанию	`proxy_ssl_verify off;`
Контекст	http, server, location

Разрешает или запрещает проверку сертификата проксируемого HTTPS-сервера.

proxy_ssl_verify_depth

Синтаксис	`proxy_ssl_verify_depth` *число*;
По умолчанию	`proxy_ssl_verify_depth 1;`
Контекст	http, server, location

Устанавливает глубину проверки в цепочке сертификатов проксируемого HTTPS-сервера.

proxy_store

Синтаксис	`proxy_store` on | off | *строка*;
По умолчанию	`proxy_store off;`
Контекст	http, server, location

Разрешает сохранение на диск файлов.

`on`	сохраняет файлы в соответствии с путями, указанными в директивах *alias* или *root*
`off`	запрещает сохранение файлов

Имя файла можно задать явно с помощью `строки` с переменными:

```
proxy_store /data/www$original_uri;
```

Время изменения файлов выставляется согласно полученному полю «Last-Modified» в заголовке ответа. Ответ сначала записывается во временный файл, а потом этот файл переименовывается. Временный файл и постоянное место хранения ответа могут располагаться на разных файловых системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если сохраняемые файлы будут находиться на той же файловой системе, что и каталог с временными файлами, задаваемый директивой *proxy_temp_path* для данного *location*.

Директиву можно использовать для создания локальных копий статических неизменяемых файлов, например, так:

```
location /images/ {
    root                /data/www;
    error_page          404 = /fetch$uri;
}

location /fetch/ {
    internal;

    proxy_pass          http://backend/;
    proxy_store         on;
    proxy_store_access  user:rw group:rw all:r;
    proxy_temp_path     /data/temp;

    alias               /data/www/;
}
```

или так:

```
location /images/ {
    root               /data/www;
    error_page         404 = @fetch;
}

location @fetch {
    internal;

    proxy_pass         http://backend;
    proxy_store        on;
    proxy_store_access user:rw group:rw all:r;
    proxy_temp_path    /data/temp;

    root               /data/www;
}
```

proxy_store_access

Синтаксис	`proxy_store_access` *пользователи:права* ...;
По умолчанию	`proxy_store_access user:rw;`
Контекст	http, server, location

Задает права доступа для создаваемых файлов и каталогов, например,

```
proxy_store_access user:rw group:rw all:r;
```

Если заданы какие-либо права для *group* или *all*, то права для user указывать необязательно:

```
proxy_store_access group:rw all:r;
```

proxy_temp_file_write_size

Синтаксис	`proxy_temp_file_write_size` *размер*;
По умолчанию	`proxy_temp_file_write_size 8k|16k;`
Контекст	http, server, location

Ограничивает размер данных, сбрасываемых во временный файл за один раз, при включенной буферизации ответов проксируемого сервера во временные файлы. По умолчанию размер ограничен двумя буферами, заданными директивами *proxy_buffer_size* и *proxy_buffers*. Максимальный размер временного файла задается директивой *proxy_max_temp_file_size*.

proxy_temp_path

Синтаксис	`proxy_temp_path` *путь* [*уровень1* [*уровень2* [*уровень3*]]]`;`
По умолчанию	`proxy_temp_path proxy_temp;`
Контекст	http, server, location

Задает имя каталога для хранения временных файлов с данными, полученными от проксируемых серверов. В каталоге может использоваться иерархия подкаталогов до трех уровней. Например, при такой конфигурации

```
proxy_temp_path /spool/angie/proxy_temp 1 2;
```

временный файл будет следующего вида:

```
/spool/angie/proxy_temp/7/45/00000123457
```

См. также параметр *use_temp_path* директивы *proxy_cache_path*.

Встроенные переменные

В модуле *http_proxy* есть встроенные переменные, которые можно использовать для формирования заголовков с помощью директивы *proxy_set_header*:

`$proxy_host`

имя и порт проксируемого сервера, как указано в директиве *proxy_pass*;

`$proxy_port`

порт проксируемого сервера, как указано в директиве *proxy_pass*, или стандартный порт протокола;

`$proxy_add_x_forwarded_for`

поле заголовка запроса клиента «X-Forwarded-For» и добавленная к нему через запятую переменная *$remote_addr*. Если же поля «X-Forwarded-For» в заголовке запроса клиента нет, то переменная *$proxy_add_x_forwarded_for* равна переменной *$remote_addr*.

Random Index

Обслуживает запросы, оканчивающиеся косой чертой (/), и выдает случайный файл в качестве индексного файла каталога. Модуль выполняется до модуля *http_index*.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_random_index_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
location / {
    random_index on;
}
```

Директивы

random_index

Синтаксис	`random_index` on | off.;
По умолчанию	`random_index off;`
Контекст	location

Разрешает или запрещает в содержащем *location* обработку этим модулем.

RealIP

Позволяет менять адрес и необязательный порт клиента на переданные в указанном поле заголовка.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_realip_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
set_real_ip_from  192.168.1.0/24;
set_real_ip_from  192.168.2.1;
set_real_ip_from  2001:0db8::/32;
real_ip_header    X-Forwarded-For;
real_ip_recursive on;
```

Директивы

set_real_ip_from

Синтаксис	`set_real_ip_from` *адрес* | *CIDR* | unix:;
По умолчанию	—
Контекст	http, server, location

Задает доверенные адреса, которые передают верный адрес для замены. Если указано специальное значение `unix:`, доверенными будут считаться все UNIX-сокеты. Доверенные адреса могут быть также заданы при помощи имени хоста.

real_ip_header

Синтаксис	`real_ip_header` *поле* | X-Real-IP | X-Forwarded-For | proxy_protocol;
По умолчанию	`real_ip_header X-Real-IP;`
Контекст	http, server, location

Задает поле заголовка запроса, значение которого будет использоваться для замены адреса клиента.

Значение поля заголовка запроса, содержащее необязательный порт, также используется для замены порта клиента. Адрес и порт должны быть указаны согласно RFC 3986.

Параметр `proxy_protocol` меняет адрес клиента на указанный в заголовке PROXY-протокола. Протокол PROXY должен быть предварительно включен при помощи установки параметра *proxy_protocol* в директиве *listen*.

real_ip_recursive

Синтаксис	`real_ip_recursive` on | off;
По умолчанию	`real_ip_recursive off;`
Контекст	http, server, location

При выключенном рекурсивном поиске исходный адрес клиента, совпадающий с одним из доверенных адресов, заменяется на последний адрес, переданный в поле заголовка запроса, заданного директивой *real_ip_header*. При включенном рекурсивном поиске исходный адрес клиента, совпадающий с одним из доверенных адресов, заменяется на последний не доверенный адрес, переданный в заданном поле заголовка запроса.

Встроенные переменные

`$realip_remote_addr`

хранит исходный адрес клиента

`$realip_remote_port`

хранит исходный порт клиента

Referer

Позволяет блокировать доступ к сайту для запросов с неверными значениями поля «Referer» в заголовке. Следует иметь в виду, что подделать запрос с нужным значением поля «Referer» не составляет большого труда, поэтому цель использования данного модуля заключается не в стопроцентном блокировании подобных запросов, а в блокировании массового потока запросов, сделанных обычными браузерами. Нужно также учитывать, что обычные браузеры могут не передавать поле «Referer» даже для верных запросов.

Пример конфигурации

```
valid_referers none blocked server_names
               *.example.com example.* www.example.org/galleries/
               ~\.google\.;

if ($invalid_referer) {
    return 403;
}
```

Директивы

referer_hash_bucket_size

Синтаксис	`referer_hash_bucket_size` *размер*;
По умолчанию	`referer_hash_bucket_size 64;`
Контекст	server, location

Задает размер корзины хэш-таблиц со значениями «Referer». Подробнее настройка хэш-таблиц обсуждается *отдельно*.

referer_hash_max_size

Синтаксис	`referer_hash_max_size` *размер*;
По умолчанию	`referer_hash_max_size 2048;`
Контекст	server, location

Задает максимальный размер хэш-таблиц со значениями «Referer». Подробнее настройка хэш-таблиц обсуждается *отдельно*.

valid_referers

Синтаксис	`valid_referers` none | blocked | server_names | *строка* ...;
По умолчанию	—
Контекст	server, location

Задает значения поля «Referer» заголовка запроса, при которых встроенная переменная *$invalid_referer* будет иметь пустую строку в качестве значения. В противном случае значение переменной равно «1». Поиск совпадения производится без учета регистра символов.

Параметры могут быть следующие:

`none`	поле «Referer» в заголовке запроса отсутствует;
`blocked`	поле «Referer» в заголовке запроса присутствует, но его значение удалено межсетевым экраном (firewall) или прокси-сервером; к таким значениям относятся строки, не начинающиеся на «*http://*» или «*https://*»;
`server_names`	в поле «Referer» заголовка запроса указано одно из имен сервера;
`произвольная строка`	задает имя сервера и необязательное начало URI. В начале или конце имени сервера может быть «*». При проверке порт сервера в поле «Referer» игнорируется;
`регулярное выражение`	в начале должен быть символ «~». Необходимо учитывать, что на совпадение с выражением будет проверяться текст, начинающийся после «*http://*» или «*https://*».

Пример:

```
valid_referers none blocked server_names
               *.example.com example.* www.example.org/galleries/
               ~\.google\.;
```

Встроенные переменные

`$invalid_referer`

Пустая строка, если значение поля «Referer» заголовка запроса считается *правильным*, иначе «1».

Rewrite

Позволяет изменять URI запроса с помощью регулярных выражений PCRE, делать перенаправления и выбирать конфигурацию по условию.

Директивы *break*, *if*, *return*, *rewrite* и *set* обрабатываются в следующем порядке:

- последовательно выполняются директивы этого модуля, описанные на уровне *server*;
- в цикле:
  - ищется *location* по URI запроса;
  - последовательно выполняются директивы этого модуля, описанные в найденном *location*;
  - цикл повторяется, если URI запроса *изменялся*, но *не более* 10 раз.

Директивы

break

Синтаксис	`break`;
По умолчанию	—
Контекст	server, location, if

Завершает обработку текущего набора директив модуля *http_ rewrite*.

Если директива указана внутри *location*, дальнейшая обработка запроса продолжается в этом *location*.

Пример:

```
if ($slow) {
    limit_rate 10k;
    break;
}
```

if

Синтаксис	`if` (*условие*) { ... }
По умолчанию	—
Контекст	server, location

Проверяется указанное условие. Если оно истинно, то выполняются указанные в фигурных скобках директивы этого модуля и запросу назначается конфигурация, указанная внутри директивы *if*. Конфигурации внутри директив *if* наследуются с предыдущего уровня конфигурации.

В качестве условия могут быть заданы:

- имя переменной; ложными значениями переменной являются пустая строка или «0»;
- сравнение переменной со строкой с помощью операторов «=» и «!=»;
- соответствие переменной регулярному выражению с учетом регистра символов — «~» и без него — «~*». В регулярных выражениях можно использовать выделения, которые затем доступны в виде переменных $1..$9. Также можно использовать отрицательные операторы «!~» и «!~*». Если в регулярном выражении встречаются символы «}» или «;», то все выражение следует заключить в одинарные или двойные кавычки.
- проверка существования файла с помощью операторов «-f» и «!-f»;
- проверка существования каталога с помощью операторов «-d» и «!-d»;
- проверка существования файла, каталога или символической ссылки с помощью операторов «-e» и «!-e»;
- проверка исполняемости файла с помощью операторов «-x» и «!-x».

Примеры:

```
if ($http_user_agent ~ MSIE) {
    rewrite ^(.*)$ /msie/$1 break;
}

if ($http_cookie ~* "id=([^;]+)(?:;|$)") {
    set $id $1;
}

if ($request_method = POST) {
    return 405;
}

if ($slow) {
    limit_rate 10k;
}

if ($invalid_referer) {
    return 403;
}
```

Примечание

Значение встроенной переменной *$invalid_referer* задается директивой *valid_referers*.

return

Синтаксис	`return` *код* [*текст*]; `return` *код URL*; `return` *URL*;
По умолчанию	—
Контекст	server, location, if

Завершает обработку и возвращает клиенту указанный `код`. Нестандартный код 444 закрывает соединение без передачи заголовка ответа.

Можно задать либо URL перенаправления (для кодов 301, 302, 303, 307 и 308) либо текст тела ответа (для остальных кодов). В тексте тела ответа и URL перенаправления можно использовать переменные. Как частный случай, URL перенаправления может быть задан как URI, локальный для данного сервера, при этом полный URL перенаправления формируется согласно схеме запроса (*$scheme*) и директивам *server_name_in_redirect* и *port_in_redirect*.

Кроме того, в качестве единственного параметра можно указать URL для временного перенаправления с кодом 302. Такой параметр должен начинаться со строк «*http://*», «*https://*» или «*$scheme*». В URL можно использовать переменные.

См. также директиву *error_page*.

rewrite

Синтаксис	`rewrite` *regex замена* [*флаг*];
По умолчанию	—
Контекст	server, location, if

Если указанное регулярное выражение `regex` соответствует URI запроса, URI изменяется в соответствии со строкой `замены`. Директивы *rewrite* выполняются последовательно, в порядке их следования в конфигурационном файле. С помощью `флага` можно прекратить дальнейшую обработку директив. Если строка `замены` начинается с «*http://*», «*https://*» или «$scheme», то обработка завершается и клиенту возвращается перенаправление.

Необязательный параметр `флаг` может быть одним из:

`last`	завершает обработку текущего набора директив модуля *http_rewrite*, после чего ищется новый *location*, соответствующий измененному URI;
`break`	завершает обработку текущего набора директив модуля *http_rewrite* аналогично директиве *break*;
`redirect`	возвращает временное перенаправление с кодом 302; используется, если строка `замены` не начинается с «*http://*», «*https://*» или «*$scheme*»;
`permanent`	возвращает постоянное перенаправление с кодом 301.

Полный URL перенаправлений формируется согласно схеме запроса (*$scheme*) и директив *server_name_in_redirect* и *port_in_redirect*.

Пример:

```
server {
#    ...
    rewrite ^(/download/.*)/media/(.*)\..*$ $1/mp3/$2.mp3 last;
    rewrite ^(/download/.*)/audio/(.*)\..*$ $1/mp3/$2.ra  last;
    return  403;
#    ...
}
```

Если же эти директивы поместить в location «/download/», то нужно заменить флаг `last` на `break`, иначе Angie PRO сделает 10 циклов и вернет ошибку 500:

```
location /download/ {
    rewrite ^(/download/.*)/media/(.*)\..*$ $1/mp3/$2.mp3 break;
    rewrite ^(/download/.*)/audio/(.*)\..*$ $1/mp3/$2.ra  break;
    return  403;
}
```

Если в строке `замены` указаны новые аргументы запроса, то предыдущие аргументы запроса добавляются после них. Если такое поведение нежелательно, можно отказаться от этого добавления, указав в конце строки замены знак вопроса, например:

```
rewrite ^/users/(.*)$ /show?user=$1? last;
```

Если в регулярном выражении встречаются символы «}» или «;», то все выражение следует заключить в одинарные или двойные кавычки.

rewrite_log

Синтаксис	`rewrite_log` on | off;
По умолчанию	`rewrite_log off;`
Контекст	http, server, location, if

Разрешает или запрещает записывать в *error_log* на уровне *notice* результаты обработки директив модуля *http_rewrite*.

set

Синтаксис	`set` *$переменная значение*;
По умолчанию	—
Контекст	server, location, if

Устанавливает значение указанной переменной. В качестве значения можно использовать текст, переменные и их комбинации.

uninitialized_variable_warn

Синтаксис	`uninitialized_variable_warn` on | off;
По умолчанию	`rewrite_log on;`
Контекст	http, server, location, if

Определяет, нужно ли писать в лог предупреждения о неинициализированных переменных.

Внутреннее устройство

Директивы модуля *http_rewrite* компилируются на стадии конфигурации во внутренние инструкции, интерпретируемые во время обработки запроса. Интерпретатор представляет из себя простую стековую виртуальную машину.

Например, директивы

```
location /download/ {
    if ($forbidden) {
        return 403;
    }

    if ($slow) {
        limit_rate 10k;
    }

    rewrite ^/(download/.*)/media/(.*)\..*$ /$1/mp3/$2.mp3 break;
}
```

будут транслированы в такие инструкции:

```
переменная $forbidden
проверка на ноль
    возврат 403
    завершение всего кода
переменная $slow
проверка на ноль
проверка регулярного выражения
копирование "/"
копирование $1
копирование "/mp3/"
копирование $2
копирование ".mp3"
завершение регулярного выражения
завершение всего кода
```

Обратите внимание, что инструкций для директивы *limit_rate* нет, поскольку она не имеет отношения к модулю *http_rewrite*. Для блока *if* создается отдельная конфигурация. Если условие истинно, запрос получает эту конфигурацию, и в ней *limit_rate* равен 10k.

Директиву

```
rewrite ^/(download/.*)/media/(.*)\..*$ /$1/mp3/$2.mp3 break;
```

можно сделать на одну инструкцию меньше, если в регулярном выражении перенести первую косую черту внутрь скобок:

```
rewrite ^(/download/.*)/media/(.*)\..*$ $1/mp3/$2.mp3 break;
```

Тогда соответствующие инструкции будут выглядеть так:

```
проверка регулярного выражения
копирование $1
копирование "/mp3/"
копирование $2
копирование ".mp3"
завершение регулярного выражения
завершение всего кода
```

SCGI

Позволяет передавать запросы SCGI-серверу.

Пример конфигурации

```
location / {
    include   scgi_params;
    scgi_pass localhost:9000;
}
```

Директивы

scgi_bind

Синтаксис	`scgi_bind` *адрес* [transparent] | off;
По умолчанию	—
Контекст	http, server, location

Задает локальный IP-адрес с необязательным портом, который будет использоваться в исходящих соединениях с SCGI-сервером. В значении параметра допустимо использование переменных. Специальное значение `off` отменяет действие унаследованной с предыдущего уровня конфигурации директивы *scgi_bind*, позволяя системе самостоятельно выбирать локальный IP-адрес и порт.

Параметр `transparent` позволяет задать нелокальный IP-адрес, который будет использоваться в исходящих соединениях с SCGI-сервером, например, реальный IP-адрес клиента:

```
scgi_bind $remote_addr transparent;
```

Для работы параметра обычно требуется запустить рабочие процессы Angie PRO с привилегиями *суперпользователя*. В Linux это не требуется, так как если указан параметр *transparent*, то рабочие процессы наследуют *capability CAP_NET_RAW* из главного процесса.

Важно

Необходимо настроить таблицу маршрутизации ядра для перехвата сетевого трафика с SCGI-сервера.

scgi_buffer_size

Синтаксис	`scgi_buffer_size` *размер*;
По умолчанию	`scgi_buffer_size 4k|8k;`
Контекст	http, server, location

Задает размер буфера, в который будет читаться первая часть ответа, получаемого от SCGI-сервера. В этой части ответа обычно находится небольшой заголовок ответа. По умолчанию размер одного буфера равен размеру страницы памяти. В зависимости от платформы это или 4K, или 8K, однако его можно сделать меньше.

scgi_buffering

Синтаксис	`scgi_buffering` *размер*;
По умолчанию	`scgi_buffering on;`
Контекст	http, server, location

`on`	Angie PRO принимает ответ SCGI-сервера как можно быстрее, сохраняя его в буферы, заданные директивами *scgi_buffer_size* и *scgi_buffers*. Если ответ не вмещается целиком в память, то его часть может быть записана на диск во *временный файл*. Запись во временные файлы контролируется директивами *scgi_max_temp_file_size* и *scgi_temp_file_write_size*.
`off`	Ответ синхронно передается клиенту сразу же по мере его поступления. Angie PRO не пытается считать весь ответ SCGI-сервера. Максимальный размер данных, который Angie PRO может принять от сервера за один раз, задается директивой *scgi_buffer_size*.

Буферизация может быть также включена или выключена путем передачи значения «yes» или «no» в поле «X-Accel-Buffering» заголовка ответа. Эту возможность можно запретить с помощью директивы *scgi_ignore_headers*.

scgi_buffers

Синтаксис	`scgi_buffers` *число размер*;
По умолчанию	`scgi_buffers 8 4k|8k;`
Контекст	http, server, location

Задает число и размер буферов для одного соединения, в которые будет читаться ответ, получаемый от SCGI-сервера. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

scgi_busy_buffers_size

Синтаксис	`scgi_busy_buffers_size` *размер*;
По умолчанию	`scgi_buffers 8k|16k;`
Контекст	http, server, location

При включенной *буферизации* ответов SCGI-сервера, ограничивает суммарный размер буферов, которые могут быть заняты для отправки ответа клиенту, пока ответ еще не прочитан целиком. Оставшиеся буферы тем временем могут использоваться для чтения ответа и, при необходимости, буферизации части ответа во временный файл. По умолчанию размер ограничен величиной двух буферов, заданных директивами *scgi_buffer_size* и *scgi_buffers*.

scgi_cache

Синтаксис	`scgi_cache` *зона* | off;
По умолчанию	`scgi_cache off;`
Контекст	http, server, location

Задает зону разделяемой памяти, используемой для кэширования. Одна и та же зона может использоваться в нескольких местах. В значении параметра можно использовать переменные.

`off`	запрещает кэширование, унаследованное с предыдущего уровня конфигурации.

scgi_cache_background_update

Синтаксис	`scgi_cache_background_update` on | off;
По умолчанию	`scgi_cache_background_update off;`
Контекст	http, server, location

Позволяет запустить фоновый подзапрос для обновления просроченного элемента кэша, в то время как клиенту возвращается устаревший кэшированный ответ.

Внимание

Использование устаревшего кэшированного ответа в момент его обновления должно быть *разрешено*.

scgi_cache_bypass

Синтаксис	`scgi_cache_bypass ...;`
По умолчанию	—
Контекст	http, server, location

Задает условия, при которых ответ не будет браться из кэша. Если значение хотя бы одного из строковых параметров непустое и не равно «0», то ответ не берется из кэша:

```
scgi_cache_bypass $cookie_nocache $arg_nocache$arg_comment;
scgi_cache_bypass $http_pragma    $http_authorization;
```

Можно использовать совместно с директивой *scgi_no_cache*.

scgi_cache_key

Синтаксис	`scgi_cache_key` *строка*;
По умолчанию	—
Контекст	http, server, location

Задает ключ для кэширования, например,

```
scgi_cache_key localhost:9000$request_uri;
```

scgi_cache_lock

Синтаксис	`scgi_cache_lock` on | off;
По умолчанию	`scgi_cache_lock off;`
Контекст	http, server, location

Если включено, одновременно только одному запросу будет позволено заполнить новый элемент кэша, идентифицируемый согласно директиве *scgi_cache_key*, передав запрос на SCGI-сервер. Остальные запросы этого же элемента будут либо ожидать появления ответа в кэше, либо освобождения блокировки этого элемента, в течение времени, заданного директивой *scgi_cache_lock_timeout*.

scgi_cache_lock_age

Синтаксис	`scgi_cache_lock_age` *время*;
По умолчанию	`scgi_cache_lock_age 5s;`
Контекст	http, server, location

Если последний запрос, переданный на SCGI-сервер для заполнения нового элемента кэша, не завершился за указанное время, на SCGI-сервер может быть передан еще один запрос.

scgi_cache_lock_timeout

Синтаксис	`scgi_cache_lock_timeout` *время*;
По умолчанию	`scgi_cache_lock_timeout 5s;`
Контекст	http, server, location

Задает таймаут для *scgi_cache_lock*. По истечении указанного времени запрос будет передан на SCGI-сервер, однако ответ не будет кэширован.

scgi_cache_max_range_offset

Синтаксис	`scgi_cache_max_range_offset` *число*;
По умолчанию	—
Контекст	http, server, location

Задает смещение в байтах для запросов с указанием диапазона запрашиваемых байт (byte-range requests). Если диапазон находится за указанным смещением, range-запрос будет передан на SCGI-сервер и ответ не будет кэширован.

scgi_cache_methods

Синтаксис	`scgi_cache_methods` GET | HEAD | POST ...;
По умолчанию	`scgi_cache_methods GET HEAD;`
Контекст	http, server, location

Если метод запроса клиента указан в этой директиве, то ответ будет кэширован. Методы «GET» и «HEAD» всегда добавляются в список, но тем не менее рекомендуется перечислять их явно. См. также директиву *scgi_no_cache*.

scgi_cache_min_uses

Синтаксис	`scgi_cache_min_uses` *число*;
По умолчанию	`scgi_cache_min_uses 1;`
Контекст	http, server, location

Задает число запросов, после которого ответ будет кэширован.

scgi_cache_path

Синтаксис	`scgi_cache_path` *путь* [levels=*уровни*] [use_temp_path=on|off] keys_zone=*имя:размер* [inactive=*время*] [max_size=*размер*] [min_free=*размер*] [manager_files=*число*] [manager_sleep=*время*] [manager_threshold=*время*] [loader_files=*число*] [loader_sleep=*время*] [loader_threshold=*время*];
По умолчанию	—
Контекст	http

Задает путь и другие параметры кэша. Данные кэша хранятся в файлах. Именем файла в кэше является результат функции MD5 от *ключа кэширования*.

Параметр `levels` задает уровни иерархии кэша: можно задать от 1 до 3 уровней, на каждом уровне допускаются значения 1 или 2.

Например, при использовании

```
scgi_cache_path /data/angie/cache levels=1:2 keys_zone=one:10m;
```

имена файлов в кэше будут такого вида:

```
/data/angie/cache/c/29/b7f54b2df7773722d382f4809d65029c
```

Кэшируемый ответ сначала записывается во временный файл, а потом этот файл переименовывается. Временные файлы и кэш могут располагаться на разных файловых системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если кэш будет находиться на той же файловой системе, что и каталог с временными файлами.

Какой из каталогов будет использоваться для временных файлов, определяется параметром `use_temp_path`.

`on`	Если параметр не задан или установлен в значение «on», будет использоваться каталог, задаваемый директивой *scgi_temp_path* для данного *location*
`off`	временные файлы будут располагаться непосредственно в каталоге кэша

Кроме того, все активные ключи и информация о данных хранятся в зоне разделяемой памяти, имя и размер которой задаются параметром `keys_zone`. Зоны размером в 1 мегабайт достаточно для хранения около 8 тысяч ключей.

Если к данным кэша не обращаются в течение времени, заданного параметром `inactive`, то данные удаляются, независимо от их свежести. По умолчанию *inactive* равен 10 минутам.

Специальный процесс **cache manager** следит за максимальным размером кэша, а также за минимальным объемом свободного места на файловой системе с кэшем, и удаляет наименее востребованные данные при превышении максимального размера кэша или недостаточном объеме свободного места. Удаление данных происходит итерациями.

`max_size`	максимальное пороговое значение размера кэша
`min_free`	минимальное пороговое значение объема свободного места на файловой системе с кэшем
`manager_files`	максимальное количество удаляемых элементов кэша за одну итерацию По умолчанию *100*
`manager_threshol`	ограничивает время работы одной итерации По умолчанию *200* миллисекунд
`manager_sleep`	время, в течение которого выдерживается пауза между итерациями По умолчанию *50* миллисекунд

Через минуту после старта Angie PRO активируется специальный процесс **cache loader**, который загружает в зону кэша информацию о ранее кэшированных данных, хранящихся на файловой системе. Загрузка также происходит итерациями.

`loader_files`	максимальное количество элементов кэша к загрузке в одну итерацию По умолчанию *100*
`loader_threshold`	ограничивает время работы одной итерации По умолчанию *200* миллисекунд
`loader_sleep`	время, в течение которого выдерживается пауза между итерациями По умолчанию *50* миллисекунд

scgi_cache_revalidate

Синтаксис	`scgi_cache_revalidate` on | off;
По умолчанию	`scgi_cache_revalidate off;`
Контекст	http, server, location

Разрешает ревалидацию просроченных элементов кэша при помощи условных запросов с полями заголовка «If-Modified-Since» и «If-None-Match».

scgi_cache_use_stale

Синтаксис	`scgi_cache_use_stale` error | timeout | invalid_header | updating | http_500 | http_503 | http_403 | http_404 | http_429 | off ...;
По умолчанию	`scgi_cache_use_stale off;`
Контекст	http, server, location

Определяет, в каких случаях можно использовать устаревший кэшированный ответ. Параметры директивы совпадают с параметрами директивы *scgi_next_upstream*.

`error`	Позволяет использовать устаревший кэшированный ответ при невозможности выбора SCGI-сервера для обработки запроса.
`updating`	Дополнительный параметр, разрешает использовать устаревший кэшированный ответ, если на данный момент он уже обновляется. Это позволяет минимизировать число обращений к SCGI-серверам при обновлении кэшированных данных.

Использование устаревшего кэшированного ответа может также быть разрешено непосредственно в заголовке ответа на определенное количество секунд после того, как ответ устарел:

- Расширение stale-while-revalidate поля заголовка «Cache-Control» разрешает использовать устаревший кэшированный ответ, если на данный момент он уже обновляется.
- Расширение stale-if-error поля заголовка «Cache-Control» разрешает использовать устаревший кэшированный ответ в случае ошибки.

Примечание

Такой способ менее приоритетен, чем задание параметров директивы.

Чтобы минимизировать число обращений к SCGI-серверам при заполнении нового элемента кэша, можно воспользоваться директивой *scgi_cache_lock*.

scgi_cache_valid

Синтаксис	`scgi_cache_valid` [*код* ...] *время*;
По умолчанию	—
Контекст	http, server, location

Задает время кэширования для разных кодов ответа. Например, директивы

```
scgi_cache_valid 200 302 10m;
scgi_cache_valid 404      1m;
```

задают время кэширования 10 минут для ответов с кодами 200 и 302 и 1 минуту для ответов с кодом 404.

Если указано только время кэширования,

```
scgi_cache_valid 5m;
```

то кэшируются только ответы 200, 301 и 302.

Кроме того, можно кэшировать любые ответы с помощью параметра `any`:

```
scgi_cache_valid 200 302 10m;
scgi_cache_valid 301      1h;
scgi_cache_valid any      1m;
```

Примечание

Параметры кэширования могут также быть заданы непосредственно в заголовке ответа. Такой способ приоритетнее, чем задание времени кэширования с помощью директивы.

- Поле заголовка «X-Accel-Expires» задает время кэширования ответа в секундах. Значение *0* запрещает кэшировать ответ. Если значение начинается с префикса *@*, оно задает абсолютное время в секундах с начала эпохи, до которого ответ может быть кэширован.
- Если в заголовке нет поля «X-Accel-Expires», параметры кэширования определяются по полям заголовка «Expires» или «Cache-Control».
- Ответ, в заголовке которого есть поле «Set-Cookie», не будет кэшироваться.
- Ответ, в заголовке которого есть поле «Vary» со специальным значением «*», не будет кэшироваться. Ответ, в заголовке которого есть поле «Vary» с другим значением, будет кэширован с учетом соответствующих полей заголовка запроса.

Обработка одного или более из этих полей заголовка может быть отключена при помощи директивы *scgi_ignore_headers*.

scgi_connect_timeout

Синтаксис	`scgi_connect_timeout` *время*;
По умолчанию	`scgi_connect_timeout 60s;`
Контекст	http, server, location

Задает таймаут для установления соединения с SCGI-сервером. Необходимо иметь в виду, что этот таймаут обычно не может превышать 75 секунд.

scgi_connection_drop

Синтаксис	`scgi_connection_drop` *время* | on | off;
По умолчанию	`scgi_connection_drop off;`
Контекст	http, server, location

Настраивает завершение всех соединений с проксируемым сервером, если он был удален из группы или помечен как постоянно недоступный в результате процесса *reresolve* или *команды API* `DELETE`.

Соединение завершается, когда обрабатывается следующее событие чтения или записи для клиента или проксируемого сервера.

Установка *времени* включает *таймаут* до завершения соединения; при выборе значения `on` соединения завершаются немедленно.

scgi_force_ranges

Синтаксис	`scgi_force_ranges` off;
По умолчанию	`scgi_force_ranges off;`
Контекст	http, server, location

Включает поддержку диапазонов запрашиваемых байт (byte-range) для кэшированных и некэшированных ответов SCGI-сервера вне зависимости от наличия поля «Accept-Ranges» в заголовках этих ответов.

scgi_hide_header

Синтаксис	`scgi_hide_header` *поле*;
По умолчанию	—
Контекст	http, server, location

По умолчанию Angie PRO не передает клиенту поля заголовка «Status» и «X-Accel-...» из ответа SCGI-сервера. Директива *scgi_hide_header* задает дополнительные поля, которые не будут передаваться. Если же передачу полей нужно разрешить, можно воспользоваться директивой *scgi_pass_header*.

scgi_ignore_client_abort

Синтаксис	`scgi_ignore_client_abort` on | off;
По умолчанию	`scgi_ignore_client_abort off;`
Контекст	http, server, location

Определяет, закрывать ли соединение с SCGI-сервером в случае, если клиент закрыл соединение, не дождавшись ответа.

scgi_ignore_headers

Синтаксис	`scgi_ignore_headers` *поле* ...;
По умолчанию	—
Контекст	http, server, location

Запрещает обработку некоторых полей заголовка из ответа SCGI-сервера. В директиве можно указать поля «X-Accel-Redirect», «X-Accel-Expires», «X-Accel-Limit-Rate», «X-Accel-Buffering», «X-Accel-Charset», «Expires», «Cache-Control», «Set-Cookie» и «Vary».

Если не запрещено, обработка этих полей заголовка заключается в следующем:

- «X-Accel-Expires», «Expires», «Cache-Control», «Set-Cookie» и «Vary» задают *параметры кэширования* ответа;
- «X-Accel-Redirect» производит *внутреннее перенаправление* на указанный URI;
- «X-Accel-Limit-Rate» задает *ограничение скорости* передачи ответа клиенту;
- «X-Accel-Buffering» включает или выключает *буферизацию* ответа;
- «X-Accel-Charset» задает желаемую *кодировку* ответа.

scgi_intercept_errors

Синтаксис	`scgi_intercept_errors` on | off;
По умолчанию	`scgi_intercept_errors off;`
Контекст	http, server, location

Определяет, передавать ли клиенту ответы SCGI-сервера с кодом больше либо равным 300, или же перехватывать их и перенаправлять на обработку Angie PRO с помощью директивы *error_page*.

scgi_limit_rate

Синтаксис	`scgi_limit_rate` *скорость*;
По умолчанию	`scgi_limit_rate 0;`
Контекст	http, server, location

Ограничивает скорость чтения ответа от SCGI-сервера. *Скорость* задается в байтах в секунду; можно использовать переменные.

0	отключает ограничение скорости

Примечание

Ограничение устанавливается на запрос, поэтому, если Angie PRO одновременно откроет два соединения к SCGI-серверу, суммарная скорость будет вдвое выше заданного ограничения. Ограничение работает только в случае, если включена *буферизация* ответов SCGI-сервера.

scgi_max_temp_file_size

Синтаксис	`scgi_max_temp_file_size` *размер*;
По умолчанию	`scgi_max_temp_file_size 1024m;`
Контекст	http, server, location

Если включена *буферизация* ответов SCGI-сервера, и ответ не вмещается целиком в буферы, заданные директивами *scgi_buffer_size* и *scgi_buffers*, часть ответа может быть записана во временный файл. Эта директива задает максимальный размер временного файла. Размер данных, сбрасываемых во временный файл за один раз, задается директивой *scgi_temp_file_write_size*.

0	отключает возможность буферизации ответов во временные файлы

Примечание

Данное ограничение не распространяется на ответы, которые будут *кэшированы* или сохранены *на диске*.

scgi_next_upstream

Синтаксис	`scgi_next_upstream` error | timeout | invalid_header | http_500 | http_503 | http_403 | http_404 | http_429 | non_idempotent | off ...;
По умолчанию	`scgi_next_upstream error timeout;`
Контекст	http, server, location

Определяет, в каких случаях запрос будет передан следующему серверу:

`error`	произошла ошибка соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`timeout`	произошел таймаут во время соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`invalid_header`	сервер вернул пустой или неверный ответ;
`http_500`	сервер вернул ответ с кодом 500;
`http_503`	сервер вернул ответ с кодом 503;
`http_403`	сервер вернул ответ с кодом 403;
`http_404`	сервер вернул ответ с кодом 404;
`http_429`	сервер вернул ответ с кодом 429;
`non_idempotent`	обычно запросы с неидемпотентным методом (*POST*, *LOCK*, *PATCH*) не передаются на другой сервер, если запрос серверу группы уже был отправлен; включение параметра явно разрешает повторять подобные запросы;
`off`	запрещает передачу запроса следующему серверу.

Примечание

Необходимо понимать, что передача запроса следующему серверу возможна только при условии, что клиенту еще ничего не передавалось. То есть, если ошибка или таймаут возникли в середине передачи ответа клиенту, то действие директивы на такой запрос не распространяется.

Директива также определяет, что считается *неудачной попыткой* работы с сервером.

`error timeout invalid_header`	всегда считаются неудачными попытками, даже если они не указаны в директиве
`http_500 http_503 http_429`	считаются неудачными попытками, только если они указаны в директиве
`http_403 http_404`	никогда не считаются неудачными попытками

Передача запроса следующему серверу может быть ограничена по *количеству попыток* и по *времени*.

scgi_next_upstream_timeout

Синтаксис	`scgi_next_upstream_timeout` *время*;
По умолчанию	`scgi_next_upstream_timeout 0;`
Контекст	http, server, location

Ограничивает время, в течение которого возможна передача запроса *следующему* серверу.

`0`	отключает это ограничение

scgi_next_upstream_tries

Синтаксис	`scgi_next_upstream_tries` *число*;
По умолчанию	`scgi_next_upstream_tries 0;`
Контекст	http, server, location

Ограничивает число допустимых попыток для передачи запроса *следующему* серверу.

`0`	отключает это ограничение

scgi_no_cache

Синтаксис	`scgi_no_cache` *строка* ...;
По умолчанию	—
Контекст	http, server, location

Задает условия, при которых ответ не будет сохраняться в кэш. Если значение хотя бы одного из строковых параметров непустое и не равно «0», то ответ не будет сохранен:

```
scgi_no_cache $cookie_nocache $arg_nocache$arg_comment;
scgi_no_cache $http_pragma    $http_authorization;
```

Можно использовать совместно с директивой *scgi_cache_bypass*.

scgi_param

Синтаксис	`scgi_param` *параметр значение* [if_not_empty];
По умолчанию	—
Контекст	http, server, location

Задает параметр, который будет передаваться SCGI-серверу. В качестве значения можно использовать текст, переменные и их комбинации. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *SCGI-param*.

Стандартные переменные окружения CGI должны передаваться как заголовки SCGI, см. файл *scgi_params* из дистрибутива:

```
location / {
    include scgi_params;
#    ...
}
```

Если директива указана с `if_not_empty`, то такой параметр с пустым значением передаваться на сервер не будет:

```
scgi_param HTTPS $https if_not_empty;
```

scgi_pass

Синтаксис	`scgi_pass` URL;
По умолчанию	—
Контекст	location, if в location

Задает адрес SCGI-сервера. Адрес может быть указан в виде доменного имени или IP-адреса, и порта:

```
scgi_pass localhost:9000;
```

или в виде пути UNIX-сокета:

```
scgi_pass unix:/tmp/scgi.socket;
```

Если доменному имени соответствует несколько адресов, то все они будут использоваться по очереди (round-robin). Кроме того, в качестве адреса можно указать *группу серверов*. Если используется группа, указать порт невозможно; вместо этого укажите порт для каждого сервера внутри группы отдельно.

В значении параметра можно использовать переменные. В этом случае, если адрес указан в виде доменного имени, имя ищется среди описанных групп серверов и если не найдено, то определяется с помощью *resolver*'а.

scgi_pass_header

Синтаксис	`scgi_pass_header` *поле* ...;
По умолчанию	—
Контекст	http, server, location

Разрешает передавать от SCGI-сервера клиенту *запрещенные для передачи* поля заголовка.

scgi_pass_request_body

Синтаксис	`scgi_pass_request_body` on | off;
По умолчанию	`scgi_pass_request_body on;`
Контекст	http, server, location

Позволяет запретить передачу исходного тела запроса на SCGI-сервер. См. также директиву *scgi_pass_request_headers*.

scgi_pass_request_headers

Синтаксис	`scgi_pass_request_headers` on | off;
По умолчанию	`scgi_pass_request_headers on;`
Контекст	http, server, location

Позволяет запретить передачу полей заголовка исходного запроса на SCGI-сервер. См. также директиву *scgi_pass_request_body*.

scgi_read_timeout

Синтаксис	`scgi_read_timeout` *время*;
По умолчанию	`scgi_read_timeout 60s;`
Контекст	http, server, location

Задает таймаут при чтении ответа SCGI-сервера. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями чтения. Если по истечении этого времени SCGI-сервер ничего не передаст, соединение закрывается.

scgi_request_buffering

Синтаксис	`scgi_request_buffering` on | off;
По умолчанию	`scgi_request_buffering on;`
Контекст	http, server, location

Разрешает или запрещает использовать буферизацию тела запроса клиента.

`on`	тело запроса полностью *читается* от клиента перед отправкой запроса на SCGI-сервер.
`off`	тело запроса отправляется на SCGI-сервер сразу же по мере его поступления. В этом случае запрос не может быть передан *следующему серверу*, если Angie PRO уже начал отправку тела запроса.

Если для отправки тела исходного запроса используется HTTP/1.1 и передача данных частями (chunked transfer encoding), то тело запроса буферизуется независимо от значения директивы.

scgi_send_timeout

Синтаксис	`scgi_send_timeout` *время*;
По умолчанию	`scgi_send_timeout 60s;`
Контекст	http, server, location

Задает таймаут при передаче запроса SCGI-серверу. Таймаут устанавливается не на всю передачу запроса, а только между двумя операциями записи. Если по истечении этого времени SCGI-сервер не примет новых данных, соединение закрывается.

scgi_socket_keepalive

Синтаксис	`scgi_socket_keepalive` on | off;
По умолчанию	`scgi_socket_keepalive off;`
Контекст	http, server, location

Конфигурирует поведение «TCP keepalive» для исходящих соединений к SCGI-серверу.

`""`	По умолчанию для сокета действуют настройки операционной системы.
`on`	для сокета включается параметр *SO_KEEPALIVE*

scgi_store

Синтаксис	`scgi_store` on | off | *строка*;
По умолчанию	`scgi_store off;`
Контекст	http, server, location

Разрешает сохранение на диск файлов.

`on`	сохраняет файлы в соответствии с путями, указанными в директивах *alias* или *root*
`off`	запрещает сохранение файлов

Имя файла можно задать явно с помощью `строки` с переменными:

```
scgi_store /data/www$original_uri;
```

Время изменения файлов выставляется согласно полученному полю «Last-Modified» в заголовке ответа. Ответ сначала записывается во временный файл, а потом этот файл переименовывается. Временный файл и постоянное место хранения ответа могут располагаться на разных файловых системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если сохраняемые файлы будут находиться на той же файловой системе, что и каталог с временными файлами, задаваемый директивой *scgi_temp_path* для данного *location*.

Директиву можно использовать для создания локальных копий статических неизменяемых файлов:

```
location /images/ {
    root               /data/www;
    error_page         404 = /fetch$uri;
}

location /fetch/ {
    internal;

    scgi_pass          backend:9000;
#   ...

    scgi_store         on;
    scgi_store_access user:rw group:rw all:r;
```

```
    scgi_temp_path    /data/temp;

    alias             /data/www/;
}
```

scgi_store_access

Синтаксис	`scgi_store_access` *пользователи:права* ...;
По умолчанию	`scgi_store_access user:rw;`
Контекст	http, server, location

Задает права доступа для создаваемых файлов и каталогов, например,

```
scgi_store_access user:rw group:rw all:r;
```

Если заданы какие-либо права для *group* или *all*, то права для user указывать необязательно:

```
scgi_store_access group:rw all:r;
```

scgi_temp_file_write_size

Синтаксис	`scgi_temp_file_write_size` *размер*;
По умолчанию	`scgi_temp_file_write_size 8k|16k;`
Контекст	http, server, location

Ограничивает размер данных, сбрасываемых во временный файл за один раз, при включенной буферизации ответов SCGI-сервера во временные файлы. По умолчанию размер ограничен двумя буферами, заданными директивами *scgi_buffer_size* и *scgi_buffers*. Максимальный размер временного файла задается директивой *scgi_max_temp_file_size*.

scgi_temp_path

Синтаксис	`scgi_temp_path` *путь* [*уровень1* [*уровень2* [*уровень3*]]]`;
По умолчанию	`scgi_temp_path scgi_temp;`
Контекст	http, server, location

Задает имя каталога для хранения временных файлов с данными, полученными от SCGI-серверов. В каталоге может использоваться иерархия подкаталогов до трех уровней. Например, при такой конфигурации

```
scgi_temp_path /spool/angie/scgi_temp 1 2;
```

временный файл будет следующего вида:

```
/spool/angie/scgi_temp/7/45/00000123457
```

См. также параметр *use_temp_path* директивы *scgi_cache_path*.

Secure Link

Позволяет проверять аутентичность запрашиваемых ссылок, защищать ресурсы от несанкционированного доступа, а также ограничивать срок действия ссылок.

Правильность запрашиваемой ссылки проверяется сравнением переданного в запросе значения контрольной суммы со значением, вычисляемым для запроса. Если ссылка имеет ограниченный срок действия и он истек, ссылка считается устаревшей. Результат этих проверок делается доступным в переменной *$secure_link*.

Модуль реализует два альтернативных режима работы. В первом режиме, который включается директивой *secure_link_secret*, можно проверить аутентичность запрашиваемых ссылок и защитить их от несанкционированного доступа. Второй режим включается директивами *secure_link* и *secure_link_md5*, и позволяет также ограничить срок действия ссылок.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_secure_link_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Директивы

secure_link

Синтаксис	`secure_link` *выражение*;
По умолчанию	—
Контекст	http, server, location

Задает строку с переменными, из которой будет выделено значение контрольной суммы и время действия ссылки.

Используемые в выражении переменные обычно связаны с запросом; см. *пример* ниже.

Выделенное из строки значение контрольной суммы сравнивается со значением MD5-хэша, вычисляемым для выражения, заданного директивой *secure_link_md5*.

Если контрольные суммы не совпадают, значением переменной *$secure_link* становится пустая строка. Если контрольные суммы совпадают, проверяется время действия ссылки.

Если срок действия ссылки задан и истек, переменная *$secure_link* получает значение `0`. В противном случае она получает значение `1`. Значение MD5-хэш передается в запросе закодированным в base64url.

Если ссылка имеет ограниченный срок действия, время ее действия задается в секундах с начала эпохи (1 января 1970 года 00:00:00 GMT). Значение указывается в выражении после MD5-хэша и отделяется от него запятой. Время действия ссылки, переданное в запросе, делается доступным в переменной *$secure_link_expires* для использования в директиве *secure_link_md5*. Если время действия ссылки не задано, ссылка имеет неограниченный срок действия.

secure_link_md5

Синтаксис	`secure_link_md5` *выражение*;
По умолчанию	—
Контекст	http, server, location

Задает выражение, для которого считается значение MD5-хэш, сравниваемое с переданным в запросе.

Выражение должно содержать защищаемую часть ссылки (ресурс) и секретную составляющую. Если ссылка имеет ограниченный срок действия, выражение также должно содержать *$secure_link_expires*.

Для предотвращения несанкционированного доступа выражение может содержать информацию о клиенте, например, его адрес и версию браузера.

Пример:

```
location /s/ {
    secure_link $arg_md5,$arg_expires;
    secure_link_md5 "$secure_link_expires$uri$remote_addr secret";

    if ($secure_link = "") {
        return 403;
    }

    if ($secure_link = "0") {
        return 410;
    }

#    ...
}
```

Ссылка «/s/link?md5=_e4Nc3iduzkWRm01TBBNYw&expires=2147483647» ограничивает доступ к «/s/link» для клиента с IP-адресом 127.0.0.1. Ссылка также имеет ограниченный срок действия до 19 января 2038 года (GMT).

Значение аргумента запроса md5 на UNIX можно получить так:

```
echo -n '2147483647/s/link127.0.0.1 secret' | \
    openssl md5 -binary | openssl base64 | tr +/ -_ | tr -d =
```

secure_link_secret

Синтаксис	`secure_link_secret` *слово*;
По умолчанию	—
Контекст	location

Задает секретное слово для проверки аутентичности запрашиваемых ссылок.

Полный URI запрашиваемой ссылки выглядит так:

```
/префикс/хэш/ссылка
```

где хэш — MD5-хэш в шестнадцатеричном виде, вычисленный для конкатенации ссылки и секретного слова, а префикс — произвольная строка без косых черт.

Если запрашиваемая ссылка проходит проверку на аутентичность, значением переменной *$secure_link* становится ссылка, выделенная из URI запроса. В противном случае значением переменной *$secure_link* становится пустая строка.

Пример:

```
location /p/ {
    secure_link_secret secret;

    if ($secure_link = "") {
        return 403;
    }

    rewrite ^ /secure/$secure_link;
}

location /secure/ {
    internal;
}
```

По запросу «/p/5e814704a28d9bc1914ff19fa0c4a00a/link» будет выполнено внутреннее перенаправление на «/secure/link».

Значение хэша для данного примера на UNIX можно получить так:

```
echo -n 'linksecret' | openssl md5 -hex
```

Встроенные переменные

`$secure_link`

Результат проверки ссылки. Конкретное значение зависит от выбранного режима работы.

`$secure_link_expires`

Время действия ссылки, переданное в запросе. Предназначено исключительно для использования в директиве *secure_link_md5*.

Slice

Фильтр, который разбивает запрос на подзапросы, каждый из которых возвращает определенный диапазон ответа. Фильтр обеспечивает более эффективное кэширование больших ответов.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_slice_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
location / {
    slice             1m;
    proxy_cache       cache;
    proxy_cache_key   $uri$is_args$args$slice_range;
    proxy_set_header  Range $slice_range;
    proxy_cache_valid 200 206 1h;
    proxy_pass        http://localhost:8000;
}
```

В данном примере ответ разбивается на кэшируемые фрагменты размером в 1 мегабайт.

Директивы

slice

Синтаксис	`slice` *размер*;
По умолчанию	`slice 0;`
Контекст	http, server, location

Задает размер фрагмента. Нулевое значение запрещает разбиение ответов на фрагменты.

> **Предупреждение**
>
> Обратите внимание, что слишком низкое значение может привести к излишнему потреблению памяти и открытию большого количества файлов.

Для того, чтобы подзапрос вернул необходимый диапазон, переменная *$slice_range* должна быть передана на проксируемый сервер в качестве поля «Range» заголовка запроса. Если включено *кэширование*, то необходимо добавить *$slice_range* в *ключ кэширования* и *включить* кэширование ответов с кодом 206.

Встроенные переменные

`$slice_range`

текущий диапазон фрагмента в формате HTTP byte range, например *bytes=0-1048575*.

Split Clients

Модуль генерирует переменные для A/B-тестирования, канареечных релизов и других сценариев, которые направляют определенный процент клиентов на один сервер или конфигурацию, а остальных — куда-то еще.

Пример конфигурации

```
http {
    split_clients "${remote_addr}AAA" $variant {
                  0.5%               .one;
                  2.0%               .two;
                  *                  "";
    }

    server {
        location / {
            index index${variant}.html;
```

Директивы

split_clients

Синтаксис	`split_clients` *строка* *$переменная* { ... }
По умолчанию	—
Контекст	http

Создает *$переменную*, хэшируя *строку*; переменные в *строке* подставляются, результат хэшируется, затем по значению хэша выбирается строковое значение *$переменной*.

Функция хэширования использует MurmurHash2 (32 бит), и весь диапазон ее значений (с 0 по 4294967295) сопоставляется с корзинами в порядке появления; процентные величины определяют размер корзин. В конце может стоять метасимвол (`*`); хэши, не попавшие в другие корзины, сопоставляются с приданным ему значением.

Пример:

```
split_clients "${remote_addr}AAA" $variant {
              0.5%               .one;
              2.0%               .two;
              *                  "";
}
```

Здесь после подстановки в строке $*remote_addr*`AAA` значения хэша распределяются следующим образом:

- значения от 0 до 21474835 (0,5%) дают `.one`;
- значения от 21474836 до 107374180 (2%) дают `.two`;
- значения от 107374181 до 4294967295 (все остальные) дают `""` (пустую строку).

SSI

Фильтр, обрабатывающий команды SSI (Server Side Includes) в проходящих через него ответах.

Пример конфигурации

```
location / {
    ssi on;
#    ...
}
```

Директивы

ssi

Синтаксис	`ssi` on | off;
По умолчанию	`ssi off;`
Контекст	http, server, location, if в location

Разрешает или запрещает обработку команд SSI в ответах.

ssi_last_modified

Синтаксис	`ssi_last_modified` on | off;
По умолчанию	`ssi_last_modified off;`
Контекст	http, server, location

Позволяет сохранить поле заголовка «Last-Modified» исходного ответа во время обработки SSI для лучшего кэширования ответов.

По умолчанию поле заголовка удаляется, так как содержимое ответа изменяется во время обработки и может содержать динамически созданные элементы или части, которые изменились независимо от исходного ответа.

ssi_min_file_chunk

Синтаксис	`ssi_min_file_chunk` *размер*;
По умолчанию	`ssi_min_file_chunk 1k;`
Контекст	http, server, location

Задает минимальный размер частей ответа, хранящихся на диске, начиная с которого имеет смысл посылать их с помощью *sendfile*.

ssi_silent_errors

Синтаксис	`ssi_silent_errors` on | off;
По умолчанию	`ssi_silent_errors off;`
Контекст	http, server, location

Разрешает не выводить строку «*[an error occurred while processing the directive]*», если во время обработки SSI произошла ошибка.

ssi_types

Синтаксис	`ssi_types` mime-*тип* ...;
По умолчанию	`ssi_types text/html;`
Контекст	http, server, location

Разрешает обработку команд SSI в ответах с указанными MIME-типами в дополнение к «*text/html*». Специальное значение «*» соответствует любому MIME-типу.

ssi_value_length

Синтаксис	`ssi_value_length` *длина*;
По умолчанию	`ssi_value_length 256;`
Контекст	http, server, location

Задает максимальную длину значений параметров в SSI-командах.

Команды SSI

Общий формат команд SSI такой:

```
<!--# команда параметр1=значение1 параметр2=значение2 ... -->
```

Поддерживаются следующие команды:

`block`

Описывает блок, который можно использовать как заглушку в команде *include*. Внутри блока могут быть другие команды SSI. Параметр команды:

`name`

имя блока.

Пример:

```
<!--# block name="one" -->
заглушка
<!--# endblock -->
```

`config`

Задает некоторые параметры, используемые при обработке SSI, а именно:

`errmsg`

строка, выводящаяся при ошибке во время обработки SSI. По умолчанию выводится такая строка:

[an error occurred while processing the directive]

`timefmt`

строка формата, передаваемая функции strftime() для вывода даты и времени. По умолчанию используется такой формат:

«%A, %d-%b-%Y %H:%M:%S %Z»

Для вывода времени в секундах подходит формат «%s».

`echo`

Выводит значение переменной. Параметры команды:

`var`

имя переменной.

`encoding`

способ кодирования. Возможны три значения — *none*, *url* и *entity*. По умолчанию используется entity.

`default`

нестандартный параметр, задающий строку, которая выводится, если переменная не определена. По умолчанию выводится строка «*(none)*».

Команда

```
<!--# echo var="name" default="нет" -->
```

заменяет такую последовательность команд:

```
<!--# if expr="$name" --><!--# echo var="name" --><!--#
     else -->нет<!--# endif -->
```

`if`

Выполняет условное включение. Поддерживаются следующие команды:

```
<!--# if expr="..." -->
...
<!--# elif expr="..." -->
...
<!--# else -->
...
<!--# endif -->
```

На данный момент поддерживается только один уровень вложенности. Параметр команды:

`expr`

выражение. В выражении может быть:

- проверка существования переменной:

```
<!--# if expr="$name" -->
```

- сравнение переменной с текстом:

```
<!--# if expr="$name = text" -->
<!--# if expr="$name != text" -->
```

- сравнение переменной с регулярным выражением:

```
<!--# if expr="$name = /text/" -->
<!--# if expr="$name != /text/" -->
```

Если в *text* встречаются переменные, то производится подстановка их значений. В регулярном выражении можно задать позиционные и именованные выделения, а затем использовать их через переменные, например:

```
<!--# if expr="$name = /(.+)@(?P<domain>.+)/" -->
  <!--# echo var="1" -->
  <!--# echo var="domain" -->
<!--# endif -->
```

`include`

Включает в ответ результат другого запроса. Параметры команды:

`file`

задает включаемый файл, например:

```
<!--# include file="footer.html" -->
```

`virtual`

задает включаемый запрос, например:

```
<!--# include virtual="/remote/body.php?argument=value" -->
```

Несколько запросов, указанных на одной странице и обрабатываемых проксируемыми или FastCGI/uwsgi/SCGI/gRPC-серверами, работают параллельно. Если нужна последовательная обработка, следует воспользоваться параметром *wait*.

`stub`

нестандартный параметр, задающий имя блока, содержимое которого будет выведено, если тело ответа на включаемый запрос пустое или если при исполнении запроса произошла ошибка, например:

```
<!--# block name="one" --> <!--# endblock -->
<!--# include virtual="/remote/body.php?argument=value" stub="one" -->
```

Содержимое замещающего блока обрабатывается в контексте включаемого запроса.

`wait`

нестандартный параметр, указывающий, нужно ли ждать полного исполнения данного запроса, прежде чем продолжать выполнение SSI, например:

```
<!--# include virtual="/remote/body.php?argument=value" wait="yes" -->
```

`set`

нестандартный параметр, указывающий, что удачный результат выполнения запроса нужно записать в заданную переменную, например:

```
<!--# include virtual="/remote/body.php?argument=value" set="one" -->
```

Максимальный размер ответа задается директивой *subrequest_output_buffer_size*:

```
location /remote/ {
    subrequest_output_buffer_size 64k;
#    ...
}
```

`set`

Присваивает значение переменной. Параметры команды:

`var`

имя переменной.

`value`

значение переменной. Если в присваиваемом значении есть переменные, то производится подстановка их значений.

Встроенные переменные

`$date_local`

текущее время в локальной временной зоне. Формат задается командой *config* с параметром *timefmt*.

`$date_gmt`

текущее время в GMT. Формат задается командой *config* с параметром *timefmt*.

SSL

Обеспечивает работу по протоколу HTTPS.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_ssl_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Важно

Для этого модуля нужна библиотека OpenSSL.

Пример конфигурации

Для уменьшения загрузки процессора рекомендуется

- установить число *рабочих процессов* равным числу процессоров,
- разрешить *keep-alive* соединения,
- включить *разделяемый кэш* сессий,
- выключить *встроенный кэш* сессий
- и, возможно, увеличить *время жизни* сессии (по умолчанию 5 минут):

```
worker_processes auto;

http {
```

```
    # ...

    server {
        listen              443 ssl;
        keepalive_timeout   70;

        ssl_protocols       TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
        ssl_ciphers         AES128-SHA:AES256-SHA:RC4-SHA:DES-CBC3-SHA:RC4-MD5;
        ssl_certificate     /usr/local/angie/conf/cert.pem;
        ssl_certificate_key /usr/local/angie/conf/cert.key;
        ssl_session_cache   shared:SSL:10m;
        ssl_session_timeout 10m;

        # ...
    }
```

Директивы

ssl_buffer_size

Синтаксис	`ssl_buffer_size` *размер*;
По умолчанию	`ssl_buffer_size 16k;`
Контекст	http, server

Задает размер буфера, используемого при отправке данных.

По умолчанию размер буфера равен 16k, что соответствует минимальным накладным расходам при передаче больших ответов. С целью минимизации времени получения начала ответа (Time To First Byte) может быть полезно использовать меньшие значения, например:

```
ssl_buffer_size 4k;
```

ssl_certificate

Синтаксис	`ssl_certificate` *файл*;
По умолчанию	—
Контекст	http, server

Указывает файл с сертификатом в формате PEM для данного виртуального сервера. Если вместе с основным сертификатом нужно указать промежуточные, то они должны находиться в этом же файле в следующем порядке: сначала основной сертификат, а затем промежуточные. В этом же файле может находиться секретный ключ в формате PEM.

Эта директива может быть указана несколько раз для загрузки сертификатов разных типов, например RSA и ECDSA:

```
server {
    listen              443 ssl;
    server_name         example.com;

    ssl_certificate     example.com.rsa.crt;
```

```
    ssl_certificate_key example.com.rsa.key;

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

    # ...
}
```

Возможность задавать отдельные цепочки сертификатов для разных сертификатов есть только в OpenSSL 1.0.2 и выше. Для более старых версий следует указывать только одну цепочку сертификатов.

Важно

В имени файла можно использовать переменные при использовании OpenSSL 1.0.2 и выше:

```
ssl_certificate     $ssl_server_name.crt;
ssl_certificate_key $ssl_server_name.key;
```

При использовании переменных сертификат загружается при каждой операции SSL-рукопожатия, что может отрицательно влиять на производительность.

Вместо `файла` можно указать значение «data:*$переменная*», при котором сертификат загружается из переменной без использования промежуточных файлов.

Ненадлежащее использование подобного синтаксиса может быть небезопасно, например данные секретного ключа могут попасть в *лог ошибок*.

Важно

Нужно иметь в виду, что из-за ограничения протокола HTTPS для максимальной совместимости виртуальные серверы должны слушать на *разных IP-адресах*.

Добавлено в версии 1.2.0: Если задан режим *ssl_ntls*, директива может принимать два аргумента (части ключа для подписи и шифрования) вместо одного:

```
listen ... ssl;

ssl_ntls  on;

# двойной сертификат NTLS
ssl_certificate      sign.crt enc.crt;
ssl_certificate_key  sign.key enc.key;

# можно использовать наряду с обычным сертификатом RSA
ssl_certificate  rsa.crt;
ssl_certificate  rsa.key;
```

ssl_certificate_key

Синтаксис	`ssl_certificate_key` *файл*;
По умолчанию	—
Контекст	http, server

Указывает файл с секретным ключом в формате PEM для данного виртуального сервера.

Важно

В имени файла можно использовать переменные при использовании OpenSSL 1.0.2 и выше.

Вместо `файла` можно указать значение «engine:*имя*:id», которое загружает ключ с указанным *id* из OpenSSL engine с заданным именем.

Вместо `файла` также можно указать значение «data:*$переменная*», при котором секретный ключ загружается из переменной без использования промежуточных файлов. При этом следует учитывать, что ненадлежащее использование подобного синтаксиса может быть небезопасно, например данные секретного ключа могут попасть в *лог ошибок*.

Добавлено в версии 1.2.0: Если задан режим *ssl_ntls*, директива может принимать два аргумента (части ключа для подписи и шифрования) вместо одного:

```
listen ... ssl;

ssl_ntls  on;

# двойной сертификат NTLS
ssl_certificate      sign.crt enc.crt;
ssl_certificate_key  sign.key enc.key;

# можно использовать наряду с обычным сертификатом RSA
ssl_certificate  rsa.crt;
ssl_certificate  rsa.key;
```

ssl_ciphers

Синтаксис	`ssl_ciphers` *шифры*;
По умолчанию	`ssl_ciphers HIGH:!aNULL:!MD5;`
Контекст	http, server

Описывает разрешенные шифры. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL, например:

```
ssl_ciphers ALL:!aNULL:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
```

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

ssl_client_certificate

Синтаксис	`ssl_client_certificate` *файл*;
По умолчанию	—
Контекст	http, server

Указывает файл с доверенными сертификатами CA в формате PEM, которые используются для *проверки* клиентских сертификатов и ответов OCSP, если включен *ssl_stapling*.

Список сертификатов будет отправляться клиентам. Если это нежелательно, можно воспользоваться директивой *ssl_trusted_certificate*.

ssl_conf_command

Синтаксис	`ssl_conf_command` *имя значение*;
По умолчанию	—
Контекст	http, server

Задает произвольные конфигурационные команды OpenSSL.

Важно

Директива поддерживается при использовании OpenSSL 1.0.2 и выше.

На одном уровне может быть указано несколько директив *ssl_conf_command*:

```
ssl_conf_command Options PrioritizeChaCha;
ssl_conf_command Ciphersuites TLS_CHACHA20_POLY1305_SHA256;
```

Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *ssl_conf_command*.

Осторожно

Изменение настроек OpenSSL напрямую может привести к неожиданному поведению.

ssl_crl

Синтаксис	`ssl_crl` *файл*;
По умолчанию	—
Контекст	http, server

Указывает файл с отозванными сертификатами (CRL) в формате PEM, используемыми для *проверки* клиентских сертификатов.

ssl_dhparam

Синтаксис	`ssl_dhparam` *файл*;
По умолчанию	—
Контекст	http, server

Указывает файл с параметрами для DHE-шифров.

Осторожно

По умолчанию параметры не заданы, и соответственно DHE-шифры не будут использоваться.

ssl_early_data

Синтаксис	`ssl_early_data` on | off;
По умолчанию	`ssl_early_data off;`
Контекст	http, server

Разрешает или запрещает TLS 1.3 early data.

Запросы, отправленные внутри early data, могут быть подвержены атакам повторного воспроизведения (replay). Для защиты от подобных атак на уровне приложения необходимо использовать переменную *$ssl_early_data*.

```
proxy_set_header Early-Data $ssl_early_data;
```

Важно

Директива поддерживается при использовании OpenSSL 1.1.1 и выше или BoringSSL.

ssl_ecdh_curve

Синтаксис	`ssl_ecdh_curve` *кривая*;
По умолчанию	`ssl_ecdh_curve auto;`
Контекст	http, server

Задает кривую для ECDHE-шифров.

Важно

При использовании OpenSSL 1.0.2 и выше можно указывать несколько кривых, например:

```
ssl_ecdh_curve prime256v1:secp384r1;
```

Специальное значение `auto` соответствует встроенному в библиотеку OpenSSL списку кривых для OpenSSL 1.0.2 и выше, или *prime256v1* для более старых версий.

Важно

При использовании OpenSSL 1.0.2 и выше директива задает список кривых, поддерживаемых сервером. Поэтому для работы ECDSA-сертификатов важно, чтобы список включал кривые, используемые в сертификатах.

ssl_ntls

Добавлено в версии 1.2.0.

Синтаксис	`ssl_ntls` on | off;
По умолчанию	`ssl_ntls off;`
Контекст	http, server

Включает серверную поддержку NTLS при использовании TLS библиотеки TongSuo

```
listen ... ssl;
ssl_ntls  on;
```

Важно

Angie PRO необходимо собрать с использованием параметра конфигурации *–with-ntls*, с соответствующей SSL библиотекой с поддержкой NTLS

```
./configure --with-openssl=../Tongsuo-8.3.0 \
            --with-openssl-opt=enable-ntls  \
            --with-ntls
```

ssl_ocsp

Синтаксис	`ssl_ocsp` on | off | leaf;
По умолчанию	`ssl_ocsp off;`
Контекст	http, server

Включает проверку OCSP для цепочки клиентских сертификатов. Параметр `leaf` включает проверку только клиентского сертификата.

Для работы проверки OCSP необходимо дополнительно установить значение директивы *ssl_verify_client* в `on` или `optional`.

Для преобразования имени хоста OCSP responder'а в адрес необходимо дополнительно задать директиву *resolver*.

Пример:

```
ssl_verify_client on;
ssl_ocsp          on;
resolver          127.0.0.53;
```

ssl_ocsp_cache

Синтаксис	`ssl_ocsp_cache` off | [shared:*имя*:*размер*];
По умолчанию	`ssl_ocsp_cache off;`
Контекст	http, server

Задает имя и размер кэша, который хранит статус клиентских сертификатов для проверки OCSP-ответов. Кэш разделяется между всеми рабочими процессами. Кэш с одинаковым названием может использоваться в нескольких виртуальных серверах.

Параметр `off` запрещает использование кэша.

ssl_ocsp_responder

Синтаксис	`ssl_ocsp_responder` url;
По умолчанию	—
Контекст	http, server

Переопределяет URL OCSP responder'а, указанный в расширении сертификата «Authority Information Access» для *проверки* клиентских сертификатов.

Поддерживаются только «*http://*» OCSP responder'ы:

```
ssl_ocsp_responder http://ocsp.example.com/;
```

ssl_password_file

Синтаксис	`ssl_password_file` *файл*;
По умолчанию	—
Контекст	http, server

Задает файл с паролями от *секретных ключей*, где каждый пароль указан на отдельной строке. Пароли применяются по очереди в момент загрузки ключа.

Пример:

```
http {
    ssl_password_file /etc/keys/global.pass;
    ...

    server {
        server_name www1.example.com;
        ssl_certificate_key /etc/keys/first.key;
    }
```

```
    server {
        server_name www2.example.com;

        # вместо файла можно указать именованный канал
        ssl_password_file /etc/keys/fifo;
        ssl_certificate_key /etc/keys/second.key;
    }
}
```

ssl_prefer_server_ciphers

Синтаксис	`ssl_prefer_server_ciphers` on | off;
По умолчанию	`ssl_prefer_server_ciphers off;`
Контекст	http, server

При использовании протоколов SSLv3 и TLS устанавливает приоритет серверных шифров над клиентскими.

ssl_protocols

Синтаксис	`ssl_protocols` [SSLv2] [SSLv3] [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;`
Контекст	http, server

Изменено в версии 1.2.0: Параметр `TLSv1.3` добавлен к используемым по умолчанию.

Разрешает указанные протоколы.

Важно

Параметры TLSv1.1 и TLSv1.2 работают только при использовании OpenSSL 1.0.1 и выше.

Параметр TLSv1.3 работает только при использовании OpenSSL 1.1.1 и выше.

ssl_reject_handshake

Синтаксис	`ssl_reject_handshake` on | off;
По умолчанию	`ssl_reject_handshake off;`
Контекст	http, server

Если включено, то операции SSL-рукопожатия в блоке *server* будут отклонены.

Например, в этой конфигурации отклоняются все операции SSL-рукопожатия с именем сервера, отличным от *example.com*:

```
server {
    listen               443 ssl default_server;
    ssl_reject_handshake on;
}

server {
    listen              443 ssl;
    server_name         example.com;
    ssl_certificate     example.com.crt;
    ssl_certificate_key example.com.key;
}
```

ssl_session_cache

Синтаксис	`ssl_session_cache` off | none | [builtin[:*размер*]] [shared:*название*:*размер*];
По умолчанию	`ssl_session_cache none;`
Контекст	http, server

Задает тип и размеры кэшей для хранения параметров сессий. Тип кэша может быть следующим:

`off`	жесткое запрещение использования кэша сессий: Angie PRO явно сообщает клиенту, что сессии не могут использоваться повторно.
`none`	мягкое запрещение использования кэша сессий: Angie PRO сообщает клиенту, что сессии могут использоваться повторно, но на самом деле не хранит параметры сессии в кэше.
`builtin`	встроенный в OpenSSL кэш, используется в рамках только одного рабочего процесса. Размер кэша задается в сессиях. Если размер не задан, то он равен 20480 сессиям. Использование встроенного кэша может вести к фрагментации памяти.
`shared`	кэш, разделяемый между всеми рабочими процессами. Размер кэша задается в байтах, в 1 мегабайт может поместиться около 4000 сессий. У каждого разделяемого кэша должно быть произвольное название. Кэш с одинаковым названием может использоваться в нескольких виртуальных серверах. Также он используется для автоматического создания, хранения и периодического обновления ключей TLS session tickets, если они не указаны явно с помощью директивы *ssl_session_ticket_key*.

Можно использовать одновременно оба типа кэша, например:

```
ssl_session_cache builtin:1000 shared:SSL:10m;
```

однако использование только разделяемого кэша без встроенного должно быть более эффективным.

ssl_session_ticket_key

Синтаксис	`ssl_session_ticket_key` *файл*;
По умолчанию	—
Контекст	http, server

Задает файл с секретным ключом, применяемым при шифровании и расшифровании TLS session tickets. Директива необходима, если один и тот же ключ нужно использовать на нескольких серверах. По умолчанию используется случайно сгенерированный ключ.

Если указано несколько ключей, то только первый ключ используется для шифрования TLS session tickets. Это позволяет настроить ротацию ключей, например:

```
ssl_session_ticket_key current.key;
ssl_session_ticket_key previous.key;
```

Файл должен содержать 80 или 48 байт случайных данных и может быть создан следующей командой:

```
openssl rand 80 > ticket.key
```

В зависимости от размера файла для шифрования будет использоваться либо AES256 (для 80-байтных ключей), либо AES128 (для 48-байтных ключей).

ssl_session_tickets

Синтаксис	`ssl_session_tickets` on | off;
По умолчанию	`ssl_session_tickets on;`
Контекст	http, server

Разрешает или запрещает возобновление сессий при помощи TLS session tickets.

ssl_session_timeout

Синтаксис	`ssl_session_timeout` *время*;
По умолчанию	`ssl_session_timeout 5m;`
Контекст	http, server

Задает время, в течение которого клиент может повторно использовать параметры сессии.

ssl_stapling

Синтаксис	`ssl_stapling` on | off;
По умолчанию	`ssl_stapling off;`
Контекст	http, server

Разрешает или запрещает прикрепление OCSP-ответов сервером. Пример:

```
ssl_stapling on;
resolver 127.0.0.53;
```

Для работы OCSP stapling должен быть известен сертификат издателя сертификата сервера. Если в заданном директивой *ssl_certificate* файле не содержится промежуточных сертификатов, то сертификат издателя сертификата сервера следует поместить в файл, заданный директивой *ssl_trusted_certificate*.

Внимание

Для преобразования имени хоста OCSP responder'а в адрес необходимо дополнительно задать директиву *resolver*.

ssl_stapling_file

Синтаксис	`ssl_stapling_file` *файл*;
По умолчанию	—
Контекст	http, server

Если задано, то вместо опроса OCSP responder'а, указанного в сертификате сервера, ответ берется из указанного файла.

Ответ должен быть в формате DER и может быть сгенерирован командой «*openssl ocsp*».

ssl_stapling_responder

Синтаксис	`ssl_stapling_responder` url;
По умолчанию	—
Контекст	http, server

Переопределяет URL OCSP responder'а, указанный в расширении сертификата «Authority Information Access».

Поддерживаются только «*http://*» OCSP responder'ы:

```
ssl_stapling_responder http://ocsp.example.com/;
```

ssl_stapling_verify

Синтаксис	`ssl_stapling_verify` on | off;
По умолчанию	`ssl_stapling_verify off;`
Контекст	http, server

Разрешает или запрещает проверку сервером ответов OCSP.

Для работоспособности проверки сертификат издателя сертификата сервера, корневой сертификат и все промежуточные сертификаты должны быть указаны как доверенные с помощью директивы *ssl_trusted_certificate*.

ssl_trusted_certificate

Синтаксис	`ssl_trusted_certificate` *файл*;
По умолчанию	—
Контекст	http, server

Задает файл с доверенными сертификатами CA в формате PEM, которые используются для *проверки* клиентских сертификатов и ответов OCSP, если включен *ssl_stapling*.

В отличие от *ssl_client_certificate*, список этих сертификатов не будет отправляться клиентам.

ssl_verify_client

Синтаксис	`ssl_verify_client` on | off | optional | optional_no_ca;
По умолчанию	`ssl_verify_client off;`
Контекст	http, server

Разрешает проверку клиентских сертификатов. Результат проверки доступен через переменную *$ssl_client_verify*.

`optional`	запрашивает клиентский сертификат, и если сертификат был предоставлен, проверяет его
`optional_no_ca`	запрашивает сертификат клиента, но не требует, чтобы он был подписан доверенным сертификатом CA. Это предназначено для случаев, когда фактическая проверка сертификата осуществляется внешним по отношению к Angie PRO сервисом.

ssl_verify_depth

Синтаксис	`ssl_verify_depth` *число*;
По умолчанию	`ssl_verify_depth 1;`
Контекст	http, server

Устанавливает глубину проверки в цепочке клиентских сертификатов.

Обработка ошибок

Модуль `http_ssl` поддерживает несколько нестандартных кодов ошибок, которые можно использовать для перенаправления с помощью директивы *error_page*:

495	при проверке клиентского сертификата произошла ошибка;
496	клиент не предоставил требуемый сертификат;
497	обычный запрос был послан на порт HTTPS.

Перенаправление делается после того, как запрос полностью разобран и доступны такие переменные, как *$request_uri*, *$uri*, *$args* и другие переменные.

Встроенные переменные

Модуль *http_ssl* поддерживает встроенные переменные:

`$ssl_alpn_protocol`

возвращает протокол, выбранный при помощи ALPN во время SSL-рукопожатия, либо пустую строку.

`$ssl_cipher`

возвращает название используемого шифра для установленного SSL-соединения.

`$ssl_ciphers`

возвращает список шифров, поддерживаемых клиентом. Известные шифры указаны по имени, неизвестные указаны в шестнадцатеричном виде, например:

AES128-SHA:AES256-SHA:0x00ff

Важно

Переменная полностью поддерживается при использовании OpenSSL версии 1.0.2 и выше. При использовании более старых версий переменная доступна только для новых сессий и может содержать только известные шифры.

`$ssl_client_escaped_cert`

возвращает клиентский сертификат в формате PEM (закодирован в формате urlencode) для установленного SSL-соединения.

`$ssl_client_fingerprint`

возвращает SHA1-отпечаток клиентского сертификата для установленного SSL-соединения.

`$ssl_client_i_dn`

возвращает строку «issuer DN» клиентского сертификата для установленного SSL-соединения согласно RFC 2253.

`$ssl_client_i_dn_legacy`

возвращает строку «issuer DN» клиентского сертификата для установленного SSL-соединения.

`$ssl_client_raw_cert`

возвращает клиентский сертификат для установленного SSL-соединения в формате PEM.

`$ssl_client_s_dn`

возвращает строку «subject DN» клиентского сертификата для установленного SSL-соединения согласно RFC 2253.

`$ssl_client_s_dn_legacy`

возвращает строку «subject DN» клиентского сертификата для установленного SSL-соединения.

`$ssl_client_serial`

возвращает серийный номер клиентского сертификата для установленного SSL-соединения.

`$ssl_client_v_end`

возвращает дату окончания срока действия клиентского сертификата.

`$ssl_client_v_remain`

возвращает число дней, оставшихся до истечения срока действия клиентского сертификата.

`$ssl_client_v_start`

возвращает дату начала срока действия клиентского сертификата.

`$ssl_client_verify`

возвращает результат проверки клиентского сертификата: `SUCCESS`, «*FAILED:reason*» и, если сертификат не был предоставлен, `NONE`.

`$ssl_curve`

возвращает согласованную кривую, использованную для обмена ключами во время SSL-рукопожатия. Известные кривые указаны по имени, неизвестные указаны в шестнадцатеричном виде, например:

prime256v1

Важно

Переменная поддерживается при использовании OpenSSL версии 3.0 и выше. При использовании более старых версий значением переменной будет пустая строка.

`$ssl_curves`

возвращает список кривых, поддерживаемых клиентом. Известные кривые указаны по имени, неизвестные указаны в шестнадцатеричном виде, например:

0x001d:prime256v1:secp521r1:secp384r1

Важно

Переменная поддерживается при использовании OpenSSL версии 1.0.2 и выше. При использовании более старых версий значением переменной будет пустая строка.

Переменная доступна только для новых сессий.

`$ssl_early_data`

возвращает `1`, если используется TLS 1.3 *early data* и операция SSL-рукопожатия не завершена, иначе «».

`$ssl_protocol`

возвращает протокол установленного SSL-соединения.

`$ssl_server_cert_type`

принимает значения `RSA`, `DSA`, `ECDSA`, `ED448`, `ED25519`, `SM2`, `RSA-PSS` или `unknown` в зависимости от типа сертификата и ключа сервера.

`$ssl_server_name`

возвращает имя сервера, запрошенное через SNI.

`$ssl_session_id`

возвращает идентификатор сессии установленного SSL-соединения.

`$ssl_session_reused`

возвращает `r`, если сессия была использована повторно, иначе «.».

Stub Status

Предоставляет доступ к базовой информации о состоянии сервера.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_stub_status_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
location = /basic_status {
    stub_status;
}
```

В данной конфигурации создается простая веб-страница с основной информацией о состоянии, которая может выглядеть следующим образом:

```
Active connections: 291
server accepts handled requests
 16630948 16630948 31070465
Reading: 6 Writing: 179 Waiting: 106
```

Директивы

stub_status

Синтаксис	`stub_status;`
По умолчанию	—
Контекст	server, location

Информация о состоянии будет доступна из данного location.

Данные

Доступна следующая информация:

`Active connections`

Текущее число активных клиентских соединений, включая Waiting-соединения.

`accepts`

Суммарное число принятых клиентских соединений.

`handled`

Суммарное число обработанных соединений. Обычно значение этого параметра совпадает с `accepts`, если не достигнуто какое-нибудь системное ограничение (например, лимит *worker_connections*).

`requests`

Суммарное число клиентских запросов.

`Reading`

Текущее число соединений, в которых Angie PRO в настоящий момент читает заголовок запроса.

`Writing`

Текущее число соединений, в которых Angie PRO в настоящий момент отвечает клиенту.

`Waiting`

Текущее число бездействующих клиентских соединений в ожидании запроса.

Встроенные переменные

`$connections_active`

то же, что и значение *Active connections*;

`$connections_reading`

то же, что и значение *Reading*;

`$connections_writing`

то же, что и значение *Writing*;

`$connections_waiting`

то же, что и значение *Waiting*.

Sub

Фильтр, изменяющий в ответе одну заданную строку на другую.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_sub_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
location / {
    sub_filter '<a href="http://127.0.0.1:8080/'  '<a href="https://$host/';
    sub_filter '<img src="http://127.0.0.1:8080/' '<img src="https://$host/';
    sub_filter_once on;
}
```

Директивы

sub_filter

Синтаксис	`sub_filter` *строка замена*;
По умолчанию	—
Контекст	http, server, location

Задает строку, которую нужно заменить, и строку замены. Заменяемая строка проверяется без учета регистра. В заменяемой строке и в строке замены можно использовать переменные. На одном

уровне конфигурации может быть указано несколько директив *sub_filter*. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *sub_filter*.

sub_filter_last_modified

Синтаксис	`sub_filter_last_modified` on | off;
По умолчанию	`sub_filter_last_modified off;`
Контекст	http, server, location

Позволяет сохранить поле заголовка «Last-Modified» исходного ответа во время замены для лучшего кэширования ответов.

По умолчанию поле заголовка удаляется, так как содержимое ответа изменяется во время обработки.

sub_filter_once

Синтаксис	`sub_filter_once` on | off;
По умолчанию	`sub_filter_once on;`
Контекст	http, server, location

Определяет, сколько раз нужно искать каждую из заменяемых строк: один раз или многократно.

sub_filter_types

Синтаксис	`sub_filter_types` mime-*тип* ...;
По умолчанию	`sub_filter_types text/html;`
Контекст	http, server, location

Разрешает замену строк в ответах с указанными MIME-типами в дополнение к «*text/html*». Специальное значение «*» соответствует любому MIME-типу.

Upstream

Предоставляет контекст для описания группы серверов, которые могут использоваться в директивах *proxy_pass*, *fastcgi_pass*, *uwsgi_pass*, *scgi_pass*, *memcached_pass* и *grpc_pass*.

Пример конфигурации

```
upstream backend {
    zone backend 1m;
    server backend1.example.com       weight=5;
    server backend2.example.com:8080;
    server backend3.example.com       service=_example._tcp resolve;
    server unix:/tmp/backend3;

    server backup1.example.com:8080   backup;
    server backup2.example.com:8080   backup;
}

resolver 127.0.0.53 status_zone=resolver;

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

Директивы

bind_conn (PRO)

Синтаксис	`bind_conn` *значение*;
По умолчанию	—
Контекст	upstream

Позволяет привязать серверное соединение к клиентскому в момент, когда *значение*, заданное строкой из переменных, становится отличным от `""` и `"0"`.

Внимание

Директива `bind_conn` должна использоваться после всех директив, задающих тот или иной метод балансировки нагрузки, иначе она не будет работать. Если она используется наряду с директивой *sticky*, то `bind_conn` должна стоять после `sticky`.

Внимание

При использовании директивы настройки модуля *Proxy* должны допускать использование постоянных соединений, например:

```
proxy_http_version 1.1;
proxy_set_header Connection "";
```

Типичный пример использования директивы — проксирование соединений с NTLM-аутентификацией, где требуется обеспечить привязку клиента к серверу в начале согласования:

```
map $http_authorization   $ntlm {
    ~*^N(?:TLM|egotiate)  1;
```

```
}

upstream ntlm_backend {
    server 127.0.0.1:8080;
    bind_conn $ntlm;
}

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

feedback (PRO)

Добавлено в версии 1.6.0: PRO

Синтаксис	`feedback` *переменная* [inverse] [factor=*число*] [account=*условная_переменная*] [last_byte];
По умолчанию	—
Контекст	upstream

Задает в `upstream` механизм балансировки нагрузки по обратной связи. Он динамически корректирует решения при балансировке, умножая вес каждого проксируемого сервера на среднее значение обратной связи, которое меняется с течением времени в зависимости от значения *переменной* и подчиняется необязательному условию.

Могут быть заданы следующие параметры:

`переменная`	Переменная, из которой берется значение обратной связи. Она должна представлять собой метрику производительности или состояния; предполагается, что сервер передает ее в заголовках или иным образом. Значение оценивается при каждом ответе от сервера и учитывается в скользящем среднем согласно настройкам `inverse` и `factor`.
`inverse`	Если параметр задан, значение обратной связи интерпретируется наоборот: более низкие значения указывают на лучшую производительность.
`factor`	Коэффициент, по которому значение обратной связи учитывается при расчете среднего. Допустимы целые числа от 0 до 99. По умолчанию — `90`. Среднее рассчитывается по формуле экспоненциального сглаживания. Чем больше коэффициент, тем меньше новые значения влияют на среднее; если указать `90`, то будет взято 90 % от предыдущего значения и лишь 10 % от нового.
`account`	Указывает условную переменную, которая контролирует, какие ответы учитываются при расчете. Среднее значение обновляется с учетом значения обратной связи из ответа, только если условная переменная этого ответа не равна `""` или `"0"`. **Примечание** По умолчанию ответы в ходе *активных проверок* не включаются в расчет; комбинация переменной *$upstream_probe* с `account` позволяет включить эти ответы или даже исключить все остальное.
`last_byte`	Позволяет обрабатывать данные от проксируемого сервера после получения полного ответа, а не только заголовка.

Пример:

```
upstream backend {

    zone backend 1m;

    feedback $feedback_value factor=80 account=$condition_value;

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

map $upstream_http_custom_score $feedback_value {
    "high"                      100;
    "medium"                    75;
    "low"                       50;
    default                     10;
}

map $upstream_probe $condition_value {
    "high_priority" "1";
    "low_priority"  "0";
    default         "1";
}
```

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

hash

Синтаксис	`hash` *ключ* [consistent];
По умолчанию	—
Контекст	upstream

Задает метод балансировки нагрузки для группы, при котором соответствие клиента серверу определяется при помощи хэшированного значения ключа. В качестве ключа может использоваться текст, переменные и их комбинации. Следует отметить, что любое добавление или удаление серверов в группе может привести к перераспределению большинства ключей на другие серверы. Метод совместим с библиотекой Perl Cache::Memcached.

Если задан параметр `consistent`, то вместо вышеописанного метода будет использоваться метод консистентного хэширования ketama. Метод гарантирует, что при добавлении сервера в группу или его удалении на другие серверы будет перераспределено минимальное число ключей. Применение метода для кэширующих серверов обеспечивает больший процент попаданий в кэш. Метод совместим с библиотекой Perl Cache::Memcached::Fast при значении параметра ketama_points равным 160.

ip_hash

Синтаксис	`ip_hash`;
По умолчанию	—
Контекст	upstream

Задает для группы метод балансировки нагрузки, при котором запросы распределяются по серверам на основе IP-адресов клиентов. В качестве ключа для хэширования используются первые три октета IPv4-адреса клиента или IPv6-адрес клиента целиком. Метод гарантирует, что запросы одного и того же клиента будут всегда передаваться на один и тот же сервер. Если же этот сервер будет считаться недоступным, то запросы этого клиента будут передаваться на другой сервер. С большой долей вероятности это также будет один и тот же сервер.

Если один из серверов нужно убрать на некоторое время, то для сохранения текущего хэширования IP-адресов клиентов этот сервер нужно пометить параметром `down`:

```
upstream backend {
    ip_hash;

    server backend1.example.com;
    server backend2.example.com;
    server backend3.example.com down;
    server backend4.example.com;
}
```

keepalive

Синтаксис	`keepalive` *соединения*;
По умолчанию	—
Контекст	upstream

Задействует кэш соединений для группы серверов.

Параметр `соединения` устанавливает максимальное число неактивных постоянных соединений с серверами группы, которые будут сохраняться в кэше каждого рабочего процесса. При превышении этого числа наиболее давно не используемые соединения закрываются.

Примечание

Следует особо отметить, что директива *keepalive* не ограничивает общее число соединений с серверами группы, которые рабочие процессы Angie PRO могут открыть. Параметр соединения следует устанавливать достаточно консервативно, чтобы серверы группы по-прежнему могли обрабатывать новые входящие соединения.

Внимание

Директива `keepalive` должна использоваться после всех директив, задающих тот или иной метод балансировки нагрузки, иначе она не будет работать.

Пример конфигурации группы серверов memcached с постоянными соединениями:

```
upstream memcached_backend {
    server 127.0.0.1:11211;
    server 10.0.0.2:11211;

    keepalive 32;
}

server {
    #...

    location /memcached/ {
        set $memcached_key $uri;
        memcached_pass memcached_backend;
    }

}
```

Для HTTP директиву *proxy_http_version* следует установить в «1.1», а поле заголовка «Connection» — очистить:

```
upstream http_backend {
    server 127.0.0.1:8080;

    keepalive 16;
}

server {
```

```
    #...

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

Примечание

Хоть это и не рекомендуется, но также возможно использование постоянных соединений с HTTP/1.0, путем передачи поля заголовка «Connection: Keep-Alive» серверу группы.

Для работы постоянных соединений с FastCGI-серверами потребуется включить директиву *fastcgi_keep_conn*:

```
upstream fastcgi_backend {
    server 127.0.0.1:9000;

    keepalive 8;
}

server {
    #...

    location /fastcgi/ {
        fastcgi_pass fastcgi_backend;
        fastcgi_keep_conn on;
    #    ...
    }
}
```

Примечание

Протоколы SCGI и uwsgi не определяют семантику постоянных соединений.

keepalive_requests

Синтаксис	`keepalive_requests` *число*;
По умолчанию	`keepalive_requests 1000;`
Контекст	upstream

Задает максимальное число запросов, которые можно сделать по одному постоянному соединению. После того как сделано максимальное число запросов, соединение закрывается.

Периодическое закрытие соединений необходимо для освобождения памяти, выделенной под конкретные соединения. Поэтому использование слишком большого максимального числа запросов может приводить к чрезмерному потреблению памяти и не рекомендуется.

keepalive_time

Синтаксис	`keepalive_time` *время*;
По умолчанию	`keepalive_time 1h;`
Контекст	upstream

Ограничивает максимальное время, в течение которого могут обрабатываться запросы в рамках постоянного соединения. По достижении заданного времени соединение закрывается после обработки очередного запроса.

keepalive_timeout

Синтаксис	`keepalive_timeout` *время*;
По умолчанию	`keepalive_timeout 60s;`
Контекст	upstream

Задает таймаут, в течение которого неактивное постоянное соединение с сервером группы не будет закрыто.

least_conn

Синтаксис	`least_conn`;
По умолчанию	—
Контекст	upstream

Задает для группы метод балансировки нагрузки, при котором запрос передается серверу с наименьшим числом активных соединений, с учетом весов серверов. Если подходит сразу несколько серверов, они выбираются циклически (в режиме round-robin) с учетом их весов.

least_time (PRO)

Синтаксис	`least_time` header | last_byte [factor=*число*] [account=*условная_переменная*];
По умолчанию	—
Контекст	upstream

Задает для группы метод балансировки нагрузки, при котором вероятность передачи запроса активному серверу обратно пропорциональна среднему времени его ответа; чем оно меньше, тем больше запросов будет получать сервер.

`header`	Директива учитывает среднее время получения заголовков ответа.
`last_byte`	Директива использует среднее время получения полного ответа.

Добавлено в версии 1.7.0: PRO

`factor`	Выполняет ту же функцию, что и *response_time_factor (PRO)*, и переопределяет его, если параметр задан.
`account`	Указывает условную переменную, которая контролирует, какие ответы учитываются при расчете. Среднее значение обновляется, только если условная переменная ответа не равна `""` или `"0"`. **Примечание** По умолчанию ответы в ходе *активных проверок* не включаются в расчет; комбинация переменной *$upstream_probe* с `account` позволяет включить эти ответы или даже исключить все остальное.

Текущие средние значения, вычисленные с учетом `factor` и `account`, представлены также как `header_time` и `response_time` в объекте `health` сервера среди *метрик апстрима* в API.

queue (PRO)

Добавлено в версии 1.4.0: PRO

Синтаксис	`queue` *число* [timeout=*время*];
По умолчанию	—
Контекст	upstream

Если для запроса не удается назначить проксируемый сервер с первой попытки (например, при краткосрочном перебое в работе или всплеске нагрузки с достижением предела *max_conns*), запрос не отклоняется; вместо этого Angie PRO пытается поставить его в очередь на обработку.

Численный параметр директивы задает максимальное количество запросов в очереди *рабочего процесса*. Если очередь целиком заполнена, клиенту отдается ошибка `502 (Bad Gateway)`.

Примечание

К запросам в очереди также применяется логика директивы *proxy_next_upstream*. В частности, если для запроса был выбран сервер, но передать его туда не удалось, то он может вернуться в очередь.

Если сервер для передачи запроса в очереди не был выбран за *время* `timeout` (по умолчанию — 60 секунд), клиенту отдается ошибка `502 (Bad Gateway)`. Еще из очереди удаляются запросы от клиентов, преждевременно закрывших соединение; в *API* есть счетчики состояний запросов, проходящих через очередь.

Внимание

Директива `queue` должна использоваться после всех директив, задающих тот или иной метод балансировки нагрузки, иначе она не будет работать.

random

Синтаксис	`random` [two];
По умолчанию	—
Контекст	upstream

Задает для группы метод балансировки нагрузки, при котором запрос передается случайно выбранному серверу, с учетом весов серверов.

Если указан необязательный параметр `two`, Angie PRO случайным образом выбирает два сервера, из которых выбирает сервер, используя метод *least_conn*, при котором запрос передается на сервер с наименьшим количеством активных соединений.

response_time_factor (PRO)

Синтаксис	`response_time_factor` *число*;
По умолчанию	`response_time_factor 90;`
Контекст	upstream

Задает для метода балансировки нагрузки *least_time (PRO)* коэффициент сглаживания **предыдущего** значения при вычислении среднего времени ответа по формуле экспоненциально взвешенного скользящего среднего.

Чем больше указанное *число*, тем меньше новые значения влияют на среднее; если указать `90`, то будет взято 90 % от предыдущего значения и лишь 10 % от нового. Допустимые значения — от 0 до 99 включительно.

Текущие средние значения представлены как `header_time` (только заголовки) и `response_time` (ответы целиком) в объекте `health` сервера среди *метрик апстрима* в API.

> **Примечание**
>
> При подсчете учитываются только успешные ответы; что считать неуспешным ответом, определяют директивы *proxy_next_upstream*, *fastcgi_next_upstream*, *uwsgi_next_upstream*, *scgi_next_upstream*, *memcached_next_upstream* и *grpc_next_upstream*. Кроме того, значение `header_time` пересчитывается, только если получены и обработаны все заголовки, а `response_time` — только если получен весь ответ.

server

Синтаксис	`server` *адрес* [*параметры*];
По умолчанию	—
Контекст	upstream

Задает адрес и другие параметры сервера. Адрес может быть указан в виде доменного имени или IP-адреса, и необязательного порта, или в виде пути UNIX-сокета, который указывается после префикса `unix:`. Если порт не указан, используется порт 80. Доменное имя, которому соответствует несколько IP-адресов, задает сразу несколько серверов.

Могут быть заданы следующие параметры:

`weight=`*число*	задает вес сервера по умолчанию 1.
`max_conns=`*число*	ограничивает максимальное число одновременных активных соединений к проксируемому серверу. Значение по умолчанию равно `0` и означает, что ограничения нет. Если группа не находится в *зоне* разделяемой памяти, то ограничение работает отдельно для каждого рабочего процесса.

Примечание

При включенных *неактивных постоянных* соединениях, нескольких *рабочих процессах* и *зоне разделяемой памяти*, суммарное число активных и неактивных соединений с проксируемым сервером может превышать значение *max_conns*.

`max_fails=`*число* — задает число неудачных попыток связи с сервером, которые должны произойти в течение заданного *fail_timeout* времени для того, чтобы сервер считался недоступным; после этого он будет повторно проверен через то же самое время.

Что считается неудачной попыткой, определяется директивами *proxy_next_upstream*, *fastcgi_next_upstream*, *uwsgi_next_upstream*, *scgi_next_upstream*, *memcached_next_upstream* и *grpc_next_upstream*.

При превышении `max_fails` сервер также признается неработающим с точки зрения *upstream_probe (PRO)*; клиентские запросы не будут направляться к нему, пока проверки не признают его работающим.

Примечание

Если директива `server` в группе разрешается в несколько серверов, ее настройка `max_fails` применяется к каждому серверу отдельно.

Если после разрешения всех директив `server` в апстриме остается только один сервер, настройка `max_fails` не действует и будет проигнорирована.

`max_fails=1`	число попыток по умолчанию
`max_fails=0`	отключает учет попыток

`fail_timeout=`*время* — задает период времени, в течение которого должно произойти определенное число неудачных попыток связи с сервером (*max_fails*), чтобы сервер считался недоступным. Затем сервер остается недоступным в течение того же самого времени, прежде чем будет проверен повторно.

Значение по умолчанию — 10 секунд.

Примечание

Если директива `server` в группе разрешается в несколько серверов, ее настройка `fail_timeout` применяется к каждому серверу отдельно.

Если после разрешения всех директив `server` в апстриме остается только один сервер, настройка `fail_timeout` не действует и будет проигнорирована.

`backup`	помечает сервер как запасной. На него будут передаваться запросы в случае, если не работают основные серверы.
`down`	помечает сервер как постоянно недоступный.
`drain`	помечает сервер как разгружаемый (draining); это значит, что он получает только запросы сессий, привязанных ранее через *sticky*. В остальном поведение такое же, как в режиме `down`.

Осторожно

Параметр `backup` нельзя использовать совместно с методами балансировки нагрузки *hash*, *ip_hash* и *random*.

Параметры `down` и `drain` взаимно исключающие.

Добавлено в версии 1.1.0.

`resolve`	позволяет отслеживать изменения списка IP-адресов, соответствующего доменному имени, и обновлять его без перезагрузки конфигурации. При этом группа должна находиться в *зоне разделяемой памяти*; также должен быть определен *преобразователь имен в адреса*.
`service=`*имя*	включает преобразование SRV-записей DNS и задает имя сервиса. Для работы параметра необходимо задать параметр *resolve* у сервера, не указывая порт сервера при имени хоста. Если в имени службы нет точек, формируется имя по стандарту RFC: к имени службы добавляется префикс `_`, затем через точку добавляется `_tcp`. Так, имя службы `http` даст в результате `_http._tcp`. Angie PRO разрешает SRV-записи, объединяя нормализованное имя службы и имя хоста и получая список серверов для полученной комбинации через DNS, вместе с их приоритетами и весами. • SRV-записи с наивысшим приоритетом (те, которые имеют минимальное значение приоритета) разрешаются как основные серверы, а прочие записи становятся запасными серверами. Если `backup` установлено с `server`, SRV-записи с наивысшим приоритетом разрешаются как запасные серверы, а прочие записи игнорируются. • Вес аналогичен параметру `weight` директивы `server`. Если вес задан как в самой директиве, так и в SRV-записи, используется вес, установленный в директиве.

В этом примере выполняется поиск записи `_http._tcp.backend.example.com`:

```
server backend.example.com service=http resolve;
```

Добавлено в версии 1.2.0: Angie

Добавлено в версии 1.1.0-P1: Angie PRO

`sid=`*id*	задает ID сервера в группе. Если параметр не задан, то ID задается как шестнадцатеричный MD5-хэш IP-адреса и порта или пути UNIX-сокета.

Добавлено в версии 1.4.0.

`slow_start=`*время*	задает *время* восстановления веса сервера, возвращающегося к работе при балансировке нагрузки методом *round-robin* или *least_conn*. Если параметр задан и сервер после сбоя снова считается работающим с точки зрения *max_fails* и *upstream_probe (PRO)*, то такой сервер равномерно набирает указанный для него вес в течение заданного времени. Если параметр не задан, то в аналогичной ситуации сервер сразу начинает работу с указанным для него весом.

Примечание

Если в апстриме задан только один `server`, `slow_start` не работает и будет игнорироваться.

state (PRO)

Добавлено в версии 1.2.0: PRO

Синтаксис	`state` *файл*;
По умолчанию	—
Контекст	upstream

Указывает *файл*, где постоянно хранится список серверов апстрима. При установке из наших пакетов для хранения таких файлов специально создается каталог `/var/lib/angie/state/` (`/var/db/angie/state/` во FreeBSD) с соответствующими правами доступа, и в конфигурации остается добавить лишь имя файла:

```
upstream backend {

    zone backend 1m;
    state /var/lib/angie/state/<ИМЯ ФАЙЛА>;
}
```

Список серверов здесь имеет формат, аналогичный `server`. Содержимое файла изменяется при любом изменении серверов в разделе */config/http/upstreams/* через API конфигурации. Файл считывается при запуске Angie PRO или перезагрузке конфигурации.

Осторожно

Чтобы использовать директиву `state` в блоке `upstream`, в нем не должно быть директив `server`, но нужна зона разделяемой памяти (*zone*).

sticky

Добавлено в версии 1.2.0: Angie

Добавлено в версии 1.1.0-P1: Angie PRO

Синтаксис	`sticky` cookie *name* [*attr*=*значение*]...; `sticky` route *$variable*...; `sticky` learn zone=*зона* create=*$create_var1*... lookup=*$lookup_var1*... [header] [timeout=*время*];
По умолчанию	—
Контекст	upstream

Настраивает привязку клиентских сессий к проксируемым серверам в режиме, заданном первым параметром; для разгрузки серверов, у которых задана директива `sticky`, можно использовать опцию `drain` в блоке *server*.

Внимание

Директива `sticky` должна использоваться после всех директив, задающих тот или иной метод балансировки нагрузки, иначе она не будет работать. Если она используется наряду с директивой *bind_conn (PRO)*, то `bind_conn` должна стоять после `sticky`.

Режим `cookie`

Этот режим использует cookie для хранения сессий. Он подходит для ситуаций, когда cookie уже используются для управления сессиями.

Здесь запрос от клиента, пока не привязанного к какому-то серверу, отправляется на сервер, выбираемый согласно настроенному методу балансировки. При этом Angie PRO устанавливает cookie с уникальным значением, идентифицирующим сервер.

Имя cookie (`name`) задается директивой `sticky`, а значение (`value`) соответствует параметру *sid* директивы *server*. Учтите, что параметр дополнительно хэшируется, если задана директива *sticky_secret*.

Последующие запросы от клиента, содержащие такой cookie, передаются на сервер, заданный значением cookie, то есть сервер с указанным *sid*. Если выбрать сервер не удается или выбранный сервер не может обработать запрос, то будет выбран другой сервер согласно настроенному методу балансировки.

Директива позволяет назначать атрибуты такого cookie; единственный атрибут, устанавливаемый по умолчанию, — `path=/`. Значения атрибутов задаются строками с переменными. Чтобы удалить атрибут, задайте для него пустое значение: `attr=`. Так, `sticky cookie path=` задает cookie без атрибута `path`.

Здесь Angie PRO создает cookie `srv_id` со сроком действия в 1 час и доменом, заданным переменной:

```
upstream backend {
    server backend1.example.com:8080;
    server backend2.example.com:8080;

    sticky cookie srv_id domain=$my_domain max-age=3600;
}
```

Режим `route`

Этот режим использует предопределенные идентификаторы маршрутов, которые могут быть встроены в URL, cookie или другие свойства запроса. Он менее гибок, так как зависит от предопределенных значений, но лучше подходит, если такие идентификаторы уже используются.

Здесь проксируемый сервер при получении запроса может назначить клиенту маршрут и вернуть его идентификатор способом, известным и клиенту, и серверу. В качестве идентификатора маршрута должно использоваться значение параметра *sid* директивы *server*. Учтите, что параметр дополнительно хэшируется, если задана директива *sticky_ secret*.

Последующие запросы от клиентов, желающих использовать этот маршрут, должны содержать выданный сервером идентификатор, причем так, чтобы он попал в переменные Angie PRO, например в *cookie* или *аргументы запроса*.

В параметрах директивы указываются переменные для маршрутизации. Чтобы выбрать сервер, куда передается поступивший запрос, используется первая непустая переменная; она затем сравнивается с параметром *sid* директивы *server*. Если выбрать сервер не удается или выбранный сервер не может обработать запрос, то будет выбран другой сервер согласно настроенному методу балансировки.

Здесь Angie PRO ищет идентификатор маршрута в cookie `route`, затем в аргументе запроса `route`:

```
upstream backend {
    server backend1.example.com:8080 "sid=server 1";
    server backend2.example.com:8080 "sid=server 2";

    sticky route $cookie_route $arg_route;
}
```

Режим `learn` (PRO 1.4.0+)

В этом режиме для привязки клиента к конкретному проксируемому серверу используется динамически генерируемый ключ; он более гибок, так как назначает серверы на ходу, хранит сеансы в зоне общей памяти и поддерживает различные способы передачи идентификаторов сессий.

Здесь сессия создается на основе ответа проксируемого сервера. С параметрами `create` и `lookup` перечисляются переменные, указывающие, как создаются новые и ищутся существующие сессии. Оба параметра можно использовать по нескольку раз.

Идентификатором сессии служит значение первой непустой переменной, указанной с `create`; например, это может быть *cookie с проксируемого сервера*.

Сессии хранятся в зоне общей памяти; ее имя и размер задаются параметром `zone`. Если к сессии не было обращений в течение *времени* `timeout`, она удаляется. Значение по умолчанию — 10 минут.

Последующие запросы от клиентов, желающих использовать сессию, должны содержать ее идентификатор, причем так, чтобы он попал в непустую переменную, указанную с `lookup`; тогда его значение будет сопоставлено с сессиями в общей памяти. Если выбрать сервер не удается или выбранный сервер не может обработать запрос, то будет выбран другой сервер согласно настроенному методу балансировки.

Параметр `header` позволяет создать сессию сразу после получения заголовков ответа от проксируемого сервера. Без него сессия создается только после завершения обработки запроса.

В примере Angie PRO создает сессию, устанавливая в ответе cookie с именем `examplecookie`:

```
upstream backend {
    server backend1.example.com:8080;
    server backend2.example.com:8080;

    sticky learn
        create=$upstream_cookie_examplecookie
        lookup=$cookie_examplecookie
        zone=client_sessions:1m;
}
```

sticky_secret

Добавлено в версии 1.2.0: Angie

Добавлено в версии 1.1.0-P1: Angie PRO

Синтаксис	`sticky_secret` *строка*;
По умолчанию	—
Контекст	upstream

Добавляет *строку* как соль в функцию MD5-хэширования для директивы *sticky* в режимах `cookie` и `route`. *Строка* может содержать переменные, например *$remote_addr*:

```
upstream backend {
    server backend1.example.com:8080;
    server backend2.example.com:8080;

    sticky cookie cookie_name;
    sticky_secret my_secret.$remote_addr;
}
```

Соль добавляется после хэшируемого значения; чтобы независимо проверить механизм хэширования:

```
$ echo -n "<VALUE><SALT>" | md5sum
```

sticky_strict

Добавлено в версии 1.2.0: Angie

Добавлено в версии 1.1.0-P1: Angie PRO

Синтаксис	`sticky_strict` on | off;
По умолчанию	`sticky_strict off;`
Контекст	upstream

При включении Angie PRO будет возвращать клиенту ошибку HTTP 502, если желаемый сервер недоступен, вместо использования любого другого доступного сервера, как это происходит, когда в группе нет доступных серверов.

upstream

Синтаксис	`upstream` *имя* { ... }
По умолчанию	—
Контекст	http

Описывает группу серверов. Серверы могут слушать на разных портах. Кроме того, можно одновременно использовать серверы, слушающие на TCP- и UNIX-сокетах.

Пример:

```
upstream backend {
    server backend1.example.com weight=5;
    server 127.0.0.1:8080       max_fails=3 fail_timeout=30s;
    server unix:/tmp/backend3;

    server backup1.example.com  backup;
}
```

По умолчанию запросы распределяются по серверам циклически (в режиме round-robin) с учетом весов серверов. В вышеприведенном примере каждые 7 запросов будут распределены так: 5 запросов на backend1.example.com и по одному запросу на второй и третий серверы.

Если при попытке работы с сервером происходит ошибка, то запрос передается следующему серверу, и так далее до тех пор, пока не будут опробованы все работающие серверы. Если не удастся получить успешный ответ ни от одного из серверов, то клиенту будет возвращен результат работы с последним сервером.

zone

Синтаксис	`zone` *имя* [*размер*];
По умолчанию	—
Контекст	upstream

Задает имя и размер зоны разделяемой памяти, в которой хранятся конфигурация группы и ее рабочее состояние, разделяемые между рабочими процессами. В одной и той же зоне могут быть сразу несколько групп. В этом случае достаточно указать размер только один раз.

Встроенные переменные

Модуль `http_upstream` поддерживает следующие встроенные переменные:

$upstream_addr

хранит IP-адрес и порт или путь к UNIX-сокету сервера группы. Если при обработке запроса были сделаны обращения к нескольким серверам, то их адреса разделяются запятой, например:

> 192.168.1.1:80, 192.168.1.2:80, unix:/tmp/sock

Если произошло внутреннее перенаправление от одной группы серверов на другую с помощью «X-Accel-Redirect» или *error_page*, то адреса, соответствующие разным группам серверов, разделяются двоеточием, например:

> 192.168.1.1:80, 192.168.1.2:80, unix:/tmp/sock : 192.168.10.1:80, 192.168.10.2:80

Если сервер не может быть выбран, то переменная хранит *имя группы серверов*.

`$upstream_bytes_received`

число байт, полученных от сервера группы. Значения нескольких соединений разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_ addr*.

`$upstream_bytes_sent`

число байт, переданных на сервер группы. Значения нескольких соединений разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_ addr*.

`$upstream_cache_status`

хранит статус доступа к кэшу ответов. Статус может быть одним из `MISS`, `BYPASS`, `EXPIRED`, `STALE`, `UPDATING`, `REVALIDATED` или `HIT`:

- `MISS`: Ответ не найден в кэше, и запрос передан на сервер.
- `BYPASS`: Кэш обойден, и запрос напрямую передан на сервер.
- `EXPIRED`: Ответ в кэше устарел, и на сервер передан новый запрос для обновления контента.
- `STALE`: Ответ в кэше устарел, но по-прежнему передается клиентам, пока через какое-то время не произойдет обновление контента с сервера.
- `UPDATING`: Ответ в кэше устарел, но по-прежнему передается клиентам, пока уже идущее обновление контента с сервера не завершится.
- `REVALIDATED`: Ответ в кэше устарел, но был успешно перепроверен и не нуждается в обновлении с сервера.
- `HIT`: Ответ был взят из кэша.

Если запрос пошел в обход кэша без обращения к нему, переменная не устанавливается.

`$upstream_connect_time`

хранит время, затраченное на установление соединения с сервером группы; время хранится в секундах с точностью до миллисекунд. В случае SSL включает в себя время, потраченное на рукопожатие. Времена нескольких соединений разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_ addr*.

`$upstream_cookie_` ***имя***

cookie с указанным именем, переданный сервером группы в поле «Set-Cookie» заголовка ответа. Необходимо иметь в виду, что cookie запоминаются только из ответа последнего сервера.

`$upstream_header_time`

хранит время, затраченное на получение заголовка ответа от сервера группы; время хранится в секундах с точностью до миллисекунд. Времена нескольких ответов разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_ addr*.

`$upstream_http_` ***имя***

хранят поля заголовка ответа сервера. Например, поле заголовка ответа «Server» доступно в переменной *$upstream_http_server*. Правила преобразования имен полей заголовка ответа в имена переменных такие же, как для переменных с префиксом «$http_». Необходимо иметь в виду, что поля заголовка запоминаются только из ответа последнего сервера.

`$upstream_queue_time`

хранит время, проведенное запросом в *очереди* до очередного выбора сервера и выраженное в секундах с точностью до миллисекунд. Времена нескольких попыток разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_addr*.

`$upstream_response_length`

хранит длину ответа, полученного от сервера группы; длина хранится в байтах. Длины нескольких ответов разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_addr*.

`$upstream_response_time`

хранит время, затраченное на получение ответа от сервера группы; время хранится в секундах с точностью до миллисекунд. Времена нескольких ответов разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_addr*.

`$upstream_status`

хранит статус ответа, полученного от сервера группы. Статусы нескольких ответов разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_addr*. Если сервер не может быть выбран, то переменная хранит статус 502 (Bad Gateway).

`$upstream_sticky_status`

Статус привязанных запросов.

`""`	Запрос отправлен в группу серверов, где привязка не включена.
`NEW`	Запрос не содержит информации о привязке к серверу.
`HIT`	Запрос с привязкой отправлен на желаемый сервер.
`MISS`	Запрос с привязкой отправлен на сервер, выбранный по алгоритму балансировки.

Статусы из нескольких соединений разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_addr*.

`$upstream_trailer_` ***имя***

хранит поля из конца ответа, полученного от сервера группы.

Upstream Probe

Реализует активные проверки работоспособности (health probes) для *Upstream*.

Пример конфигурации

```
server {
    listen ...;

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

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

Директивы

upstream_probe (PRO)

Добавлено в версии 1.2.0: PRO

Синтаксис	`upstream_probe` *имя* [uri=*адрес*] [port=*число*] [interval=*время*] [method=*метод*] [test=*условие*] [essential [persistent]] [fails=*число*] [passes=*число*] [max_body=*размер*] [mode=always|idle|onfail];
По умолчанию	—
Контекст	location

Задает активную проверку работоспособности серверов тех *upstream*, которые указаны в директивах *proxy_pass*, *uwsgi_pass* и т. д. в том же контексте `location`, где находится директива `upstream_probe`. При этом Angie PRO регулярно выполняет запросы согласно указанным параметрам к каждому серверу в составе апстрима.

Сервер проходит проверку, если запрос к нему успешно выполняется с учетом всех параметров самой директивы `upstream_probe` и всех параметров, влияющих на использование апстримов тем контекстом `location`, где она задана. Это касается в том числе директив *proxy_next_upstream*, *uwsgi_next_upstream* и пр., а также *proxy_set_header* и т. д.

Чтобы использовать проверки, в апстриме необходима зона разделяемой памяти (*zone*). Для одного апстрима можно определить несколько проверок.

Могут быть заданы следующие параметры:

`имя`	Обязательное имя проверки.
`uri`	URI запроса, который добавляется к аргументу *proxy_pass*, *uwsgi_pass* и т. д. По умолчанию — `/`.
`port`	Альтернативный порт для запроса.
`interval`	Интервал между проверками. По умолчанию — `5s`.
`method`	HTTP-метод запроса проверки. По умолчанию — `GET`.
`test`	Проверяемое при запросе условие; задается строкой с переменными. Если результат подстановки переменных — `""` или `"0"`, проверка не пройдена.
`essential`	Если параметр задан, то изначально состояние сервера подлежит уточнению и клиентские запросы не передаются ему, пока проверка не будет пройдена.
`persistent`	Установка этого параметра требует сначала включить `essential`; серверы с `persistent`, работавшие до *перезагрузки конфигурации*, начинают получать запросы без необходимости сначала пройти эту проверку.
`fails`	Число последовательных неуспешных запросов, при котором проверка считает сервер неработающим. По умолчанию — 1.
`passes`	Число последовательных успешных запросов, при котором проверка считает сервер работающим. По умолчанию — 1.
`max_body`	Максимальный объем памяти для тела ответа. По умолчанию — `256k`.
`mode`	Режим проверки в зависимости от работоспособности серверов: • `always` — серверы проверяются независимо от состояния; • `idle` — проверяются неработающие серверы, а также серверы, где с последнего клиентского запроса прошло время `interval`. • `onfail` — проверяются серверы только в неработающем состоянии. По умолчанию — `always`.

Пример:

```
upstream backend {
    zone backend 1m;

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

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

server {
    listen ...;

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

        upstream_probe backend_probe
            uri=/probe
            port=10004
            interval=5s
            test=$good
            essential
            persistent
            fails=3
```

```
            passes=3
            max_body=10m
            mode=idle;
    }
}
```

Детали работы:

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

Встроенные переменные

Модуль `http_upstream_probe` поддерживает следующие встроенные переменные:

`$upstream_probe` (PRO)

Имя активной сейчас проверки *upstream_probe*.

`$upstream_probe_body` (PRO)

Тело ответа от сервера, полученного при проверке *upstream_probe*. Его размер ограничен параметром `max_body`.

UserID

Выдает cookie для идентификации клиентов. Для записи в лог полученных и выданных cookie можно использовать встроенные переменные *$uid_got* и *$uid_set*. Модуль совместим с модулем mod_uid для Apache.

Пример конфигурации

```
userid         on;
userid_name    uid;
userid_domain  example.com;
userid_path    /;
userid_expires 365d;
userid_p3p     'policyref="/w3c/p3p.xml", CP="CUR ADM OUR NOR STA NID"';
```

Директивы

userid

Синтаксис	`userid` on | v1 | log | off;
По умолчанию	`userid off;`
Контекст	http, server, location

Разрешает или запрещает выдачу cookie и запись приходящих cookie в лог:

`on`	разрешает выдачу cookie версии 2 и запись приходящих cookie в лог;
`v1`	разрешает выдачу cookie версии 1 и запись приходящих cookie в лог;
`log`	запрещает выдачу cookie, но разрешает запись приходящих cookie в лог;
`off`	запрещает выдачу cookie и запись приходящих cookie в лог.

userid_domain

Синтаксис	`userid_domain` *имя* | none;
По умолчанию	`userid_domain none;`
Контекст	http, server, location

Задает домен, для которого устанавливается cookie. Параметр `none` запрещает выдавать домен для cookie.

userid_expires

Синтаксис	`userid_expires` *время* | max | off;
По умолчанию	`userid_expires off;`
Контекст	http, server, location

Задает время, в течение которого браузер должен хранить cookie. Параметр max устанавливает срок хранения cookie до 31 декабря 2037 года 23:55:55 GMT. Указание параметра `off` позволяет ограничить время действия cookie сессией браузера.

userid_flags

Синтаксис	`userid_flags` off | *флаг* ...;
По умолчанию	`userid_flags off;`
Контекст	http, server, location

Если параметр не `off`, задает один или несколько дополнительных флагов для cookie: *secure*, *httponly*, *samesite=strict*, *samesite=lax*, *samesite=none*.

userid_mark

Синтаксис	`userid_mark` *буква* | *цифра* | = | off;
По умолчанию	`userid_mark off;`
Контекст	http, server, location

Если параметр не `off`, включает механизм маркировки cookie и задает символ, используемый в качестве метки. Этот механизм позволяет добавить или изменить *userid_p3p* и/или время хранения cookie, но при этом оставить неизменным идентификатор клиента. Меткой может быть любая буква английского алфавита (с учетом регистра), цифра или знак «=».

Если метка задана, то она сравнивается с первым дополняющим символом в base64 представлении идентификатора клиента, передаваемом в cookie. Если они не совпадают, то cookie перепосылается с заданной меткой, временем хранения и заголовком «P3P».

userid_name

Синтаксис	`userid_name` *имя*;
По умолчанию	`userid_name uid;`
Контекст	http, server, location

Задает имя cookie.

userid_p3p

Синтаксис	`userid_p3p` *строка* | none;
По умолчанию	`userid_p3p none;`
Контекст	http, server, location

Задает значение для поля заголовка «P3P», которое будет выдаваться вместе с cookie. Если задано специальное значение `none`, то в ответе не будет заголовка «P3P».

userid_path

Синтаксис	`userid_path` *путь*;
По умолчанию	`userid_path /;`
Контекст	http, server, location

Задает путь, для которого устанавливается cookie.

userid_service

Синтаксис	`userid_service` *номер*;
По умолчанию	`userid_service <IP-адрес сервера>;`
Контекст	http, server, location

Если идентификаторы выдаются несколькими серверами (сервисами), то каждому сервису следует назначить свой собственный `номер`, для обеспечения уникальности выдаваемых идентификаторов клиентов. По умолчанию для cookie первой версии используется ноль. Для cookie второй версии по умолчанию используется число, составленное из последних четырех октетов IP-адреса сервера.

Встроенные переменные

`$uid_got`

Имя cookie и полученный идентификатор клиента.

`$uid_reset`

Если значением является непустая строка не равная `0`, то клиентские идентификаторы перевыдаются. Специальное значение `log` дополнительно приводит к выдаче сообщений о перевыданных идентификаторах в *error_log*.

`$uid_set`

Имя cookie и выданный идентификатор клиента.

uWSGI

Позволяет передавать запросы uWSGI-серверу.

Пример конфигурации

```
location / {
    include    uwsgi_params;
    uwsgi_pass localhost:9000;
}
```

Директивы

uwsgi_bind

Синтаксис	`uwsgi_bind` *адрес* [transparent] | off;
По умолчанию	—
Контекст	http, server, location

Задает локальный IP-адрес с необязательным портом, который будет использоваться в исходящих соединениях с uwsgi-сервером. В значении параметра допустимо использование переменных. Специальное значение `off` отменяет действие унаследованной с предыдущего уровня конфигурации директивы *uwsgi_bind*, позволяя системе самостоятельно выбирать локальный IP-адрес и порт.

Параметр `transparent` позволяет задать нелокальный IP-адрес, который будет использоваться в исходящих соединениях с uwsgi-сервером, например, реальный IP-адрес клиента:

```
uwsgi_bind $remote_addr transparent;
```

Для работы параметра обычно требуется запустить рабочие процессы Angie PRO с привилегиями *суперпользователя*. В Linux это не требуется, так как если указан параметр *transparent*, то рабочие процессы наследуют *capability CAP_NET_RAW* из главного процесса.

Важно

Необходимо настроить таблицу маршрутизации ядра для перехвата сетевого трафика с uwsgi-сервера.

uwsgi_buffer_size

Синтаксис	`uwsgi_buffer_size` *размер*;
По умолчанию	`uwsgi_buffer_size 4k|8k;`
Контекст	http, server, location

Задает размер буфера, в который будет читаться первая часть ответа, получаемого от uwsgi-сервера. В этой части ответа обычно находится небольшой заголовок ответа. По умолчанию размер одного буфера равен размеру страницы памяти. В зависимости от платформы это или 4K, или 8K, однако его можно сделать меньше.

uwsgi_buffering

Синтаксис	`uwsgi_buffering` *размер*;
По умолчанию	`uwsgi_buffering on;`
Контекст	http, server, location

`on`	Angie PRO принимает ответ uwsgi-сервера как можно быстрее, сохраняя его в буферы, заданные директивами *uwsgi_buffer_size* и *uwsgi_buffers*. Если ответ не вмещается целиком в память, то его часть может быть записана на диск во *временный файл*. Запись во временные файлы контролируется директивами *uwsgi_max_temp_file_size* и *uwsgi_temp_file_write_size*.
`off`	Ответ синхронно передается клиенту сразу же по мере его поступления. Angie PRO не пытается считать весь ответ uwsgi-сервера. Максимальный размер данных, который Angie PRO может принять от сервера за один раз, задается директивой *uwsgi_buffer_size*.

Буферизация может быть также включена или выключена путем передачи значения «yes» или «no» в поле «X-Accel-Buffering» заголовка ответа. Эту возможность можно запретить с помощью директивы *uwsgi_ignore_headers*.

uwsgi_buffers

Синтаксис	`uwsgi_buffers` *число размер*;
По умолчанию	`uwsgi_buffers 8 4k|8k;`
Контекст	http, server, location

Задает число и размер буферов для одного соединения, в которые будет читаться ответ, получаемый от uwsgi-сервера. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

uwsgi_busy_buffers_size

Синтаксис	`uwsgi_busy_buffers_size` *размер*;
По умолчанию	`uwsgi_buffers 8k|16k;`
Контекст	http, server, location

При включенной *буферизации* ответов uwsgi-сервера, ограничивает суммарный размер буферов, которые могут быть заняты для отправки ответа клиенту, пока ответ еще не прочитан целиком. Оставшиеся буферы тем временем могут использоваться для чтения ответа и, при необходимости, буферизации части ответа во временный файл. По умолчанию размер ограничен величиной двух буферов, заданных директивами *uwsgi_buffer_size* и *uwsgi_buffers*.

uwsgi_cache

Синтаксис	`uwsgi_cache` *зона* | off;
По умолчанию	`uwsgi_cache off;`
Контекст	http, server, location

Задает зону разделяемой памяти, используемой для кэширования. Одна и та же зона может использоваться в нескольких местах. В значении параметра можно использовать переменные.

`off`	запрещает кэширование, унаследованное с предыдущего уровня конфигурации.

uwsgi_cache_background_update

Синтаксис	`uwsgi_cache_background_update` on | off;
По умолчанию	`uwsgi_cache_background_update off;`
Контекст	http, server, location

Позволяет запустить фоновый подзапрос для обновления просроченного элемента кэша, в то время как клиенту возвращается устаревший кэшированный ответ.

Внимание

Использование устаревшего кэшированного ответа в момент его обновления должно быть *разрешено*.

uwsgi_cache_bypass

Синтаксис	`uwsgi_cache_bypass ...;`
По умолчанию	—
Контекст	http, server, location

Задает условия, при которых ответ не будет браться из кэша. Если значение хотя бы одного из строковых параметров непустое и не равно «0», то ответ не берется из кэша:

```
uwsgi_cache_bypass $cookie_nocache $arg_nocache$arg_comment;
uwsgi_cache_bypass $http_pragma    $http_authorization;
```

Можно использовать совместно с директивой *uwsgi_no_cache*.

uwsgi_cache_key

Синтаксис	`uwsgi_cache_key` *строка*;
По умолчанию	—
Контекст	http, server, location

Задает ключ для кэширования, например,

```
uwsgi_cache_key localhost:9000$request_uri;
```

uwsgi_cache_lock

Синтаксис	`uwsgi_cache_lock` on | off;
По умолчанию	`uwsgi_cache_lock off;`
Контекст	http, server, location

Если включено, одновременно только одному запросу будет позволено заполнить новый элемент кэша, идентифицируемый согласно директиве *uwsgi_cache_key*, передав запрос на uwsgi-сервер. Остальные запросы этого же элемента будут либо ожидать появления ответа в кэше, либо освобождения блокировки этого элемента, в течение времени, заданного директивой *uwsgi_cache_lock_timeout*.

uwsgi_cache_lock_age

Синтаксис	`uwsgi_cache_lock_age` *время*;
По умолчанию	`uwsgi_cache_lock_age 5s;`
Контекст	http, server, location

Если последний запрос, переданный на uwsgi-сервер для заполнения нового элемента кэша, не завершился за указанное время, на uwsgi-сервер может быть передан еще один запрос.

uwsgi_cache_lock_timeout

Синтаксис	`uwsgi_cache_lock_timeout` *время*;
По умолчанию	`uwsgi_cache_lock_timeout 5s;`
Контекст	http, server, location

Задает таймаут для *uwsgi_cache_lock*. По истечении указанного времени запрос будет передан на uwsgi-сервер, однако ответ не будет кэширован.

uwsgi_cache_max_range_offset

Синтаксис	`uwsgi_cache_max_range_offset` *число*;
По умолчанию	—
Контекст	http, server, location

Задает смещение в байтах для запросов с указанием диапазона запрашиваемых байт (byte-range requests). Если диапазон находится за указанным смещением, range-запрос будет передан на uwsgi-сервер и ответ не будет кэширован.

uwsgi_cache_methods

Синтаксис	`uwsgi_cache_methods` GET | HEAD | POST ...;
По умолчанию	`uwsgi_cache_methods GET HEAD;`
Контекст	http, server, location

Если метод запроса клиента указан в этой директиве, то ответ будет кэширован. Методы «GET» и «HEAD» всегда добавляются в список, но тем не менее рекомендуется перечислять их явно. См. также директиву *uwsgi_no_cache*.

uwsgi_cache_min_uses

Синтаксис	`uwsgi_cache_min_uses` *число*;
По умолчанию	`uwsgi_cache_min_uses 1;`
Контекст	http, server, location

Задает число запросов, после которого ответ будет кэширован.

uwsgi_cache_path

Синтаксис	`uwsgi_cache_path` *путь* [levels=*уровни*] [use_temp_path=on|off] keys_zone=*имя:размер* [inactive=*время*] [max_size=*размер*] [min_free=*размер*] [manager_files=*число*] [manager_sleep=*время*] [manager_threshold=*время*] [loader_files=*число*] [loader_sleep=*время*] [loader_threshold=*время*];
По умолчанию	—
Контекст	http

Задает путь и другие параметры кэша. Данные кэша хранятся в файлах. Именем файла в кэше является результат функции MD5 от *ключа кэширования*.

Параметр `levels` задает уровни иерархии кэша: можно задать от 1 до 3 уровней, на каждом уровне допускаются значения 1 или 2.

Например, при использовании

```
uwsgi_cache_path /data/angie/cache levels=1:2 keys_zone=one:10m;
```

имена файлов в кэше будут такого вида:

```
/data/angie/cache/c/29/b7f54b2df7773722d382f4809d65029c
```

Кэшируемый ответ сначала записывается во временный файл, а потом этот файл переименовывается. Временные файлы и кэш могут располагаться на разных файловых системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если кэш будет находиться на той же файловой системе, что и каталог с временными файлами.

Какой из каталогов будет использоваться для временных файлов, определяется параметром `use_temp_path`.

`on`	Если параметр не задан или установлен в значение «on», будет использоваться каталог, задаваемый директивой *uwsgi_temp_path* для данного *location*
`off`	временные файлы будут располагаться непосредственно в каталоге кэша

Кроме того, все активные ключи и информация о данных хранятся в зоне разделяемой памяти, имя и размер которой задаются параметром `keys_zone`. Зоны размером в 1 мегабайт достаточно для хранения около 8 тысяч ключей.

Если к данным кэша не обращаются в течение времени, заданного параметром `inactive`, то данные удаляются, независимо от их свежести. По умолчанию *inactive* равен 10 минутам.

Специальный процесс **cache manager** следит за максимальным размером кэша, а также за минимальным объемом свободного места на файловой системе с кэшем, и удаляет наименее востребован-

ные данные при превышении максимального размера кэша или недостаточном объеме свободного места. Удаление данных происходит итерациями.

`max_size`	максимальное пороговое значение размера кэша
`min_free`	минимальное пороговое значение объема свободного места на файловой системе с кэшем
`manager_files`	максимальное количество удаляемых элементов кэша за одну итерацию По умолчанию *100*
`manager_threshol`	ограничивает время работы одной итерации По умолчанию *200* миллисекунд
`manager_sleep`	время, в течение которого выдерживается пауза между итерациями По умолчанию *50* миллисекунд

Через минуту после старта Angie PRO активируется специальный процесс **cache loader**, который загружает в зону кэша информацию о ранее кэшированных данных, хранящихся на файловой системе. Загрузка также происходит итерациями.

`loader_files`	максимальное количество элементов кэша к загрузке в одну итерацию По умолчанию *100*
`loader_threshold`	ограничивает время работы одной итерации По умолчанию *200* миллисекунд
`loader_sleep`	время, в течение которого выдерживается пауза между итерациями По умолчанию *50* миллисекунд

uwsgi_cache_revalidate

Синтаксис	`uwsgi_cache_revalidate` on | off;
По умолчанию	`uwsgi_cache_revalidate off;`
Контекст	http, server, location

Разрешает ревалидацию просроченных элементов кэша при помощи условных запросов с полями заголовка «If-Modified-Since» и «If-None-Match».

uwsgi_cache_use_stale

Синтаксис	`uwsgi_cache_use_stale` error | timeout | invalid_header | updating | http_500 | http_503 | http_403 | http_404 | http_429 | off ...;
По умолчанию	`uwsgi_cache_use_stale off;`
Контекст	http, server, location

Определяет, в каких случаях можно использовать устаревший кэшированный ответ. Параметры директивы совпадают с параметрами директивы *uwsgi_next_upstream*.

`error`	Позволяет использовать устаревший кэшированный ответ при невозможности выбора uwsgi-сервера для обработки запроса.
`updating`	Дополнительный параметр, разрешает использовать устаревший кэшированный ответ, если на данный момент он уже обновляется. Это позволяет минимизировать число обращений к uwsgi-серверам при обновлении кэшированных данных.

Использование устаревшего кэшированного ответа может также быть разрешено непосредственно в заголовке ответа на определенное количество секунд после того, как ответ устарел:

- Расширение stale-while-revalidate поля заголовка «Cache-Control» разрешает использовать устаревший кэшированный ответ, если на данный момент он уже обновляется.
- Расширение stale-if-error поля заголовка «Cache-Control» разрешает использовать устаревший кэшированный ответ в случае ошибки.

Примечание

Такой способ менее приоритетен, чем задание параметров директивы.

Чтобы минимизировать число обращений к uwsgi-серверам при заполнении нового элемента кэша, можно воспользоваться директивой *uwsgi_cache_lock*.

uwsgi_cache_valid

Синтаксис	`uwsgi_cache_valid` [*код* ...] *время*;
По умолчанию	—
Контекст	http, server, location

Задает время кэширования для разных кодов ответа. Например, директивы

```
uwsgi_cache_valid 200 302 10m;
uwsgi_cache_valid 404      1m;
```

задают время кэширования 10 минут для ответов с кодами 200 и 302 и 1 минуту для ответов с кодом 404.

Если указано только время кэширования,

```
uwsgi_cache_valid 5m;
```

то кэшируются только ответы 200, 301 и 302.

Кроме того, можно кэшировать любые ответы с помощью параметра `any`:

```
uwsgi_cache_valid 200 302 10m;
uwsgi_cache_valid 301      1h;
uwsgi_cache_valid any      1m;
```

Примечание

Параметры кэширования могут также быть заданы непосредственно в заголовке ответа. Такой способ приоритетнее, чем задание времени кэширования с помощью директивы.

- Поле заголовка «X-Accel-Expires» задает время кэширования ответа в секундах. Значение *0* запрещает кэшировать ответ. Если значение начинается с префикса *@*, оно задает абсолютное время в секундах с начала эпохи, до которого ответ может быть кэширован.
- Если в заголовке нет поля «X-Accel-Expires», параметры кэширования определяются по полям заголовка «Expires» или «Cache-Control».
- Ответ, в заголовке которого есть поле «Set-Cookie», не будет кэшироваться.

- Ответ, в заголовке которого есть поле «Vary» со специальным значением «*», не будет кэшироваться. Ответ, в заголовке которого есть поле «Vary» с другим значением, будет кэширован с учетом соответствующих полей заголовка запроса.

Обработка одного или более из этих полей заголовка может быть отключена при помощи директивы *uwsgi_ignore_headers*.

uwsgi_connect_timeout

Синтаксис	`uwsgi_connect_timeout` *время*;
По умолчанию	`uwsgi_connect_timeout 60s;`
Контекст	http, server, location

Задает таймаут для установления соединения с uwsgi-сервером. Необходимо иметь в виду, что этот таймаут обычно не может превышать 75 секунд.

uwsgi_connection_drop

Синтаксис	`uwsgi_connection_drop` *время* | on | off;
По умолчанию	`uwsgi_connection_drop off;`
Контекст	http, server, location

Настраивает завершение всех соединений с проксируемым сервером, если он был удален из группы или помечен как постоянно недоступный в результате процесса *reresolve* или *команды API* `DELETE`.

Соединение завершается, когда обрабатывается следующее событие чтения или записи для клиента или проксируемого сервера.

Установка *времени* включает *таймаут* до завершения соединения; при выборе значения `on` соединения завершаются немедленно.

uwsgi_force_ranges

Синтаксис	`uwsgi_force_ranges` off;
По умолчанию	`uwsgi_force_ranges off;`
Контекст	http, server, location

Включает поддержку диапазонов запрашиваемых байт (byte-range) для кэшированных и некэшированных ответов uwsgi-сервера вне зависимости от наличия поля «Accept-Ranges» в заголовках этих ответов.

uwsgi_hide_header

Синтаксис	`uwsgi_hide_header` *поле*;
По умолчанию	—
Контекст	http, server, location

По умолчанию Angie PRO не передает клиенту поля заголовка «Date», «Server», «X-Pad» и «X-Accel-...» из ответа uwsgi-сервера. Директива *uwsgi_hide_header* задает дополнительные поля, которые не будут передаваться. Если же передачу полей нужно разрешить, можно воспользоваться директивой *uwsgi_pass_header*.

uwsgi_ignore_client_abort

Синтаксис	`uwsgi_ignore_client_abort` on | off;
По умолчанию	`uwsgi_ignore_client_abort off;`
Контекст	http, server, location

Определяет, закрывать ли соединение с uwsgi-сервером в случае, если клиент закрыл соединение, не дождавшись ответа.

uwsgi_ignore_headers

Синтаксис	`uwsgi_ignore_headers` *поле* ...;
По умолчанию	—
Контекст	http, server, location

Запрещает обработку некоторых полей заголовка из ответа uwsgi-сервера. В директиве можно указать поля «X-Accel-Redirect», «X-Accel-Expires», «X-Accel-Limit-Rate», «X-Accel-Buffering», «X-Accel-Charset», «Expires», «Cache-Control», «Set-Cookie» и «Vary».

Если не запрещено, обработка этих полей заголовка заключается в следующем:

- «X-Accel-Expires», «Expires», «Cache-Control», «Set-Cookie» и «Vary» задают *параметры кэширования* ответа;
- «X-Accel-Redirect» производит *внутреннее перенаправление* на указанный URI;
- «X-Accel-Limit-Rate» задает *ограничение скорости* передачи ответа клиенту;
- «X-Accel-Buffering» включает или выключает *буферизацию* ответа;
- «X-Accel-Charset» задает желаемую *кодировку* ответа.

uwsgi_intercept_errors

Синтаксис	`uwsgi_intercept_errors` on | off;
По умолчанию	`uwsgi_intercept_errors off;`
Контекст	http, server, location

Определяет, передавать ли клиенту ответы uwsgi-сервера с кодом больше либо равным 300, или же перехватывать их и перенаправлять на обработку Angie PRO с помощью директивы *error_page*.

uwsgi_limit_rate

Синтаксис	`uwsgi_limit_rate` *скорость*;
По умолчанию	`uwsgi_limit_rate 0;`
Контекст	http, server, location

Ограничивает скорость чтения ответа от uwsgi-сервера. *Скорость* задается в байтах в секунду; можно использовать переменные.

0	отключает ограничение скорости

Примечание

Ограничение устанавливается на запрос, поэтому, если Angie PRO одновременно откроет два соединения к uwsgi-серверу, суммарная скорость будет вдвое выше заданного ограничения. Ограничение работает только в случае, если включена *буферизация* ответов uwsgi-сервера.

uwsgi_max_temp_file_size

Синтаксис	`uwsgi_max_temp_file_size` *размер*;
По умолчанию	`uwsgi_max_temp_file_size 1024m;`
Контекст	http, server, location

Если включена *буферизация* ответов uwsgi-сервера, и ответ не вмещается целиком в буферы, заданные директивами *uwsgi_buffer_size* и *uwsgi_buffers*, часть ответа может быть записана во временный файл. Эта директива задает максимальный размер временного файла. Размер данных, сбрасываемых во временный файл за один раз, задается директивой *uwsgi_temp_file_write_size*.

0	отключает возможность буферизации ответов во временные файлы

Примечание

Данное ограничение не распространяется на ответы, которые будут *кэшированы* или сохранены *на диске*.

uwsgi_modifier1

Синтаксис	`uwsgi_modifier1` *число*;
По умолчанию	`uwsgi_modifier1 0;`
Контекст	http, server, location

Задает значение поля modifier1 в заголовке пакета uwsgi.

uwsgi_modifier2

Синтаксис	`uwsgi_modifier2` *число*;
По умолчанию	`uwsgi_modifier1 0;`
Контекст	http, server, location

Задает значение поля modifier2 в заголовке пакета uwsgi.

uwsgi_next_upstream

Синтаксис	`uwsgi_next_upstream` error | timeout | invalid_header | http_500 | http_503 | http_403 | http_404 | http_429 | non_idempotent | off . . . ;
По умолчанию	`uwsgi_next_upstream error timeout;`
Контекст	http, server, location

Определяет, в каких случаях запрос будет передан следующему в группе *upstream* серверу:

`error`	произошла ошибка соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`timeout`	произошел таймаут во время соединения с сервером, передачи ему запроса или чтения заголовка ответа сервера;
`invalid_header`	сервер вернул пустой или неверный ответ;
`http_500`	сервер вернул ответ с кодом 500;
`http_503`	сервер вернул ответ с кодом 503;
`http_403`	сервер вернул ответ с кодом 403;
`http_404`	сервер вернул ответ с кодом 404;
`http_429`	сервер вернул ответ с кодом 429;
`non_idempotent`	обычно запросы с неидемпотентным методом (*POST*, *LOCK*, *PATCH*) не передаются на другой сервер, если запрос серверу группы уже был отправлен; включение параметра явно разрешает повторять подобные запросы;
`off`	запрещает передачу запроса следующему серверу.

Примечание

Необходимо понимать, что передача запроса следующему серверу возможна только при условии, что клиенту еще ничего не передавалось. То есть, если ошибка или таймаут возникли в середине передачи ответа клиенту, то действие директивы на такой запрос не распространяется.

Директива также определяет, что считается *неудачной попыткой* работы с сервером.

`error timeout invalid_header`	всегда считаются неудачными попытками, даже если они не указаны в директиве
`http_500 http_503 http_429`	считаются неудачными попытками, только если они указаны в директиве
`http_403 http_404`	никогда не считаются неудачными попытками

Передача запроса следующему серверу может быть ограничена по *количеству попыток* и по *времени*.

uwsgi_next_upstream_timeout

Синтаксис	`uwsgi_next_upstream_timeout` *время*;
По умолчанию	`uwsgi_next_upstream_timeout 0;`
Контекст	http, server, location

Ограничивает время, в течение которого возможна передача запроса *следующему* серверу.

`0`	отключает это ограничение

uwsgi_next_upstream_tries

Синтаксис	`uwsgi_next_upstream_tries` *число*;
По умолчанию	`uwsgi_next_upstream_tries 0;`
Контекст	http, server, location

Ограничивает число допустимых попыток для передачи запроса *следующему* серверу.

`0`	отключает это ограничение

uwsgi_no_cache

Синтаксис	`uwsgi_no_cache` *строка* ...;
По умолчанию	—
Контекст	http, server, location

Задает условия, при которых ответ не будет сохраняться в кэш. Если значение хотя бы одного из строковых параметров непустое и не равно «0», то ответ не будет сохранен:

```
uwsgi_no_cache $cookie_nocache $arg_nocache$arg_comment;
uwsgi_no_cache $http_pragma    $http_authorization;
```

Можно использовать совместно с директивой *uwsgi_cache_bypass*.

uwsgi_pass

Синтаксис	`uwsgi_pass` [*протокол*://] *адрес*;
По умолчанию	—
Контекст	location, if в location

Задает протокол и адрес uwsgi-сервера. В качестве протокола можно указать `uwsgi` или `suwsgi` (secured uwsgi, uwsgi через SSL). Адрес может быть указан в виде доменного имени или IP-адреса, и порта:

```
uwsgi_pass localhost:9000;
uwsgi_pass uwsgi://localhost:9000;
uwsgi_pass suwsgi://[2001:db8::1]:9090;
```

или в виде пути UNIX-сокета, который указывается после слова `unix` и заключается в двоеточия:

```
uwsgi_pass unix:/tmp/uwsgi.socket;
```

Если доменному имени соответствует несколько адресов, то все они будут использоваться по очереди (round-robin). Кроме того, в качестве адреса можно указать *группу серверов*. Если используется группа, указать порт невозможно; вместо этого укажите порт для каждого сервера внутри группы отдельно.

В значении параметра можно использовать переменные. В этом случае, если адрес указан в виде доменного имени, имя ищется среди описанных групп серверов и если не найдено, то определяется с помощью *resolver*'а.

uwsgi_pass_header

Синтаксис	`uwsgi_pass_header` *поле* ...;
По умолчанию	—
Контекст	http, server, location

Разрешает передавать от uwsgi-сервера клиенту *запрещенные для передачи* поля заголовка.

uwsgi_pass_request_body

Синтаксис	`uwsgi_pass_request_body` on | off;
По умолчанию	`uwsgi_pass_request_body on;`
Контекст	http, server, location

Позволяет запретить передачу исходного тела запроса на uwsgi-сервер. См. также директиву *uwsgi_pass_request_headers*.

uwsgi_pass_request_headers

Синтаксис	`uwsgi_pass_request_headers` on | off;
По умолчанию	`uwsgi_pass_request_headers on;`
Контекст	http, server, location

Позволяет запретить передачу полей заголовка исходного запроса на uwsgi-сервер. См. также директиву *uwsgi_pass_request_body*.

uwsgi_read_timeout

Синтаксис	`uwsgi_read_timeout` *время*;
По умолчанию	`uwsgi_read_timeout 60s;`
Контекст	http, server, location

Задает таймаут при чтении ответа uwsgi-сервера. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями чтения. Если по истечении этого времени uwsgi-сервер ничего не передаст, соединение закрывается.

uwsgi_request_buffering

Синтаксис	`uwsgi_request_buffering` on | off;
По умолчанию	`uwsgi_request_buffering on;`
Контекст	http, server, location

Разрешает или запрещает использовать буферизацию тела запроса клиента.

`on`	тело запроса полностью *читается* от клиента перед отправкой запроса на uwsgi-сервер.
`off`	тело запроса отправляется на uwsgi-сервер сразу же по мере его поступления. В этом случае запрос не может быть передан *следующему серверу*, если Angie PRO уже начал отправку тела запроса.

Если для отправки тела исходного запроса используется HTTP/1.1 и передача данных частями (chunked transfer encoding), то тело запроса буферизуется независимо от значения директивы.

uwsgi_send_timeout

Синтаксис	`uwsgi_send_timeout` *время*;
По умолчанию	`uwsgi_send_timeout 60s;`
Контекст	http, server, location

Задает таймаут при передаче запроса uwsgi-серверу. Таймаут устанавливается не на всю передачу запроса, а только между двумя операциями записи. Если по истечении этого времени uwsgi-сервер не примет новых данных, соединение закрывается.

uwsgi_socket_keepalive

Синтаксис	`uwsgi_socket_keepalive` on | off;
По умолчанию	`uwsgi_socket_keepalive off;`
Контекст	http, server, location

Конфигурирует поведение «TCP keepalive» для исходящих соединений к uwsgi-серверу.

`""`	По умолчанию для сокета действуют настройки операционной системы.
`on`	для сокета включается параметр *SO_KEEPALIVE*

uwsgi_ssl_certificate

Синтаксис	`uwsgi_ssl_certificate` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с сертификатом в формате PEM для аутентификации на suwsgi-сервере. В имени файла можно использовать переменные.

uwsgi_ssl_certificate_key

Синтаксис	`uwsgi_ssl_certificate_key` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с секретным ключом в формате PEM для аутентификации на suwsgi-сервере.

Вместо файла можно указать значение «engine:*имя*:id», которое загружает ключ с указанным *id* из OpenSSL engine с заданным именем.

В имени файла можно использовать переменные.

uwsgi_ssl_ciphers

Синтаксис	`uwsgi_ssl_ciphers` *шифры*;
По умолчанию	`uwsgi_ssl_ciphers DEFAULT;`
Контекст	http, server, location

Описывает разрешенные шифры для запросов к suwsgi-серверу. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL.

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

uwsgi_ssl_conf_command

Синтаксис	`uwsgi_ssl_conf_command` *имя значение*;
По умолчанию	—
Контекст	http, server, location

Задает произвольные конфигурационные команды OpenSSL при установлении соединения с uwsgi HTTPS-сервером.

Важно

Директива поддерживается при использовании OpenSSL 1.0.2 и выше.

На одном уровне может быть указано несколько директив *uwsgi_ssl_conf_command*. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *uwsgi_ssl_conf_command*.

Осторожно

Следует учитывать, что изменение настроек OpenSSL напрямую может привести к неожиданному поведению.

uwsgi_ssl_crl

Синтаксис	`uwsgi_ssl_crl` *файл*;
По умолчанию	—
Контекст	http, server, location

Указывает файл с отозванными сертификатами (CRL) в формате PEM, используемыми при *проверке* сертификата suwsgi-сервера.

uwsgi_ssl_name

Синтаксис	`uwsgi_ssl_name` *имя*;
По умолчанию	`uwsgi_ssl_name` `имя хоста` из uwsgi_pass;`
Контекст	http, server, location

Позволяет переопределить имя сервера, используемое при *проверке* сертификата uwsgi HTTPS-сервера, а также для *передачи его через SNI* при установлении соединения с suwsgi-сервером.

По умолчанию используется имя хоста из URL'а, заданного директивой *uwsgi_pass*.

uwsgi_ssl_password_file

Синтаксис	`uwsgi_ssl_password_file` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с паролями от *секретных ключей*, где каждый пароль указан на отдельной строке. Пароли применяются по очереди в момент загрузки ключа.

uwsgi_ssl_protocols

Синтаксис	`uwsgi_ssl_protocols` [SSLv2] [SSLv3] [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`uwsgi_ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;`
Контекст	http, server, location

Изменено в версии 1.2.0: Параметр `TLSv1.3` добавлен к используемым по умолчанию.

Разрешает указанные протоколы для запросов к suwsgi-серверу.

uwsgi_ssl_server_name

Синтаксис	`uwsgi_ssl_server_name` on | off;
По умолчанию	`uwsgi_ssl_server_name off;`
Контекст	http, server, location

Разрешает или запрещает передачу имени сервера, заданного директивой *uwsgi_ssl_name*, через расширение Server Name Indication протокола TLS (SNI, RFC 6066) при установлении соединения с защищенным uwsgi-сервером.

uwsgi_ssl_session_reuse

Синтаксис	`uwsgi_ssl_session_reuse` on | off;
По умолчанию	`uwsgi_ssl_session_reuse on;`
Контекст	http, server, location

Определяет, использовать ли повторно SSL-сессии при работе с suwsgi-сервером. Если в логах появляются ошибки «*SSL3_GET_FINISHED:digest check failed*», то можно попробовать выключить повторное использование сессий.

uwsgi_ssl_trusted_certificate

Синтаксис	`uwsgi_ssl_trusted_certificate` *файл*;
По умолчанию	—
Контекст	http, server, location

Задает файл с доверенными сертификатами CA в формате PEM, используемыми при *проверке* сертификата uwsgi HTTPS-сервера.

uwsgi_ssl_verify

Синтаксис	`uwsgi_ssl_verify` on | off;
По умолчанию	`uwsgi_ssl_verify off;`
Контекст	http, server, location

Разрешает или запрещает проверку сертификата suwsgi-сервера.

uwsgi_ssl_verify_depth

Синтаксис	`uwsgi_ssl_verify_depth` *число*;
По умолчанию	`uwsgi_ssl_verify_depth 1;`
Контекст	http, server, location

Устанавливает глубину проверки в цепочке сертификатов suwsgi-сервера.

uwsgi_store

Синтаксис	`uwsgi_store` on | off | *строка*;
По умолчанию	`uwsgi_store off;`
Контекст	http, server, location

Разрешает сохранение на диск файлов.

`on`	сохраняет файлы в соответствии с путями, указанными в директивах *alias* или *root*
`off`	запрещает сохранение файлов

Имя файла можно задать явно с помощью `строки` с переменными:

```
uwsgi_store /data/www$original_uri;
```

Время изменения файлов выставляется согласно полученному полю «Last-Modified» в заголовке ответа. Ответ сначала записывается во временный файл, а потом этот файл переименовывается. Временный файл и постоянное место хранения ответа могут располагаться на разных файловых

системах. Однако нужно учитывать, что в этом случае вместо дешевой операции переименовывания в пределах одной файловой системы файл копируется с одной файловой системы на другую. Поэтому лучше, если сохраняемые файлы будут находиться на той же файловой системе, что и каталог с временными файлами, задаваемый директивой *uwsgi_temp_path* для данного *location*.

Директиву можно использовать для создания локальных копий статических неизменяемых файлов:

```
location /images/ {
    root                /data/www;
    error_page          404 = /fetch$uri;
}

location /fetch/ {
    internal;

    uwsgi_pass          backend:9000;
    ...

    uwsgi_store         on;
    uwsgi_store_access  user:rw group:rw all:r;
    uwsgi_temp_path     /data/temp;

    alias               /data/www/;
}
```

uwsgi_store_access

Синтаксис	`uwsgi_store_access` *пользователи:права* ...;
По умолчанию	`uwsgi_store_access user:rw;`
Контекст	http, server, location

Задает права доступа для создаваемых файлов и каталогов, например,

```
uwsgi_store_access user:rw group:rw all:r;
```

Если заданы какие-либо права для *group* или *all*, то права для user указывать необязательно:

```
uwsgi_store_access group:rw all:r;
```

uwsgi_temp_file_write_size

Синтаксис	`uwsgi_temp_file_write_size` *размер*;
По умолчанию	`uwsgi_temp_file_write_size 8k|16k;`
Контекст	http, server, location

Ограничивает размер данных, сбрасываемых во временный файл за один раз, при включенной буферизации ответов uwsgi-сервера во временные файлы. По умолчанию размер ограничен двумя буферами, заданными директивами *uwsgi_buffer_size* и *uwsgi_buffers*. Максимальный размер временного файла задается директивой *uwsgi_max_temp_file_size*.

uwsgi_temp_path

Синтаксис	`uwsgi_temp_path` *путь* [*уровень1* [*уровень2* [*уровень3*]]]`;`
По умолчанию	`uwsgi_temp_path uwsgi_temp;`
Контекст	http, server, location

Задает имя каталога для хранения временных файлов с данными, полученными от uwsgi-серверов. В каталоге может использоваться иерархия подкаталогов до трех уровней. Например, при такой конфигурации

```
uwsgi_temp_path /spool/angie/uwsgi_temp 1 2;
```

временный файл будет следующего вида:

```
/spool/angie/uwsgi_temp/7/45/00000123457
```

См. также параметр *use_temp_path* директивы *uwsgi_cache_path*.

HTTP/2

Обеспечивает поддержку HTTP/2.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_v2_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
server {
    listen 443 ssl;

    http2 on;

    ssl_certificate server.crt;
    ssl_certificate_key server.key;
}
```

Важно

Чтобы принимать HTTP/2-соединения по TLS, необходимо наличие поддержки расширения «Application-Layer Protocol Negotiation» (ALPN) протокола TLS, появившейся в OpenSSL версии 1.0.2.

Если директива *ssl_prefer_server_ciphers* установлена в значение «on», *шифры* должны быть настроены таким образом, чтобы соответствовать черному списку RFC 9113, Appendix A а также поддерживаться клиентами.

Директивы

http2

Добавлено в версии 1.2.0.

Синтаксис	`http2` on | off;
По умолчанию	`http2 off;`
Контекст	http, server

Разрешает протокол HTTP/2.

http2_body_preread_size

Синтаксис	`http2_body_preread_size` *размер*;
По умолчанию	—
Контекст	http, server

Задает размер буфера для каждого запроса, в который может сохраняться тело запроса до того, как оно начнет обрабатываться.

http2_chunk_size

Синтаксис	`http2_chunk_size` *размер*;
По умолчанию	`http2_chunk_size 8k;`
Контекст	http, server, location

Задает максимальный размер частей, на которое будет разделяться тело ответа. Слишком маленькое значение может привести к росту накладных расходов. Слишком большое значение может негативно сказаться на приоритизации из-за блокировки очереди.

http2_max_concurrent_pushes

Устарело, начиная с версии 1.2.0.

Синтаксис	`http2_max_concurrent_pushes` *число*;
По умолчанию	`http2_max_concurrent_pushes 10;`
Контекст	http, server

Ограничивает максимальное число параллельных *push*-запросов в соединении.

http2_max_concurrent_streams

Синтаксис	`http2_max_concurrent_streams` *число*;
По умолчанию	`http2_max_concurrent_streams 128;`
Контекст	http, server

Задает максимальное число параллельных HTTP/2-потоков в соединении.

http2_push

Устарело, начиная с версии 1.2.0.

Синтаксис	`http2_push` *uri* | off;
По умолчанию	`http2_push off;`
Контекст	http, server, location

Заблаговременно отправляет (push) запрос к заданному uri вместе с ответом на оригинальный запрос. Будут обработаны только относительные URI с абсолютными путями, например:

```
http2_push /static/css/main.css;
```

В значении `uri` допустимо использование переменных.

На одном уровне конфигурации можно указать несколько *http2_push* директив. Параметр `off` отменяет действие унаследованных с предыдущего уровня конфигурации директив *http2_push*.

http2_push_preload

Устарело, начиная с версии 1.2.0.

Синтаксис	`http2_push_preload` on | off;
По умолчанию	`http2_push_preload off;`
Контекст	http, server, location

Разрешает автоматическое преобразование preload links, указанных в полях «Link» заголовка ответа, в push-запросы.

http2_recv_buffer_size

Синтаксис	`http2_recv_buffer_size` *размер*;
По умолчанию	`http2_recv_buffer_size 256k;`
Контекст	http

Задает размер входного буфера для *рабочего процесса*.

Встроенные переменные

Модуль *http_v2* поддерживает следующие встроенные переменные:

`$http2`

согласованный идентификатор протокола:

`h2`	для HTTP/2 через TLS
`h2c`	для HTTP/2 через незашифрованный TCP
`""`	пустая строка для остальных случаев

HTTP/3

Обеспечивает поддержку протокола HTTP/3 для соединений с клиентами, а также для соединений с проксируемыми серверами, настраиваемых при помощи следующих директив из модуля *Proxy*:

- *proxy_http3_hq*
- *proxy_http3_max_concurrent_streams*
- *proxy_http3_stream_buffer_size*
- *proxy_http_version*
- *proxy_pass*
- *proxy_quic_active_connection_id_limit*
- *proxy_quic_gso*
- *proxy_quic_host_key*

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_v3_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
http {
    log_format quic '$remote_addr - $remote_user [$time_local] '
                    '"$request" $status $body_bytes_sent '
                    '"$http_referer" "$http_user_agent" "$http3"';

    access_log logs/access.log quic;

    server {
        # для лучшей совместимости рекомендуется
        # использовать одинаковый порт для http/3 и https
        listen 8443 quic reuseport;
        listen 8443 ssl;

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

        location / {
            # используется для объявления о поддержке http/3
            add_header Alt-Svc 'h3=":8443"; ma=86400';
```

```
        }
    }
}
```

Важно

Чтобы принимать HTTP/3-соединения по TLS, необходимо наличие поддержки протокола TLSv1.3, появившейся в OpenSSL версии 1.1.1.

Директивы

http3

Синтаксис	`http3` on | off;
По умолчанию	`http3 on;`
Контекст	http, server

Разрешает согласование протокола HTTP/3.

http3_hq

Синтаксис	`http3_hq` on | off;
По умолчанию	`http3_hq off;`
Контекст	http, server

Разрешает согласование протокола HTTP/0.9, используемого в функциональных тестах QUIC.

http3_max_concurrent_streams

Синтаксис	`http3_max_concurrent_streams` *число*;
По умолчанию	`http3_max_concurrent_streams 128;`
Контекст	http, server

Задает максимальное число параллельных HTTP/3-потоков в соединении.

http3_stream_buffer_size

Синтаксис	`http3_stream_buffer_size` *размер*;
По умолчанию	`http3_stream_buffer_size 64k;`
Контекст	http, server

Задает *размер* буфера, используемого для чтения и записи QUIC-потоков.

quic_active_connection_id_limit

Синтаксис	`quic_active_connection_id_limit` *число*;
По умолчанию	`quic_active_connection_id_limit 2;`
Контекст	http, server

Устанавливает значение транспортного параметра QUIC *active_connection_id_limit*. Это максимальное значение ID соединений, возможное для хранения на сервере.

quic_bpf

Синтаксис	`quic_bpf` on | off;
По умолчанию	`quic_bpf off;`
Контекст	main

Разрешает маршрутизацию пакетов QUIC при помощи eBPF. Если маршрутизация включена, то обеспечивается поддержка миграции QUIC-соединений.

Важно

Директива поддерживается только на Linux 5.7+.

quic_gso

Синтаксис	`quic_gso` on | off;
По умолчанию	`quic_gso off;`
Контекст	http, server

Разрешает отправку оптимизированного пакетного режима при помощи segmentation offloading.

Важно

Оптимизированная отправка поддерживается только на Linux с поддержкой *UDP_SEGMENT*.

quic_host_key

Синтаксис	`quic_host_key` *файл*;
По умолчанию	—
Контекст	http, server

Задает *файл* с секретным ключом, применяемым при шифровании stateless reset и address validation токенов. По умолчанию создается случайный ключ при каждой перезагрузке. Токены, созданные при помощи старых ключей, не принимаются.

quic_retry

Синтаксис	`quic_retry` on | off;
По умолчанию	`quic_retry off;`
Контекст	http, server

Разрешает функциональность QUIC Address Validation, в том числе отправку нового токена в *Retry*-пакете или *NEW_TOKEN* frame и валидацию токена, полученного в *Initial*-пакете.

Встроенные переменные

Модуль *http_v3* поддерживает следующие встроенные переменные:

`$http3`

согласованный идентификатор протокола:

`h3`	для HTTP/3-соединений
`hq`	для hq-соединений
`""`	пустая строка для остальных случаев

`$quic_connection`

порядковый номер QUIC-соединения

XSLT

Фильтр, преобразующий XML-ответ с помощью одного или нескольких XSLT-шаблонов.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-http_xslt_module`.

В наших репозиториях модуль собран динамически и доступен отдельным пакетом *angie-pro-module-xslt*.

Важно

Для этого модуля нужны библиотеки libxml2 и libxslt.

Пример конфигурации

```
location / {
    xml_entities    /site/dtd/entities.dtd;
    xslt_stylesheet /site/xslt/one.xslt param=value;
    xslt_stylesheet /site/xslt/two.xslt;
}
```

Директивы

xml_entities

Синтаксис	`xml_entities` *путь*;
По умолчанию	—
Контекст	http, server, location

Задает файл DTD, в котором описаны символьные сущности. Этот файл компилируется на стадии конфигурации. По техническим причинам модуль не имеет возможности использовать внешнее подмножество, заданное в обрабатываемом XML, поэтому оно игнорируется, а вместо него используется специально заданный файл. В этом файле не нужно описывать структуру XML, достаточно только объявления необходимых символьных сущностей, например:

```
<!ENTITY nbsp " ">
```

xslt_last_modified

Синтаксис	`xslt_last_modified` on | off;
По умолчанию	`xslt_last_modified off;`
Контекст	http, server, location

Позволяет сохранить поле заголовка «Last-Modified» исходного ответа во время XSLT-преобразований для лучшего кэширования ответов.

По умолчанию поле заголовка удаляется, так как содержимое ответа изменяется во время преобразования и может содержать динамически созданные элементы или части, которые изменились независимо от исходного ответа.

xslt_param

Синтаксис	`xslt_param` *параметр значение*;
По умолчанию	—
Контекст	http, server, location

Задает параметры для XSLT-шаблонов. Значение рассматривается как выражение XPath. В значении можно использовать переменные. Если нужно передать в шаблон строковое значение, можно воспользоваться директивой *xslt_string_param*.

Директив *xslt_param* может быть несколько. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *xslt_param* и *xslt_string_param*.

xslt_string_param

Синтаксис	`xslt_string_param` *параметр значение*;
По умолчанию	—
Контекст	http, server, location

Задает строковые параметры для XSLT-шаблонов. Выражения XPath в значении параметра не интерпретируются. В значении можно использовать переменные.

Директив *xslt_string_param* может быть несколько. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *xslt_param* и *xslt_string_param*.

xslt_stylesheet

Синтаксис	`xslt_stylesheet` *шаблон* [*параметр*=*значение* ...];
По умолчанию	—
Контекст	location

Задает XSLT-шаблон и необязательные параметры для этого шаблона. Шаблон компилируется на стадии конфигурации.

Параметры можно задавать как по отдельности, так и группировать в одной строке, разделяя символом «:». Если же в самих параметрах встречается символ «:», то его нужно экранировать в виде «*%3A*». Кроме того, libxslt требует, чтобы параметры, содержащие не только алфавитно-цифровые символы, были заключены в одинарные или двойные кавычки, например:

```
param1='http%3A//www.example.com':param2=value2
```

В описании параметров можно использовать переменные, например, целая строка параметров может быть взята из одной переменной:

```
location / {
    xslt_stylesheet /site/xslt/one.xslt
                    $arg_xslt_params
                    param1='$value1':param2=value2
```

```
                    param3=value3;
}
```

Можно указать несколько шаблонов — в этом случае они будут применяться последовательно в порядке их описания.

xslt_types

Синтаксис	`xslt_types` mime-*тип* ...;
По умолчанию	`xslt_types text/xml;`
Контекст	http, server, location

Разрешает преобразования в ответах с указанными MIME-типами в дополнение к «*text/xml*». Специальное значение * соответствует любому MIME-типу. Если в результате преобразования выдается HTML-ответ, то его MIME-тип меняется на «*text/html*».

Базовый HTTP-модуль реализует основную функциональность HTTP-сервера: это определение серверных блоков, настройка локаций для маршрутизации запросов, передача статических файлов и контроль доступа, настройка редиректов, поддержка соединений *keep-alive* и управление заголовками запросов и ответов.

Остальные модули этого раздела расширяют эту функциональность, позволяя гибко настраивать и оптимизировать работу HTTP-сервера под различные сценарии и требования.

Директивы

absolute_redirect

Синтаксис	`absolute_redirect` on | off;
По умолчанию	`absolute_redirect on;`
Контекст	http, server, location

Если запрещено, то перенаправления, выдаваемые Angie PRO, будут относительными.

См. также директивы *server_name_in_redirect* и *port_in_redirect*.

aio

Синтаксис	`aio` on | off | threads[=*pool*];
По умолчанию	`aio off;`
Контекст	http, server, location

Разрешает или запрещает использование файлового асинхронного ввода-вывода (AIO) во FreeBSD и Linux:

```
location /video/ {
  aio            on;
  output_buffers 1 64k;
}
```

Во FreeBSD AIO можно использовать, начиная с FreeBSD 4.3. До FreeBSD 11.0 AIO можно либо собрать в ядре статически:

```
options VFS_AIO
```

либо загрузить динамически через загружаемый модуль ядра:

```
kldload aio
```

В Linux AIO можно использовать только начиная с версии ядра 2.6.22. Кроме того, необходимо также дополнительно включить *directio*, иначе чтение будет блокирующимся:

```
location /video/ {
  aio            on;
  directio       512;
  output_buffers 1 128k;
}
```

В Linux *directio* можно использовать только для чтения блоков, выравненных на границу 512 байт (или 4K для XFS). Невыравненный конец файла будет читаться блокированно. То же относится к запросам с указанием диапазона запрашиваемых байт (byte-range requests) и к запросам FLV не с начала файла: чтение невыравненных начала и конца ответа будет блокирующимся.

При одновременном включении AIO и *sendfile* в Linux для файлов, размер которых больше либо равен указанному в директиве *directio*, будет использоваться AIO, а для файлов меньшего размера или при выключенном *directio* — *sendfile*:

```
location /video/ {
  sendfile       on;
  aio            on;
  directio       8m;
}
```

Кроме того, читать и *отправлять* файлы можно в многопоточном режиме, не блокируя при этом рабочий процесс:

```
location /video/ {
  sendfile       on;
  aio            threads;
}
```

Операции чтения или отправки файлов будут обрабатываться потоками из указанного *пула*. Если пул потоков не задан явно, используется пул с именем *default*. Имя пула может быть задано при помощи переменных:

```
aio threads=pool$disk;
```

По умолчанию поддержка многопоточности выключена, ее сборку следует разрешить с помощью конфигурационного параметра *–with-threads*. В настоящий момент многопоточность совместима только с методами *epoll*, *kqueue* и *eventport*. Отправка файлов в многопоточном режиме поддерживается только на Linux.

См. также директиву *sendfile*.

aio_write

Синтаксис	`aio_write` on | off;
По умолчанию	`aio_write off;`
Контекст	http, server, location

При включенном *aio* разрешает его использование для записи файлов. В настоящий момент это работает только при использовании *aio threads* и ограничено записью временных файлов с данными, полученными от проксируемых серверов.

alias

Синтаксис	`alias` *путь*;
По умолчанию	—
Контекст	location

Задает замену для указанного *location*'а. Например, при такой конфигурации:

```
location /i/ {
  alias /data/w3/images/;
}
```

на запрос `/i/top.gif` будет отдан файл */data/w3/images/top.gif*.

В значении параметра *путь* можно использовать переменные, кроме *$document_root* и *$realpath_root*.

Если *alias* используется внутри *location*'а, заданного регулярным выражением, то регулярное выражение должно содержать выделения, а сам *alias* — ссылки на эти выделения, например:

```
location ~ ^/users/(.+\.(?:gif|jpe?g|png))$ {
  alias /data/w3/images/$1;
}
```

Если *location* и последняя часть значения директивы совпадают:

```
location /images/ {
  alias /data/w3/images/;
}
```

то лучше воспользоваться директивой *root*:

```
location /images/ {
  root /data/w3;
}
```

auth_delay

Синтаксис	`auth_delay` *время*;
По умолчанию	`auth_delay 0s;`
Контекст	http, server, location

Задерживает обработку неавторизованных запросов с кодом ответа 401 для предотвращения атак по времени в случае ограничения доступа по *паролю* или по *результату подзапроса*.

auto_redirect

Синтаксис	`auto_redirect` [on | off | default];
По умолчанию	`auto_redirect default;`
Контекст	http, server, location

Контролирует поведение *перенаправления*, когда префикс `location` заканчивается косой чертой:

```
location /prefix/ {
    auto_redirect on;
}
```

Здесь запрос к `/prefix` будет перенаправлен на `/prefix/`.

Установка значений `on` и `off` отключает и включает перенаправление в явном виде. Если указано `default`, перенаправление включается, только если `location` обрабатывает запросы через *api*, *proxy_pass*, *fastcgi_pass*, *uwsgi_pass*, *scgi_pass*, *memcached_pass*, или *grpc_pass*.

chunked_transfer_encoding

Синтаксис	`chunked_transfer_encoding` on | off;
По умолчанию	`chunked_transfer_encoding on;`
Контекст	http, server, location

Позволяет запретить формат передачи данных частями (chunked transfer encoding) в HTTP/1.1. Это может понадобиться при использовании программ, не поддерживающих chunked encoding, несмотря на требования стандарта.

client_body_buffer_size

Синтаксис	`client_body_buffer_size` *размер*;
По умолчанию	`client_body_buffer_size 8k|16k;`
Контекст	http, server, location

Задает размер буфера для чтения тела запроса клиента. Если тело запроса больше заданного буфера, то все тело запроса или только его часть записывается *во временный файл*. По умолчанию

размер одного буфера равен двум размерам страницы. На *x86*, других 32-битных платформах и *x86-64* это 8K. На других 64-битных платформах это обычно 16K.

client_body_in_file_only

Синтаксис	`client_body_in_file_only` on | clean | off;
По умолчанию	`client_body_in_file_only off;`
Контекст	http, server, location

Определяет, сохранять ли все тело запроса клиента в файл. Директиву можно использовать для отладки и при использовании переменной *$request_body_file* или метода *$r->request_body_file* модуля *Perl*.

`on`	временные файлы по окончании обработки запроса не удаляются
`clean`	разрешает удалять временные файлы, оставшиеся по окончании обработки запроса

client_body_in_single_buffer

Синтаксис	`client_body_in_single_buffer` on | off;
По умолчанию	`client_body_in_single_buffer off;`
Контекст	http, server, location

Определяет, сохранять ли все тело запроса клиента в одном буфере. Директива рекомендуется при использовании переменной *$request_body* для уменьшения требуемого числа операций копирования.

client_body_temp_path

Синтаксис	`client_body_temp_path` *путь* [*уровень1* [*уровень2* [*уровень3*]]];
По умолчанию	`client_body_temp_path client_body_temp;`
Контекст	http, server, location

Задает каталог для хранения временных файлов с телами запросов клиентов. В каталоге может использоваться иерархия подкаталогов до трех уровней. Например, при такой конфигурации

```
client_body_temp_path /spool/angie/client_temp 1 2;
```

путь к временному файлу будет следующего вида:

```
/spool/angie/client_temp/7/45/00000123457
```

client_body_timeout

Синтаксис	`client_body_timeout` *время;*
По умолчанию	`client_body_timeout 60s;`
Контекст	http, server, location

Задает таймаут при чтении тела запроса клиента. Таймаут устанавливается не на всю передачу тела запроса, а только между двумя последовательными операциями чтения. Если по истечении этого времени клиент ничего не передаст, обработка запроса прекращается с ошибкой 408 (Request Time-out).

client_header_buffer_size

Синтаксис	`client_header_buffer_size` *размер*;
По умолчанию	`client_header_buffer_size 1k;`
Контекст	http, server

Задает размер буфера для чтения заголовка запроса клиента. Для большинства запросов достаточно буфера размером в 1K байт. Однако если в запросе есть длинные cookies, или же запрос пришел от WAP-клиента, то он может не поместиться в 1K. Поэтому, если строка запроса или поле заголовка запроса не помещаются полностью в этот буфер, то выделяются буферы большего размера, задаваемые директивой *large_client_header_buffers*.

Если директива указана на уровне *server*, то может использоваться значение из сервера по умолчанию. Подробнее см. в разделе *Выбор виртуального сервера*.

client_header_timeout

Синтаксис	`client_header_timeout` *время;*
По умолчанию	`client_header_timeout 60s;`
Контекст	http, server

Задает таймаут при чтении заголовка запроса клиента. Если по истечении этого времени клиент не передаст полностью заголовок, обработка запроса прекращается с ошибкой 408 (Request Time-out).

client_max_body_size

Синтаксис	`client_max_body_size` *размер*;
По умолчанию	`client_max_body_size 1m;`
Контекст	http, server, location

Задает максимально допустимый размер тела запроса клиента. Если размер больше заданного, то клиенту возвращается ошибка 413 (Request Entity Too Large). Следует иметь в виду, что браузеры не умеют корректно показывать эту ошибку.

0	отключает проверку размера тела запроса клиента

connection_pool_size

Синтаксис	`connection_pool_size` *размер*;
По умолчанию	`connection_pool_size 256 | 512;`
Контекст	http, server, location

Позволяет производить точную настройку выделения памяти под конкретные соединения. Эта директива не оказывает существенного влияния на производительность, и ее не следует использовать. По умолчанию:

`256 байт`	на 32-битных платформах
`512 байт`	на 64-битных платформах

default_type

Синтаксис	`default_type` mime-*тип*;
По умолчанию	`default_type text/plain;`
Контекст	http, server, location

Задает MIME-тип ответов по умолчанию. Соответствие расширений имен файлов MIME-типу ответов задается с помощью директивы *types*.

directio

Синтаксис	`directio` *размер* | off;
По умолчанию	`directio off;`
Контекст	http, server, location

Разрешает использовать флаги *O_DIRECT* (FreeBSD, Linux), *F_NOCACHE* (macOS) или функцию *directio()* (Solaris) при чтении файлов, размер которых больше либо равен указанному. Директива автоматически запрещает использование *sendfile* для данного запроса. Рекомендуется использовать для больших файлов:

```
directio 4m;
```

или при использовании *aio* в Linux.

directio_alignment

Синтаксис	`directio_alignment` *размер*;
По умолчанию	`directio_alignment 512;`
Контекст	http, server, location

Устанавливает выравнивание для *directio*. В большинстве случаев достаточно 512-байтового выравнивания, однако при использовании XFS под Linux его нужно увеличить до 4K.

disable_symlinks

Синтаксис	`disable_symlinks` off; `disable_symlinks` on | if_not_owner [from=*часть*];
По умолчанию	`disable_symlinks off;`
Контекст	http, server, location

Определяет, как следует поступать с символическими ссылками при открытии файлов:

`off`	Символические ссылки в пути допускаются и не проверяются. Это стандартное поведение.
`on`	Если любой компонент пути является символической ссылкой, доступ к файлу запрещается.
`if_not_owner`	Доступ к файлу запрещается, если любой компонент пути является символической ссылкой, а ссылка и объект, на который она ссылается, имеют разных владельцев.
`from=`*часть*	При проверке символических ссылок (параметры *on* и *if_not_owner*) обычно проверяются все компоненты пути. Можно не проверять символические ссылки в начальной части пути, указав дополнительно параметр *from=часть*. В этом случае символические ссылки проверяются лишь начиная с компонента пути, который следует за заданной начальной частью. Если значение не является начальной частью проверяемого пути, путь проверяется целиком, как если бы этот параметр не был указан вовсе. Если значение целиком совпадает с именем файла, символические ссылки не проверяются. В значении параметра можно использовать переменные.

Пример:

```
disable_symlinks on from=$document_root;
```

Эта директива доступна только на системах, в которых есть интерфейсы *openat()* и *fstatat()*. К таким системам относятся современные версии FreeBSD, Linux и Solaris.

Предупреждение

Параметры *on* и *if_not_owner* требуют дополнительных затрат на обработку.

На системах, не поддерживающих операцию открытия каталогов только для поиска, для использования этих параметров требуется, чтобы рабочие процессы имели право читать все проверяемые каталоги.

Примечание

Модули *AutoIndex*, *Random Index* и *DAV* в настоящий момент игнорируют эту директиву.

error_page

Синтаксис	`error_page` *код* ... [=[*ответ*]] uri;
По умолчанию	—
Контекст	http, server, location, if в location

Задает URI, который будет показываться для указанных ошибок. В значении *uri* можно использовать переменные.

Пример:

```
error_page 404             /404.html;
error_page 500 502 503 504 /50x.html;
```

При этом делается внутреннее перенаправление на указанный *uri*, а метод запроса клиента меняется на «GET» (для всех методов, отличных от «GET» и «HEAD»).

Кроме того, можно поменять код ответа на другой, используя синтаксис вида *=ответ*, например:

```
error_page 404 =200 /empty.gif;
```

Если ошибочный ответ обрабатывается проксированным сервером или FastCGI/uwsgi/SCGI/gRPC-сервером, и этот сервер может вернуть разные коды ответов, например, 200, 302, 401 или 404, то можно выдавать возвращаемый им код:

```
error_page 404 = /404.php;
```

Если при внутреннем перенаправлении не нужно менять URI и метод, то можно передать обработку ошибки в именованный *location*:

```
location / {
  error_page 404 = @fallback;
}

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

Примечание

Если при обработке uri происходит ошибка, клиенту возвращается ответ с кодом последней случившейся ошибки.

Также существует возможность использовать перенаправления URL для обработки ошибок:

```
error_page 403      http://example.com/forbidden.html;
error_page 404 =301 http://example.com/notfound.html;
```

В этом случае по умолчанию клиенту возвращается код ответа 302. Его можно изменить только на один из кодов ответа, относящихся к перенаправлениям (301, 302, 303, 307 и 308).

etag

Синтаксис	`etag` on | off;
По умолчанию	`etag on;`
Контекст	http, server, location

Разрешает или запрещает автоматическую генерацию поля «ETag» заголовка ответа для статических ресурсов.

http

Синтаксис	`http` { ... }
По умолчанию	—
Контекст	main

Предоставляет контекст конфигурационного файла, в котором указываются директивы HTTP-сервера.

if_modified_since

Синтаксис	`if_modified_since` off | exact | before;
По умолчанию	`if_modified_since exact;`
Контекст	http, server, location

Определяет, как сравнивать время модификации ответа с временем в поле «If-Modified-Since» заголовка запроса:

`off`	ответ всегда считается изменившимся
`exact`	точное совпадение
`before`	время модификации ответа меньше или равно времени, заданному в поле «If-Modified-Since» заголовка запроса

ignore_invalid_headers

Синтаксис	`ignore_invalid_headers` on | off;
По умолчанию	`ignore_invalid_headers on;`
Контекст	http, server

Если включено, Angie PRO игнорирует поля заголовка с недопустимыми именами. Допустимыми считаются имена, состоящие из английских букв, цифр, дефисов и возможно знаков подчеркивания (последнее контролируется директивой *underscores_in_headers*).

Если директива указана на уровне *server*, то может использоваться значение из сервера по умолчанию.

internal

Синтаксис	`internal;`
По умолчанию	—
Контекст	location

Указывает, что *location* может использоваться только для внутренних запросов. Для внешних запросов клиенту будет возвращаться ошибка 404 (Not Found). Внутренними запросами являются:

- запросы, перенаправленные директивами *error_page*, *index*, *random_index* и *try_files*;
- запросы, перенаправленные с помощью поля «X-Accel-Redirect» заголовка ответа вышестоящего сервера;
- подзапросы, формируемые командой *include virtual* модуля *SSI*, директивами модуля *Addition*, а также директивами *auth_request* и *mirror*;
- запросы, измененные директивой *rewrite*.

Пример:

```
error_page 404 /404.html;

location = /404.html {
  internal;
}
```

Примечание

Для предотвращения зацикливания, которое может возникнуть при использовании некорректных конфигураций, количество внутренних перенаправлений ограничено десятью. По достижении этого ограничения будет возвращена ошибка 500 (Internal Server Error). В таком случае в лог-файле ошибок можно увидеть сообщение *rewrite or internal redirection cycle*.

keepalive_disable

Синтаксис	`keepalive_disable` none | *браузер* ...;
По умолчанию	`keepalive_disable msie6;`
Контекст	http, server, location

Запрещает соединения *keep-alive* с некорректно ведущими себя браузерами. Параметры *браузер* указывают, на какие браузеры это распространяется.

`none`	разрешает соединения *keep-alive* со всеми браузерами
`msie6`	запрещает соединения *keep-alive* со старыми версиями MSIE после получения запроса POST
`safari`	запрещает соединения *keep-alive* с Safari и подобными им браузерами на macOS и подобных ей ОС

keepalive_requests

Синтаксис	`keepalive_requests` *число;*
По умолчанию	`keepalive_requests 1000;`
Контекст	http, server, location

Задает максимальное число запросов, которые можно сделать по одному *keep-alive* соединению. После того, как сделано максимальное число запросов, соединение закрывается.

Периодическое закрытие соединений необходимо для освобождения памяти, выделенной под конкретные соединения. Поэтому использование слишком большого максимального числа запросов может приводить к чрезмерному потреблению памяти и не рекомендуется.

keepalive_time

Синтаксис	`keepalive_time` *время;*
По умолчанию	`keepalive_time 1h;`
Контекст	http, server, location

Ограничивает максимальное время, в течение которого могут обрабатываться запросы в рамках соединения *keep-alive*. По достижении заданного времени соединение закрывается после обработки очередного запроса.

keepalive_timeout

Синтаксис	`keepalive_timeout` *таймаут* [*заголовок_таймаута*];
По умолчанию	`keepalive_timeout 75s;`
Контекст	http, server, location

`таймаут`	задает время, в течение которого *keep-alive* соединение с клиентом не будет закрыто со стороны сервера
`0`	запрещает keep-alive соединения с клиентами

Второй, *необязательный*, параметр задает значение в поле «Keep-Alive: timeout=время» заголовка ответа. Два параметра могут отличаться друг от друга.

Поле «Keep-Alive: timeout=время» заголовка понимают Mozilla и Konqueror. MSIE сам закрывает keep-alive соединение примерно через 60 секунд.

large_client_header_buffers

Синтаксис	`large_client_header_buffers` *количество размер*;
По умолчанию	`large_client_header_buffers 4 8k;`
Контекст	http, server

Задает максимальное число и размер буферов для чтения большого заголовка запроса клиента. Строка запроса не должна превышать размера одного буфера, иначе клиенту возвращается ошибка 414 (Request-URI Too Large). Поле заголовка запроса также не должно превышать размера одного буфера, иначе клиенту возвращается ошибка 400 (Bad Request). Буферы выделяются только по мере необходимости. По умолчанию размер одного буфера равен 8K байт. Если по окончании обработки запроса соединение переходит в состояние *keep-alive*, эти буферы освобождаются.

Если директива указана на уровне *server*, то может использоваться значение из сервера по умолчанию.

limit_except

Синтаксис	`limit_except` *метод1* [*метод2*...] { ... };
По умолчанию	—
Контекст	location

Ограничивает HTTP-методы, доступные внутри location. Параметр метод может быть одним из *GET*, *HEAD*, *POST*, *PUT*, *DELETE*, *MKCOL*, *COPY*, *MOVE*, *OPTIONS*, *PROPFIND*, *PROPPATCH*, *LOCK*, *UNLOCK* или *PATCH*. Если разрешен метод *GET*, то метод *HEAD* также будет разрешен. Доступ к остальным методам может быть ограничен при помощи директив модулей *Access* и *Auth Basic*.

```
limit_except GET {
  allow 192.168.1.0/32;
  deny  all;
}
```

Примечание

Ограничение в примере действует для всех методов, **кроме** *GET* и *HEAD*.

limit_rate

Синтаксис	`limit_rate` *скорость;*
По умолчанию	`limit_rate 0;`
Контекст	http, server, location, if в location

Ограничивает скорость передачи ответа клиенту. Скорость задается в байтах в секунду. Значение *0* отключает ограничение скорости. Ограничение устанавливается на запрос, поэтому, если клиент одновременно откроет два соединения, суммарная скорость будет вдвое выше заданного ограничения.

В значении параметра можно использовать переменные. Это может быть полезно в случаях, когда скорость нужно ограничивать в зависимости от какого-либо условия:

```
map $slow $rate {
  1     4k;
  2     8k;
}

limit_rate $rate;
```

Ограничение скорости можно также задать в переменной *$limit_rate*, однако использовать данный метод не рекомендуется:

```
server {

  if ($slow) {
    set $limit_rate 4k;
  }

}
```

Кроме того, ограничение скорости может быть задано в поле «X-Accel-Limit-Rate» заголовка ответа проксированного сервера. Эту возможность можно запретить с помощью директив *proxy_ignore_headers*, *fastcgi_ignore_headers*, *uwsgi_ignore_headers* и *scgi_ignore_headers*.

limit_rate_after

Синтаксис	`limit_rate_after` *размер*;
По умолчанию	`limit_rate_after 0;`
Контекст	http, server, location, if в location

Задает начальный объем данных, после передачи которого начинает ограничиваться скорость передачи ответа клиенту. В значении параметра можно использовать переменные.

Пример:

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

lingering_close

Синтаксис	`lingering_close` on | always | off;
По умолчанию	`lingering_close on;`
Контекст	http, server, location

Управляет закрытием соединений с клиентами.

`on`	Angie PRO будет *ждать* и *обрабатывать* дополнительные данные, поступающие от клиента, перед полным закрытием соединения, но только если эвристика указывает на то, что клиент может еще послать данные.
`always`	Angie PRO всегда будет ждать и обрабатывать дополнительные данные, поступающие от клиента.
`off`	Angie PRO не будет ждать поступления дополнительных данных и сразу же закроет соединение. Это поведение нарушает протокол и поэтому не должно использоваться без необходимости.

Для управления закрытием HTTP/2-соединений директива должна быть задана на уровне *server*.

lingering_time

Синтаксис	`lingering_time` *время;*
По умолчанию	`lingering_time 30s;`
Контекст	http, server, location

Если действует *lingering_close*, эта директива задает максимальное время, в течение которого Angie PRO будет обрабатывать (читать и игнорировать) дополнительные данные, поступающие от клиента. По прошествии этого времени соединение будет закрыто, даже если будут еще данные.

lingering_timeout

Синтаксис	`lingering_timeout` *время;*
По умолчанию	`lingering_timeout 5s;`
Контекст	http, server, location

Если действует *lingering_close*, эта директива задает максимальное время ожидания поступления дополнительных данных от клиента. Если в течение этого времени данные не были получены, соединение закрывается. В противном случае данные читаются и игнорируются, и Angie PRO снова ждет поступления данных. Цикл «ждать-читать-игнорировать» повторяется, но не дольше чем задано директивой *lingering_time*.

listen

Синтаксис	`listen` *адрес*[:*порт*] [default_server] [ssl] [http2 | quic] [proxy_protocol] [setfib=*число*] [fastopen=*число*] [backlog=*число*] [rcvbuf=*размер*] [sndbuf=*размер*] [accept_filter=*фильтр*] [deferred] [bind] [ipv6only=on|off] [reuseport] [so_keepalive=on|off|[keepidle]:[keepintvl]:[keepcnt]]; `listen` *порт* [default_server] [ssl] [http2 | quic] [proxy_protocol] [setfib=*число*] [fastopen=*число*] [backlog=*число*] [rcvbuf=*размер*] [sndbuf=*размер*] [accept_filter=*фильтр*] [deferred] [bind] [ipv6only=on|off] [reuseport] [so_keepalive=on|off|[keepidle]:[keepintvl]:[keepcnt]]; `listen` unix:*путь* [default_server] [ssl] [http2 | quic] [proxy_protocol] [backlog=*число*] [rcvbuf=*размер*] [sndbuf=*размер*] [accept_filter=*фильтр*] [deferred] [bind] [so_keepalive=on|off|[keepidle]:[keepintvl]:[keepcnt]];
По умолчанию	`listen *:80 | *:8000;`
Контекст	server

Задает *адрес* и *порт* для слушающего сокета или путь для UNIX-сокета, на которых сервер будет принимать запросы. Можно указать *адрес* и *порт*, либо только *адрес* или только *порт*. Кроме того, *адрес* может быть именем хоста, например:

```
listen 127.0.0.1:8000;
listen 127.0.0.1;
listen 8000;
listen *:8000;
listen localhost:8000;
```

IPv6-адреса задаются в квадратных скобках:

```
listen [::]:8000;
listen [::1];
```

UNIX-сокеты задаются при помощи префикса `unix:`:

```
listen unix:/var/run/angie.sock;
```

Если указан только *адрес*, то используется порт *80*.

Если директива не указана, то используется либо **:80*, если Angie PRO работает с привилегиями суперпользователя, либо **:8000*.

`default_server`	сервер, в котором указан этот параметр, будет сервером по умолчанию для указанной пары *адрес:порт* (*слушающий сокет*). Если же директив с параметром *default_server* нет, сервером по умолчанию для слущающего сокета будет первый встречающийся в конфигурации сервер, в котором описан этот слушающий сокет.
`ssl`	указывает на то, что все соединения, принимаемые на данном слушающем сокете, должны работать в режиме SSL. Это позволяет задать *компактную конфигурацию* для сервера, работающего сразу в двух режимах — HTTP и HTTPS.
`http2`	позволяет принимать на слушающем сокете HTTP/2-соединения. Обычно, чтобы это работало, следует также указать параметр *ssl*, однако Angie PRO можно также настроить и на прием HTTP/2-соединений без SSL. Устарело, начиная с версии 1.2.0. Используйте взамен директиву *http2*.
`quic`	позволяет принимать на этом порту QUIC-соединения. Для использования этой опции в Angie PRO должен быть включен и настроен модуль *HTTP3*. Когда `quic` включен, также можно указать `reuseport`, чтобы использовать несколько рабочих процессов.
`proxy_protocol`	указывает на то, что все соединения, принимаемые на данном слушающем сокете, должны использовать протокол PROXY.

В директиве *listen* можно также указать несколько дополнительных параметров, специфичных для связанных с сокетами системных вызовов. Эти параметры можно задать в любой директиве *listen*, но только один раз для слушающего сокета.

`setfib=`*число*	задает таблицу маршрутизации, FIB (параметр *SO_SETFIB*) для слушающего сокета. В настоящий момент это работает только на FreeBSD.
`fastopen=`*число*	включает «TCP Fast Open» для слушающего сокета и ограничивает максимальную длину очереди соединений, которые еще не завершили процесс трехстороннего рукопожатия.

Осторожно

Не включайте «TCP Fast Open», не убедившись, что сервер может адекватно обрабатывать многократное получение одного и того же SYN-пакета с данными.

`backlog=`*число*	задает параметр *backlog* в вызове *listen()*, который ограничивает максимальный размер очереди ожидающих приема соединений. По умолчанию *backlog* устанавливается равным *-1* для FreeBSD, DragonFly BSD и macOS, и *511* для других платформ.
`rcvbuf=`*размер*	задает размер буфера приема (параметр *SO_RCVBUF*) для слушающего сокета.
`sndbuf=`*размер*	задает размер буфера передачи (параметр *SO_SNDBUF*) для слушающего сокета.
`accept_filter=`*фильтр*	задает название accept-фильтра (параметр *SO_ACCEPTFILTER*) для слушающего сокета, который включается для фильтрации входящих соединений перед передачей их в *accept()*. Работает только на FreeBSD и NetBSD 5.0+. Можно использовать два фильтра: *dataready* и *httpready*.
`deferred`	указывает использовать отложенный *accept()* (параметр *TCP_DEFER_ACCEPT* сокета) на Linux.
`bind`	указывает, что для данного слушающего сокета нужно делать *bind()* отдельно. Это нужно потому, что если описаны несколько директив *listen* с одинаковым портом, но разными адресами, и одна из директив *listen* слушает на всех адресах для данного *порта* (**:порт*), то Angie PRO сделает *bind()* только на **:порт*. Необходимо заметить, что в этом случае для определения адреса, на который пришло соединение, делается системный вызов *getsockname()*. Если же используются параметры *setfib*, *fastopen*, *backlog*, *rcvbuf*, *sndbuf*, *accept_filter*, *deferred*, *ipv6only*, *reuseport* или *so_keepalive*, то для данной пары *адрес:порт* всегда делается отдельный вызов *bind()*.
`ipv6only=on` | `off`	определяет (через параметр сокета *IPV6_V6ONLY*), будет ли слушающий на wildcard-адресе [::] IPv6-сокет принимать только IPv6-соединения, или же одновременно IPv6- и IPv4-соединения. По умолчанию параметр включен. Установить его можно только один раз на старте.
`reuseport`	указывает, что нужно создавать отдельный слушающий сокет для каждого рабочего процесса (через параметр сокета *SO_REUSEPORT* для Linux 3.9+ и DragonFly BSD или *SO_REUSEPORT_LB* для FreeBSD 12+), позволяя ядру распределять входящие соединения между рабочими процессами. В настоящий момент это работает только на Linux 3.9+, DragonFly BSD и FreeBSD 12+.

Осторожно

Ненадлежащее использование параметра *reuseport* может быть небезопасно.

`so_keepalive=on` | `off` | `[keepidle]:[keepintvl]:[keepcnt]` конфигурирует для слушающего сокета поведение «TCP keepalive».

`''`	если параметр опущен, для сокета будут действовать настройки операционной системы
`on`	для сокета включается параметр *SO_KEEPALIVE*
`off`	для сокета параметр *SO_KEEPALIVE* выключается

Некоторые операционные системы поддерживают настройку параметров «TCP keepalive» на уровне сокета посредством параметров *TCP_KEEPIDLE*, *TCP_KEEPINTVL* и *TCP_KEEPCNT*. На таких системах их можно сконфигурировать с помощью параметров *keepidle*, *keepintvl* и *keepcnt*. Один или два параметра могут быть опущены, в таком случае для соответствующего параметра сокета будут действовать стандартные системные настройки. Например,

```
so_keepalive=30m::10
```

установит таймаут бездействия (*TCP_KEEPIDLE*) в 30 минут, для интервала проб (*TCP_KEEPINTVL*) будет действовать стандартная системная настройка, а счетчик проб (*TCP_KEEPCNT*) будет равен 10.

Пример:

```
listen 127.0.0.1 default_server accept_filter=dataready backlog=1024;
```

location

Синтаксис	`location` ([= | ~ | ~* | ^~] *uri* | *@имя*)+ { ... }
По умолчанию	—
Контекст	server, location

Устанавливает конфигурацию в зависимости от того, соответствует ли URI запроса какому-либо из выражений сопоставления.

Для сопоставления используется URI запроса в нормализованном виде, после декодирования текста, заданного в виде *%XX*, преобразования относительных элементов пути «.» и «..» в реальные и возможной *замены* двух и более подряд идущих косых черт на одну.

Задать *location* можно префиксной строкой или регулярным выражением.

Регулярные выражения задаются с модификатором:

~*	Для поиска совпадения без учета регистра символов
~	С учетом регистра

Чтобы найти *location*, соответствующий запросу, вначале проверяются *location*'ы, заданные префиксными строками (префиксные *location*'ы). Среди них ищется *location* с совпадающим префиксом максимальной длины и запоминается.

Примечание

Для операционных систем, нечувствительных к регистру символов, таких как macOS, сравнение с префиксными строками производится без учета регистра. Однако сравнение ограничено только однобайтными *locale*'ями.

Затем проверяются регулярные выражения в порядке их следования в конфигурационном файле. Проверка регулярных выражений прекращается после первого же совпадения, и используется соответствующая конфигурация. Если совпадение с регулярным выражением не найдено, то используется конфигурация запомненного ранее префиксного *location*'а.

За некоторыми исключениями, о которых говорится ниже, блоки *location* могут быть вложенными.

Регулярные выражения могут создавать группы захвата, которые затем можно использовать в других директивах.

Если у совпавшего префиксного *location*'а указан модификатор ^~, то регулярные выражения не проверяются.

Кроме того, с помощью модификатора = можно задать точное совпадение URI и *location*. При точном совпадении поиск сразу же прекращается. Например, если запрос / случается часто, можно ускорить обработку таких запросов, указав `location =/`, так как поиск прекратится после первого же сравнения. Такой *location* не может иметь вложенные *location*, так как он задает полное совпадение.

Пример:

```
location =/ {
    #конфигурация А
}

location / {
    #конфигурация Б
}

location /documents/ {
    #конфигурация В
}

location ^~/images/ {
    #конфигурация Г
}

location ~*\.(gif|jpg|jpeg)$ {
    #конфигурация Д
}
```

Для запроса `/` будет выбрана конфигурация А, для запроса `/index.html` — конфигурация Б, для запроса `/documents/document.html` — конфигурация В, для запроса `/images/1.gif` — конфигурация Г, а для запроса `/documents/1.jpg` — конфигурация Д.

Примечание

Если префиксный *location* задан с косой чертой в конце и включена директива *auto_ redirect*, происходит следующее: На запрос с URI без косой черты в конце, в остальном совпадающий с префиксом, будет возвращено постоянное перенаправление с кодом 301, указывающее на URI запроса с добавленной в конце косой чертой.

Если задать `location` с точным совпадением URI, перенаправление не используется:

```
location /user/ {
  proxy_pass http://user.example.com;
}

location =/user {
  proxy_pass http://login.example.com;
}
```

Префикс @ задает *именованный location*. Такой *location* не используется при обычной обработке запросов, а предназначен только для перенаправления в него запросов. Такие *location* не могут быть вложенными и не могут содержать вложенные *location*.

Комбинированные *location*

Для удобства несколько *location* с одинаковой конфигурацией можно записать компактно, перечислив в одном *location* сразу несколько выражений сопоставления и задав для них единую конфигурацию. Такие *location* называются *комбинированными*.

Если, например, предположить, что в предыдущем примере конфигурации А, Г и Д совпадают, то их можно записать с помощью комбинированного *location*:

```
location =/
         ~~/images/
         ~*\.(gif|jpg|jpeg)$ {
   #общая конфигурация
}
```

Именованный *location* также может быть частью комбинированного:

```
location =/
         @named_combined {
   #...
}
```

Осторожно

В комбинированных *location* между модификатором выражения сопоставления и самим выражением не может стоять пробел. Правильно: `location ~*/match(ing|es|er)$ ....`

Примечание

Сейчас комбинированные *location* не могут **непосредственно** содержать директивы *proxy_pass*, в которых задан URI, а также *api* и *alias*. При этом такие директивы можно использовать в других *location*, вложенных в комбинированный.

log_not_found

Синтаксис	`log_not_found` on | off;
По умолчанию	`log_not_found on;`
Контекст	http, server, location

Разрешает или запрещает записывать в *error_log* ошибки о том, что файл не найден.

log_subrequest

Синтаксис	`log_subrequest` on | off;
По умолчанию	`log_subrequest off;`
Контекст	http, server, location

Разрешает или запрещает записывать в *access_log* подзапросы.

max_ranges

Синтаксис	`max_ranges` *число*
По умолчанию	—
Контекст	http, server, location

Ограничивает максимальное допустимое число диапазонов в запросах с указанием диапазона запрашиваемых байт (byte-range requests). Запросы, превышающие указанное ограничение, обрабатываются как если бы они не содержали указания диапазонов. По умолчанию число диапазонов не ограничено.

`0`	полностью запрещает поддержку диапазонов

merge_slashes

Синтаксис	`merge_slashes` on | off;
По умолчанию	`merge_slashes on;`
Контекст	http, server

Разрешает или запрещает преобразование URI путем замены двух и более подряд идущих косых черт («/») на одну.

Необходимо иметь в виду, что это преобразование необходимо для корректной проверки префиксных строк и регулярных выражений. Если его не делать, то запрос `//scripts/one.php` не попадет в

```
location /scripts/ { }
```

и может быть обслужен как статический файл. Поэтому он преобразуется к виду `/scripts/one.php`.

Запрет преобразования может понадобиться, если в URI используются имена, закодированные методом *base64*, в котором задействован символ «/». Однако из соображений безопасности лучше избегать отключения преобразования.

Если директива указана на уровне *server*, то может использоваться значение из сервера по умолчанию.

msie_padding

Синтаксис	`msie_padding` on | off;
По умолчанию	`msie_padding on;`
Контекст	http, server, location

Разрешает или запрещает добавлять в ответы для MSIE со статусом больше 400 комментарий для увеличения размера ответа до 512 байт.

msie_refresh

Синтаксис	`msie_refresh` on | off;
По умолчанию	`msie_refresh off;`
Контекст	http, server, location

Разрешает или запрещает выдавать для MSIE клиентов refresh'ы вместо перенаправлений.

open_file_cache

Синтаксис	`open_file_cache` off; `open_file_cache` max=*N* [inactive=*время*];
По умолчанию	`open_file_cache off;`
Контекст	http, server, location

Задает кэш, в котором могут храниться:

- дескрипторы открытых файлов, информация об их размерах и времени модификации;
- информация о существовании каталогов;
- информация об ошибках поиска файла — «нет файла», «нет прав на чтение» и тому подобное.

Кэширование ошибок нужно разрешить отдельно директивой *open_file_cache_errors*.

`max`	задает максимальное число элементов в кэше; при переполнении кэша удаляются наименее востребованные элементы (LRU);
`inactive`	задает время, после которого элемент кэша удаляется, если к нему не было обращений в течение этого времени; по умолчанию 60 секунд;
`off`	запрещает кэш.

Пример:

```
open_file_cache          max=1000 inactive=20s;
open_file_cache_valid    30s;
open_file_cache_min_uses 2;
open_file_cache_errors   on;
```

open_file_cache_errors

Синтаксис	`open_file_cache_errors` on | off;
По умолчанию	`open_file_cache_errors off;`
Контекст	http, server, location

Разрешает или запрещает кэширование ошибок поиска файлов в *open_file_cache*.

open_file_cache_min_uses

Синтаксис	`open_file_cache_min_uses` *число;*
По умолчанию	`open_file_cache_min_uses 1;`
Контекст	http, server, location

Задает минимальное число обращений к файлу в течение времени, заданного параметром inactive директивы *open_file_cache*, необходимых для того, чтобы дескриптор файла оставался открытым в кэше.

open_file_cache_valid

Синтаксис	`open_file_cache_valid` *время;*
По умолчанию	`open_file_cache_valid 60s;`
Контекст	http, server, location

Определяет время, через которое следует проверять актуальность информации об элементе в *open_file_cache*.

output_buffers

Синтаксис	`output_buffers` *число размер;*
По умолчанию	`output_buffers 2 32k;`
Контекст	http, server, location

Задает *число* и *размер* буферов, используемых при чтении ответа с диска.

port_in_redirect

Синтаксис	`port_in_redirect` on | off;
По умолчанию	`port_in_redirect on;`
Контекст	http, server, location

Разрешает или запрещает указывать порт в *абсолютных* перенаправлениях, выдаваемых Angie PRO.

Использование в перенаправлениях основного имени сервера управляется директивой *server_name_in_redirect*.

postpone_output

Синтаксис	`postpone_output` *размер*;
По умолчанию	`postpone_output 1460;`
Контекст	http, server, location

Если это возможно, то отправка данных клиенту будет отложена пока Angie PRO не накопит по крайней мере указанное количество байт для отправки.

0	запрещает отложенную отправку данных

read_ahead

Синтаксис	`read_ahead` *размер*;
По умолчанию	`read_ahead 0;`
Контекст	http, server, location

Задает ядру размер предчтения при работе с файлами.

На Linux используется системный вызов *posix_fadvise(0, 0, 0, POSIX_FADV_SEQUENTIAL)*, поэтому параметр размер там игнорируется.

На FreeBSD используется системный вызов *fcntl(O_READAHEAD,* размер *)*, появившийся во FreeBSD 9.0-CURRENT.

recursive_error_pages

Синтаксис	`recursive_error_pages` on | off;
По умолчанию	`recursive_error_pages off;`
Контекст	http, server, location

Разрешает или запрещает делать несколько перенаправлений через директиву *error_page*. Число таких перенаправлений *ограничено*.

request_pool_size

Синтаксис	`request_pool_size` *размер*;
По умолчанию	`request_pool_size 4k;`
Контекст	http, server

Позволяет производить точную настройку выделений памяти под конкретные запросы. Эта директива не оказывает существенного влияния на производительность, и ее не следует использовать.

reset_timedout_connection

Синтаксис	`reset_timedout_connection` on | off;
По умолчанию	`reset_timedout_connection off;`
Контекст	http, server, location

Разрешает или запрещает сброс соединений по таймауту, а также при закрытии соединений с помощью нестандартного кода 444. Сброс делается следующим образом. Перед закрытием сокета для него задается параметр *SO_LINGER* с таймаутом *0*. После этого при закрытии сокета клиенту отсылается *TCP RST*, а вся память, связанная с этим сокетом, освобождается. Это позволяет избежать длительного нахождения уже закрытого сокета в состоянии *FIN_WAIT1* с заполненными буферами.

Примечание

соединения *keep-alive* по истечении таймаута закрываются обычным образом.

resolver

Синтаксис	`resolver` *адрес* ... [valid=*время*] [ipv4=on|off] [ipv6=on|off] [status_zone=*зона*];
По умолчанию	—
Контекст	http, server, location, upstream

Задает серверы DNS, используемые для преобразования имен вышестоящих серверов в адреса, например:

```
resolver 127.0.0.53 [::1]:5353;
```

Адрес может быть указан в виде доменного имени или IP-адреса, и необязательного порта. Если порт не указан, используется порт 53. Серверы DNS опрашиваются циклически.

По умолчанию Angie PRO кэширует ответы, используя значение TTL из ответа.

`valid`	*необязательный* параметр, позволяет переопределить срок кэширования ответа

```
resolver 127.0.0.53 [::1]:5353 valid=30s;
```

По умолчанию Angie PRO будет искать как IPv4-, так и IPv6-адреса при преобразовании имен в адреса.

`ipv4=off`	запрещает поиск IPv4-адресов
`ipv6=off`	запрещает поиск IPv6-адресов

`status_zone`	*необязательный* параметр; включает сбор метрик запросов и ответов DNS-сервера (*/status/resolvers/<zone>*) в указанной зоне

Совет

Для предотвращения DNS-спуфинга рекомендуется использовать DNS-серверы в защищенной доверенной локальной сети.

resolver_timeout

Синтаксис	`resolver_timeout` *время;*
По умолчанию	`resolver_timeout 30s;`
Контекст	http, server, location, upstream

Задает таймаут для преобразования имени в адрес, например:

```
resolver_timeout 5s;
```

root

Синтаксис	`root` *путь;*
По умолчанию	`root html;`
Контекст	http, server, location, if в location

Задает корневой каталог для запросов. Например, при такой конфигурации

```
location /i/ {
  root /data/w3;
}
```

в ответ на запрос `/i/top.gif` будет отдан файл `/data/w3/i/top.gif`.

В значении параметра путь можно использовать переменные, кроме *$document_root* и *$realpath_root*.

Путь к файлу формируется путем простого добавления URI к значению директивы root. Если же URI необходимо поменять, следует воспользоваться директивой *alias*.

satisfy

Синтаксис	`satisfy` all | any;
По умолчанию	`satisfy all;`
Контекст	http, server, location

Разрешает доступ, если его разрешают все (*all*) или хотя бы один (*any*) из модулей *Access*, *Auth Basic* или *Auth Request*.

```
location / {
  satisfy any;

  allow 192.168.1.0/32;
  deny  all;

  auth_basic           "closed site";
  auth_basic_user_file conf/htpasswd;
}
```

send_lowat

Синтаксис	`send_lowat` *размер*;
По умолчанию	`send_lowat 0;`
Контекст	http, server, location

При установке этой директивы в ненулевое значение Angie PRO будет пытаться минимизировать число операций отправки на клиентских сокетах либо при помощи флага `NOTE_LOWAT` метода *kqueue*, либо при помощи параметра сокета `SO_SNDLOWAT`. В обоих случаях будет использован указанный размер.

send_timeout

Синтаксис	`send_timeout` *время;*
По умолчанию	`send_timeout 60s;`
Контекст	http, server, location

Задает таймаут при передаче ответа клиенту. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями записи. Если по истечении этого времени клиент ничего не примет, соединение будет закрыто.

sendfile

Синтаксис	`sendfile` on | off;
По умолчанию	`sendfile off;`
Контекст	http, server, location, if в location

Разрешает или запрещает использовать *sendfile()*.

Возможно использование *aio* для подгрузки данных для *sendfile()*:

```
location /video/ {
  sendfile       on;
  tcp_nopush     on;
  aio            on;
}
```

В такой конфигурации функция *sendfile()* вызывается с флагом *SF_NODISKIO*, в результате чего она не блокируется на диске, а сообщает об отсутствии данных в памяти. После этого Angie PRO инициирует асинхронную подгрузку данных, читая один байт. При этом ядро FreeBSD подгружает в память первые 128K байт файла, однако при последующих чтениях файл подгружается частями только по 16K. Изменить это можно с помощью директивы *read_ahead*.

sendfile_max_chunk

Синтаксис	`sendfile_max_chunk` *размер*;
По умолчанию	`sendfile_max_chunk 2m;`
Контекст	http, server, location

Ограничивает объем данных, который может передан за один вызов *sendfile()*. Без этого ограничения одно быстрое соединение может целиком захватить рабочий процесс.

server

Синтаксис	`server { ... }`
По умолчанию	—
Контекст	http

Задает конфигурацию для виртуального сервера. Четкого разделения виртуальных серверов на IP-based (на основании IP-адреса) и name-based (на основании поля «Host» заголовка запроса) нет. Вместо этого директивами *listen* описываются все адреса и порты, на которых нужно принимать соединения для этого сервера, а в директиве *server_name* указываются все имена серверов.

Подробнее: *Как обрабатываются запросы*

server_name

Синтаксис	`server_name` *имя* ...;
По умолчанию	`server_name "";`
Контекст	server

Задает имена виртуального сервера, например:

```
server {
  server_name example.com www.example.com;
}
```

Первое имя становится основным именем сервера.

В именах серверов можно использовать звездочку («*») для замены первой или последней части имени:

```
server {
  server_name example.com *.example.com www.example.*;
}
```

Такие имена называются именами с маской.

Два первых вышеприведенных имени можно объединить в одно:

```
server {
  server_name .example.com;
}
```

В качестве имени сервера можно также использовать регулярное выражение, указав перед ним тильду («~»):

```
server {
  server_name ~^www\d+\.example\.com$ www.example.com;
}
```

Регулярное выражение может содержать выделения, которые могут затем использоваться в других директивах:

```
server {
  server_name ~^(www\.)?(.+)$;

  location / {
     root /sites/$2;
  }
}

server {
  server_name _;

  location / {
     root /sites/default;
  }
}
```

Именованные выделения в регулярном выражении создают переменные, которые могут затем использоваться в других директивах:

```
  server {
    server_name ~^(www\.)?(?<domain>.+)$;

    location / {
       root /sites/$domain;
    }
  }

server {
    server_name _;

    location / {
       root /sites/default;
    }
  }
```

Примечание

Если параметр директивы установлен в *$hostname*, то подставляется имя хоста (*hostname*) машины.

При поиске виртуального сервера по имени, если имени соответствует несколько из указанных вариантов, например, одновременно подходят и имя с маской, и регулярное выражение, будет выбран первый подходящий вариант в следующем порядке приоритета:

- точное имя
- самое длинное имя с маской в начале, например «*.example.com»
- самое длинное имя с маской в конце, например «mail.*»
- первое подходящее регулярное выражение (в порядке следования в конфигурационном файле)

Внимание

Чтобы использовать `server_name` с TLS, необходимо терминировать TLS-соединение. Эта директива сопоставляется с `Host` в HTTP-запросе, поэтому рукопожатие должно быть закончено, а соединение расшифровано.

server_name_in_redirect

Синтаксис	`server_name_in_redirect` on | off;
По умолчанию	`server_name_in_redirect off`;
Контекст	http, server, location

Разрешает или запрещает использовать в *абсолютных* перенаправлениях, выдаваемых Angie PRO, основное имя сервера, задаваемое директивой *server_name*.

`on`	используется основное имя сервера, задаваемое директивой *server_name*
`off`	используется имя, указанное в поле «Host» заголовка запроса. Если же этого поля нет, то используется IP-адрес сервера.

Использование в перенаправлениях порта управляется директивой *port_in_redirect*.

server_names_hash_bucket_size

Синтаксис	`server_names_hash_bucket_size` *размер*;
По умолчанию	`server_names_hash_bucket_size 32 | 64 | 128;`
Контекст	http

Задает размер корзины в хэш-таблицах имен серверов. Значение по умолчанию зависит от размера строки кэша процессора. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

server_names_hash_max_size

Синтаксис	`server_names_hash_max_size` *размер*;
По умолчанию	`server_names_hash_max_size 512;`
Контекст	http

Задает максимальный размер хэш-таблиц имен серверов. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

server_tokens

Синтаксис	`server_tokens` on | off | build | *строка*;
По умолчанию	`server_tokens on;`
Контекст	http, server, location

Разрешает или запрещает указывать версию Angie PRO на страницах ошибок и в поле заголовка ответа `Server`. Если указан параметр *build*, то вместе с версией будет также указано имя сборки, заданное соответствующим параметром скрипта configure.

Добавлено в версии 1.1.0: PRO

В Angie PRO директива может быть задана *строкой*, которая может также содержать переменные. Тогда на страницах ошибок и в поле заголовка ответа `Server` вместо имени сервера, версии и имени сборки будет указываться значение этой строки с подставленными переменными. Пустая *строка* запрещает выдачу поля `Server`.

status_zone

Синтаксис	`status_zone` *зона*;
По умолчанию	—
Контекст	server, location, if в location

Выделяет зону разделяемой памяти для сбора метрик */status/http/location_zones/<zone>* и */status/http/server_zones/<zone>*.

Несколько контекстов `server` могут совместно использовать одну и ту же зону для сбора данных; особое значение `off` выключает сбор данных во вложенных блоках `location`.

subrequest_output_buffer_size

Синтаксис	`subrequest_output_buffer_size` *размер*;
По умолчанию	`subrequest_output_buffer_size 4k | 8k;`
Контекст	http, server, location

Задает размер буфера, используемого для хранения тела ответа подзапроса. По умолчанию размер одного буфера равен размеру страницы памяти. В зависимости от платформы это или *4K*, или *8K*, однако его можно сделать меньше.

Примечание

Директива применима только для подзапросов, тело ответа которых сохраняется в памяти. Например, подобные подзапросы создаются при помощи *SSI*.

tcp_nodelay

Синтаксис	`tcp_nodelay` on | off;
По умолчанию	`tcp_nodelay on`;
Контекст	http, server, location

Разрешает или запрещает использование параметра *TCP_NODELAY*. Параметр включается при переходе соединения в состояние *keep-alive*. Также, он включается на SSL-соединениях, при небуферизованном проксировании и при *проксировании WebSocket*.

tcp_nopush

Синтаксис	`tcp_nopush` on | off;
По умолчанию	`tcp_nopush off`;
Контекст	http, server, location

Разрешает или запрещает использование параметра сокета *TCP_NOPUSH* во FreeBSD или *TCP_CORK* в Linux. Параметр включаются только при использовании *sendfile*. Включение параметра позволяет

- передавать заголовок ответа и начало файла в одном пакете в Linux и во FreeBSD 4.*;
- передавать файл полными пакетами.

try_files

Синтаксис	`try_files` файл ... *uri*; `try_files` файл ... =*код*;
По умолчанию	—
Контекст	server, location

Проверяет существование файлов в заданном порядке и использует для обработки запроса первый найденный файл, причем обработка делается в контексте этого же *location*'а. Путь к файлу строится из параметра *файл* в соответствии с директивами *root* и *alias*. С помощью косой черты в конце имени можно проверить существование каталога, например, *$uri/*. В случае, если ни один файл не найден, то делается внутреннее перенаправление на *uri*, заданный последним параметром. Например:

```
location /images/ {
  try_files $uri /images/default.gif;
}

location = /images/default.gif {
  expires 30s;
}
```

Последний параметр может также указывать на именованный *location*, может также быть кодом:

```
location / {
  try_files $uri $uri/index.html $uri.html =404;
}
```

В следующем примере директива *try_files*

```
location / {
  try_files $uri $uri/ @drupal;
}
```

аналогична директивам

```
location / {
  error_page 404 = @drupal;
  log_not_found off;
}
```

А здесь

```
location ~ \.php$ {
  try_files $uri @drupal;

  fastcgi_pass ...;

  fastcgi_param SCRIPT_FILENAME /path/to$fastcgi_script_name;

#  ...
}
```

try_files проверяет существование PHP-файла, прежде чем передать запрос FastCGI-серверу.

```
location / {
  try_files /system/maintenance.html
            $uri $uri/index.html $uri.html
            @mongrel;
}

location @mongrel {
  proxy_pass http://mongrel;
}
```

```
location / {
  try_files $uri $uri/ @drupal;
}

location ~ \.php$ {
  try_files $uri @drupal;

  fastcgi_pass ...;

  fastcgi_param SCRIPT_FILENAME /path/to$fastcgi_script_name;
  fastcgi_param SCRIPT_NAME     $fastcgi_script_name;
  fastcgi_param QUERY_STRING    $args;

#  ... прочие fastcgi_param
}

location @drupal {
  fastcgi_pass ...;

  fastcgi_param SCRIPT_FILENAME /path/to/index.php;
  fastcgi_param SCRIPT_NAME     /index.php;
  fastcgi_param QUERY_STRING    q=$uri&$args;

#  ... прочие fastcgi_param
}
```

```
location / {
  try_files $uri $uri/ @wordpress;
}

location ~ \.php$ {
  try_files $uri @wordpress;

  fastcgi_pass ...;

  fastcgi_param SCRIPT_FILENAME /path/to$fastcgi_script_name;
#  ... прочие fastcgi_param
}

location @wordpress {
  fastcgi_pass ...;

  fastcgi_param SCRIPT_FILENAME /path/to/index.php;
#  ... прочие fastcgi_param
}
```

types

Синтаксис	`types { ... }`
По умолчанию	`types` *`text/html html; image/gif gif; image/jpeg jpg;`*
Контекст	http, server, location

Задает соответствие расширений имен файлов и MIME-типов ответов. Расширения нечувствительны к регистру символов. Одному MIME-типу может соответствовать несколько расширений, например:

```
types {
  application/octet-stream bin exe dll;
  application/octet-stream deb;
  application/octet-stream dmg;
}
```

Достаточно полная таблица соответствий входит в дистрибутив Angie PRO и находится в файле `conf/mime.types`.

Для того чтобы для определенного *location*'а для всех ответов выдавался MIME-тип «application/octet-stream», можно использовать следующее:

```
location /download/ {
  types        { }
  default_type application/octet-stream;
}
```

types_hash_bucket_size

Синтаксис	`types_hash_bucket_size` *размер*;
По умолчанию	`types_hash_bucket_size 64;`
Контекст	http, server, location

Задает размер корзины в хэш-таблицах типов. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

types_hash_max_size

Синтаксис	`types_hash_max_size` *размер*;
По умолчанию	`types_hash_max_size 1024;`
Контекст	http, server, location

Задает максимальный размер хэш-таблиц типов. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

underscores_in_headers

Синтаксис	`underscores_in_headers` on | off;
По умолчанию	`underscores_in_headers off;`
Контекст	http, server

Разрешает или запрещает использование символов подчеркивания в полях заголовка запроса клиента. Если использование символов подчеркивания запрещено, поля заголовка запроса, в именах которых есть подчеркивания, помечаются как недопустимые и подпадают под действие директивы *ignore_invalid_headers*.

Если директива указана на уровне *server*, то может использоваться значение из сервера по умолчанию.

variables_hash_bucket_size

Синтаксис	`variables_hash_bucket_size` *размер*;
По умолчанию	`variables_hash_bucket_size 64;`
Контекст	http

Задает размер корзины в хэш-таблице переменных. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

variables_hash_max_size

Синтаксис	`variables_hash_max_size` *размер*;
По умолчанию	`variables_hash_max_size 1024;`
Контекст	http

Задает максимальный размер хэш-таблиц переменных. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

Встроенные переменные

Модуль *http_core* поддерживает встроенные переменные, имена которых совпадают с именами переменных веб-сервера Apache. Прежде всего, это переменные, представляющие из себя поля заголовка запроса клиента, такие как *$http_user_agent*, *$http_cookie* и тому подобное. Кроме того, есть и другие переменные:

`$angie_version`

версия Angie PRO

`$arg_` ***имя***

аргумент *имя* в строке запроса

`$args`

аргументы в строке запроса

`$binary_remote_addr`

адрес клиента в бинарном виде, длина значения всегда 4 байта для IPv4-адресов или 16 байт для IPv6-адресов

`$body_bytes_sent`

число байт, переданное клиенту, без учета заголовка ответа; переменная совместима с параметром «%B» модуля Apache *mod_log_config*

`$bytes_sent`

число байт, переданных клиенту

`$connection`

порядковый номер соединения

`$connection_requests`

текущее число запросов в соединении

`$connection_time`

время соединения в секундах с точностью до миллисекунд

`$content_length`

поле «Content-Length» заголовка запроса

`$content_type`

поле «Content-Type» заголовка запроса

`$cookie_` ***имя***

cookie *имя*

`$document_root`

значение директивы *root* или *alias* для текущего запроса

`$document_uri`

то же, что и *$uri*

`$host`

в порядке приоритета: имя хоста из строки запроса, или имя хоста из поля «Host» заголовка запроса, или имя сервера, соответствующего запросу

`$hostname`

имя хоста

`$http_` ***имя***

произвольное поле заголовка запроса; последняя часть имени переменной соответствует имени поля, приведенному к нижнему регистру, с заменой символов тире на символы подчеркивания

`$https`

on если соединение работает в режиме SSL, либо пустая строка

`$is_args`

?, если в строке запроса есть аргументы, и пустая строка, если их нет

`$limit_rate`

установка этой переменной позволяет ограничивать скорость передачи ответа, см. *limit_rate*

`$msec`

текущее время в секундах с точностью до миллисекунд

`$pid`

номер (PID) рабочего процесса

`$pipe`

p если запрос был pipelined, иначе .

`$proxy_protocol_addr`

адрес клиента, полученный из заголовка протокола PROXY Протокол PROXY должен быть предварительно включен при помощи установки параметра *proxy_protocol* в директиве *listen*.

`$proxy_protocol_port`

порт клиента, полученный из заголовка протокола PROXY Протокол PROXY должен быть предварительно включен при помощи установки параметра *proxy_protocol* в директиве *listen*.

`$proxy_protocol_server_addr`

адрес сервера, полученный из заголовка протокола PROXY Протокол PROXY должен быть предварительно включен при помощи установки параметра *proxy_protocol* в директиве *listen*.

`$proxy_protocol_server_port`

порт сервера, полученный из заголовка протокола PROXY Протокол PROXY должен быть предварительно включен при помощи установки параметра *proxy_protocol* в директиве *listen*.

`$proxy_protocol_tlv_` ***имя***

TLV, полученный из заголовка протокола PROXY. *Имя* может быть именем типа TLV или его числовым значением. В последнем случае значение задается в шестнадцатеричном виде и должно начинаться с *0x*:

$proxy_protocol_tlv_alpn $proxy_protocol_tlv_0x01

SSL TLV могут также быть доступны как по имени типа TLV, так и по его числовому значению, оба должны начинаться с *ssl_*:

$proxy_protocol_tlv_ssl_version $proxy_protocol_tlv_ssl_0x21

Поддерживаются следующие имена типов TLV:

- *alpn (0x01)* - протокол более высокого уровня, используемый поверх соединения
- *authority (0x02)* - значение имени хоста, передаваемое клиентом
- *unique_id (0x05)* - уникальный идентификатор соединения
- *netns (0x30)* - имя пространства имен

- *ssl (0x20)* - структура SSL TLV в бинарном виде

Поддерживаются следующие имена типов SSL TLV:

- *ssl_ version (0x21)* - версия SSL, используемая в клиентском соединении
- *ssl_ cn (0x22)* - Common Name сертификата
- *ssl_ cipher (0x23)* - имя используемого шифра
- *ssl_ sig_ alg (0x24)* - алгоритм, используемый для подписи сертификата
- *ssl_ key_ alg (0x25)* - алгоритм публичного ключа

Также поддерживается следующее специальное имя типа SSL TLV:

- *ssl_ verify* - результат проверки клиентского сертификата: *0*, если клиент предоставил сертификат и он был успешно верифицирован, либо ненулевое значение

Протокол PROXY должен быть предварительно включен при помощи установки параметра *proxy_ protocol* в директиве *listen*.

`$query_string`

то же, что и *$args*

`$realpath_root`

абсолютный путь, соответствующий значению директивы *root* или *alias* для текущего запроса, в котором все символические ссылки преобразованы в реальные пути

`$remote_addr`

адрес клиента

`$remote_port`

порт клиента

`$remote_user`

имя пользователя, использованное в Basic аутентификации

`$request`

первоначальная строка запроса целиком

`$request_body`

тело запроса Значение переменной *появляется* в *location*'ах, обрабатываемых директивами *proxy_pass*, *fastcgi_pass*, *uwsgi_pass* и *scgi_pass*, когда тело было прочитано в *буфер в памяти*.

`$request_body_file`

имя временного файла, в котором хранится тело запроса По завершении обработки файл необходимо удалить. Для того чтобы тело запроса всегда записывалось в файл, следует включить *client_body_in_file_only*. При передаче имени временного файла в проксированном запросе или в запросе к FastCGI/uwsgi/SCGI-серверу следует запретить передачу самого тела директивами *proxy_pass_request_body off*, *fastcgi_pass_request_body off*, *uwsgi_pass_request_body off* или *scgi_pass_request_body off* соответственно.

`$request_completion`

«OK» если запрос завершился, либо пустая строка

`$request_filename`

путь к файлу для текущего запроса, формируемый из директив *root* или *alias* и URI запроса

`$request_id`

уникальный идентификатор запроса, сформированный из 16 случайных байт, в шестнадцатеричном виде

`$request_length`

длина запроса (включая строку запроса, заголовок и тело запроса)

`$request_method`

метод запроса, обычно «GET» или «POST»

`$request_time`

время обработки запроса в секундах с точностью до миллисекунд; время, прошедшее с момента чтения первых байт от клиента

`$request_uri`

первоначальный URI запроса целиком (с аргументами)

`$scheme`

схема запроса, «http» или «https»

`$sent_http_` ***имя***

произвольное поле заголовка ответа; последняя часть имени переменной соответствует имени поля, приведенному к нижнему регистру, с заменой символов тире на символы подчеркивания

`$sent_trailer_` ***имя***

произвольное поле, отправленное в конце ответа; последняя часть имени переменной соответствует имени поля, приведенному к нижнему регистру, с заменой символов тире на символы подчеркивания

`$server_addr`

адрес сервера, принявшего запрос Получение значения этой переменной обычно требует одного системного вызова. Чтобы избежать системного вызова, в директивах *listen* следует указывать адреса и использовать параметр *bind*.

`$server_name`

имя сервера, принявшего запрос

`$server_port`

порт сервера, принявшего запрос

`$server_protocol`

протокол запроса, обычно «HTTP/1.0», «HTTP/1.1» или «HTTP/2.0»

`$status`

статус ответа

`$time_iso8601`

локальное время в формате по стандарту ISO 8601

`$time_local`

локальное время в Common Log Format

`$tcpinfo_rtt, $tcpinfo_rttvar, $tcpinfo_snd_cwnd, $tcpinfo_rcv_space`

информация о клиентском TCP-соединении; доступна на системах, поддерживающих параметр сокета *TCP_INFO*

`$uri`

текущий URI запроса в *нормализованном* виде Значение *$uri* может изменяться в процессе обработки запроса, например, при внутренних перенаправлениях или при использовании индексных файлов.

Потоковый модуль

Access

Модуль позволяет ограничить доступ для определенных адресов клиентов.

Пример конфигурации

```
server {
    ...
    deny  192.168.1.1;
    allow 192.168.1.0/24;
    allow 10.1.1.0/16;
    allow 2001:0db8::/32;
    deny  all;
}
```

Правила проверяются в порядке их записи до первого соответствия. В данном примере доступ разрешен только для IPv4-сетей *10.1.1.0/16* и *192.168.1.0/24*, кроме адреса *192.168.1.1*, и для IPv6-сети *2001:0db8::/32*.

Директивы

allow

Синтаксис	`allow` *адрес* | *CIDR* | unix: | all;
По умолчанию	—
Контекст	stream, server

Разрешает доступ для указанной сети или адреса. Если указано специальное значение `unix:`, разрешает доступ для всех UNIX-сокетов.

deny

Синтаксис	`deny` *адрес* | *CIDR* | unix: | all;
По умолчанию	—
Контекст	stream, server

Запрещает доступ для указанной сети или адреса. Если указано специальное значение `unix:`, запрещает доступ для всех UNIX-сокетов.

Geo

Создает переменные, значения которых зависят от IP-адреса клиента.

Пример конфигурации

```
geo $geo {
    default        0;

    127.0.0.1      2;
    192.168.1.0/24 1;
    10.1.0.0/16    1;

    ::1            2;
    2001:0db8::/32 1;
}
```

Директивы

geo

Синтаксис	`geo` [*$адрес*] *$переменная* { ... }
По умолчанию	—
Контекст	stream

Описывает для указанной переменной зависимость значения от IP-адреса клиента. По умолчанию адрес берется из переменной *$remote_addr*, но его также можно получить из другой переменной, например:

```
geo $arg_remote_addr $geo {
    ...;
}
```

Примечание

Поскольку переменные вычисляются только в момент использования, само по себе наличие даже большого числа объявлений переменных `geo` не влечет за собой никаких дополнительных расходов на обработку соединений.

Если значение переменной не представляет из себя правильный IP-адрес, то используется адрес «255.255.255.255».

Адреса задаются либо префиксами в формате CIDR (включая одиночные адреса), либо в виде диапазонов.

Также поддерживаются следующие специальные параметры:

`delete`	удаляет описанную сеть
`default`	значение переменной, если адрес клиента не соответствует ни одному из заданных адресов. При задании адресов в формате CIDR вместо *default* можно использовать «*0.0.0.0/0*» и «*::/0*». Если параметр *default* не указан, значением по умолчанию будет пустая строка.
`include`	включает файл с адресами и значениями. Включений может быть несколько.
`ranges`	указывает, что адреса задаются в виде диапазонов. Этот параметр должен быть первым. Для ускорения загрузки гео-базы нужно располагать адреса в порядке возрастания.

Пример:

```
geo $country {
    default         ZZ;
    include         conf/geo.conf;
    delete          127.0.0.0/16;

    127.0.0.0/24    US;
    127.0.0.1/32    RU;
    10.1.0.0/16     RU;
    192.168.1.0/24 UK;
}
```

В файле *conf/geo.conf* могут быть такие строки:

```
10.2.0.0/16     RU;
192.168.2.0/24 RU;
```

В качестве значения выбирается максимальное совпадение, например, для адреса *127.0.0.1* будет выбрано значение `RU`, а не `US`.

Пример описания диапазонов:

```
geo $country {
    ranges;
    default                    ZZ;
    127.0.0.0-127.0.0.0        US;
    127.0.0.1-127.0.0.1        RU;
    127.0.0.2-127.0.0.255      US;
    10.1.0.0-10.1.255.255      RU;
    192.168.1.0-192.168.1.255 UK;
}
```

GeoIP

Создает переменные, значения которых зависят от IP-адреса клиента, используя готовые базы данных MaxMind.

При использовании баз данных с поддержкой IPv6 IPv4-адреса ищутся отображенными на IPv6.

При сборке из исходного кода модуль необходимо включить с помощью параметра сборки `--with-stream_geoip_module`.

Важно

Для этого модуля нужна библиотека MaxMind GeoIP.

Пример конфигурации

```
stream {
    geoip_country         GeoIP.dat;
    geoip_city            GeoLiteCity.dat;

    map $geoip_city_continent_code $nearest_server {
        default        example.com;
        EU           eu.example.com;
        NA           na.example.com;
        AS           as.example.com;
    }
#   ...
}
```

Директивы

geoip_country

Синтаксис	`geoip_country` *файл*;
По умолчанию	—
Контекст	stream

Задает базу данных для определения страны в зависимости от значения IP-адреса клиента. При использовании этой базы данных доступны следующие переменные:

`$geoip_country_c`	двухбуквенный код страны, например, «RU», «US».
`$geoip_country_c`	трехбуквенный код страны, например, «RUS», «USA».
`$geoip_country_n`	название страны, например, «Russian Federation», «United States».

geoip_city

Синтаксис	`geoip_city` *файл*;
По умолчанию	—
Контекст	stream

Задает базу данных для определения страны, региона и города в зависимости от значения IP-адреса клиента. При использовании этой базы данных доступны следующие переменные:

`$geoip_city_cont`	двухбуквенный код континента, например, «EU», «NA».
`$geoip_city_coun`	двухбуквенный код страны, например, «RU», «US».
`$geoip_city_coun`	трехбуквенный код страны, например, «RUS», «USA».
`$geoip_city_coun`	название страны, например, «Russian Federation», «United States».
`$geoip_dma_code`	DMA-код региона в США (также известный как «код агломерации»), согласно геотаргетингу Google AdWords API.
`$geoip_latitude`	широта.
`$geoip_longitude`	долгота.
`$geoip_region`	двухсимвольный код региона страны (область, край, штат, провинция, федеральная земля и тому подобное), например, «48», «DC».
`$geoip_region_na`	название региона страны (область, край, штат, провинция, федеральная земля и тому подобное), например, «Moscow City», «District of Columbia».
`$geoip_city`	название города, например, «Moscow», «Washington».
`$geoip_postal_co`	почтовый индекс.

geoip_org

Синтаксис	`geoip_org` *файл*;
По умолчанию	—
Контекст	stream

Задает базу данных для определения названия организации в зависимости от значения IP-адреса клиента. При использовании этой базы данных доступна следующая переменная:

`$geoip_org`	название организации, например, «The University of Melbourne».

JS

Позволяет задавать обработчики на njs — подмножестве языка JavaScript.

В наших репозиториях модуль собран динамически и доступен отдельным пакетом *angie-pro-module-njs*; подключить его можно с помощью директивы *load_module*.

Пример конфигурации

```
stream {
    js_import stream.js;

    js_set $bar stream.bar;
    js_set $req_line stream.req_line;

    server {
        listen 12345;

        js_preread stream.preread;
        return     $req_line;
    }

    server {
        listen 12346;

        js_access  stream.access;
        proxy_pass 127.0.0.1:8000;
        js_filter  stream.header_inject;
    }
}

http {
    server {
        listen 8000;
        location / {
            return 200 $http_foo\n;
        }
    }
}
```

Файл `stream.js`:

```
var line = '';

function bar(s) {
    var v = s.variables;
    s.log("hello from bar() handler!");
    return "bar-var" + v.remote_port + "; pid=" + v.pid;
}

function preread(s) {
    s.on('upload', function (data, flags) {
        var n = data.indexOf('\n');
        if (n != -1) {
            line = data.substr(0, n);
            s.done();
        }
    });
}

function req_line(s) {
    return line;
}

// Чтение строки HTTP-запроса.
```

```
// Получение байт в 'req' до того как
// будет прочитана строка запроса.
// Добавление HTTP-заголовка в запрос клиента

var my_header =  'Foo: foo';
function header_inject(s) {
    var req = '';
    s.on('upload', function(data, flags) {
        req += data;
        var n = req.search('\n');
        if (n != -1) {
            var rest = req.substr(n + 1);
            req = req.substr(0, n + 1);
            s.send(req + my_header + '\r\n' + rest, flags);
            s.off('upload');
        }
    });
}

function access(s) {
    if (s.remoteAddress.match('^192.*')) {
        s.deny();
        return;
    }

    s.allow();
}

export default {bar, preread, req_line, header_inject, access};
```

Директивы

js_access

Синтаксис	`js_access` *функция* | *модуль.функция*;
По умолчанию	—
Контекст	stream, server

Задает функцию njs, которая будет вызываться в *access-фазе*. Можно ссылаться на функцию модуля.

Функция вызывается однократно при первом достижении сессией *access-фазе*. Функция вызывается со следующими аргументами:

s	объект stream-сессии

В этой фазе может происходить инициализация, также при помощи метода s.on() может регистрироваться вызов для каждого входящего блока данных пока не будет вызван один из методов: s.done(), s.decline(), s.allow(). При вызове любого из этих методов обработка сессии переходит на *следующую фазу* и все текущие вызовы s.on() сбрасываются.

js_fetch_buffer_size

Синтаксис	`js_fetch_buffer_size` *размер*;
По умолчанию	`js_fetch_buffer_size 16k;`
Контекст	stream, server

Задает размер буфера, который будет использоваться для чтения и записи для Fetch API.

js_fetch_ciphers

Синтаксис	`js_fetch_ciphers` *шифры*;
По умолчанию	`js_fetch_ciphers HIGH:!aNULL:!MD5;`
Контекст	stream, server

Описывает разрешенные шифры для HTTPS-соединений при помощи Fetch API. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL.

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

js_fetch_max_response_buffer_size

Синтаксис	`js_fetch_max_response_buffer_size` *размер*;
По умолчанию	`js_fetch_max_response_buffer_size 1m;`
Контекст	stream, server

Задает максимальный размер ответа, полученного при помощи Fetch API.

js_fetch_protocols

Синтаксис	`js_fetch_protocols` [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`js_fetch_protocols TLSv1 TLSv1.1 TLSv1.2;`
Контекст	stream, server

Разрешает указанные протоколы для HTTPS-соединений при помощи Fetch API.

js_fetch_timeout

Синтаксис	`js_fetch_timeout` *время*;
По умолчанию	`js_fetch_timeout 60s;`
Контекст	stream, server

Задает таймаут при чтении и записи при помощи Fetch API. Таймаут устанавливается не на всю передачу ответа, а только между двумя операциями чтения. Если по истечении этого времени данные не передавались, соединение закрывается.

js_fetch_trusted_certificate

Синтаксис	`js_fetch_trusted_certificate` *файл*;
По умолчанию	—
Контекст	stream, server

Задает файл с доверенными сертификатами CA в формате PEM, используемыми при проверке HTTPS-сертификата при помощи Fetch API.

js_fetch_verify

Синтаксис	`js_fetch_verify` on | off;
По умолчанию	`js_fetch_verify on;`
Контекст	stream, server

Разрешает или запрещает проверку сертификата HTTPS-сервера при помощи Fetch API.

js_fetch_verify_depth

Синтаксис	`js_fetch_verify_depth` *число*;
По умолчанию	`js_fetch_verify_depth 100;`
Контекст	stream, server

Устанавливает глубину проверки в цепочке HTTPS-сертификатов при помощи Fetch API.

js_filter

Синтаксис	`js_filter` *функция* | *модуль.функция*;
По умолчанию	—
Контекст	stream, server

Задает фильтр данных. Можно ссылаться на функцию модуля.

Функция фильтра вызывается однократно при первом достижении сессией *content-фазы*. Функция фильтра вызывается со следующими аргументами:

`s`	объект stream-сессии

В этой фазе может происходить инициализация, также при помощи метода s.on() может регистрироваться вызов для каждого входящего блока данных. Для отмены регистрации вызова и отмены фильтра можно использовать метод s.off().

Примечание

Так как обработчик *js_filter* должен сразу возвращать результат, то поддерживаются только синхронные операции. Таким образом, асинхронные операции, например ngx.fetch() или setTimeout(), не поддерживаются.

js_import

Синтаксис	`js_import` *модуль.js* | *имя_экспорта* from *модуль.js*;
По умолчанию	—
Контекст	stream, server

Импортирует модуль, позволяющий задавать обработчики location и переменных на njs. *Имя_экспорта* является пространством имен при доступе к функциям модуля. Если *имя_экспорта* не задано, то пространством имен будет являться имя модуля.

```
js_import stream.js;
```

В примере при доступе к экспорту в качестве пространства имен используется имя модуля *stream*. Если импортируемый модуль экспортирует *foo()*, то для доступа используется *stream.foo*.

Директив *js_import* может быть несколько.

js_path

Синтаксис	`js_path` *путь*;
По умолчанию	—
Контекст	stream, server

Задает дополнительный путь для модулей njs.

js_preload_object

Синтаксис	`js_preload_object` *имя.json* | *имя from файл.json*;
По умолчанию	—
Контекст	stream, server

Предварительно загружает неизменяемый объект во время конфигурации. *Имя* используется в качестве имени глобальной переменной, через которую объект доступен в коде njs. Если *имя* не указано, то будет использоваться имя файла.

```
js_preload_object map.json;
```

В примере *map* используется в качестве имени во время доступа к предварительно загруженному объекту.

Директив *js_preload_object* может быть несколько.

js_preread

Синтаксис	`js_preread` *функция* | *модуль.функция*;
По умолчанию	—
Контекст	stream, server

Задает функцию njs, которая будет вызываться в *preread-фазе*. Можно ссылаться на функцию модуля.

Функция вызывается однократно при первом достижении сессией *preread-фазы*. Функция вызывается со следующими аргументами:

`s`	объект stream-сессии

В этой фазе может происходить инициализация, также при помощи метода s.on() может регистрироваться вызов для каждого входящего блока данных пока не будет вызван один из методов: s.done(), s.decline(), s.allow(). При вызове любого из этих методов обработка сессии переходит *на следующую фазу* и все текущие вызовы s.on() сбрасываются.

Примечание

Так как обработчик *js_preread* должен сразу возвращать результат, то поддерживаются только синхронные операции. Таким образом, асинхронные операции, например ngx.fetch() или

setTimeout(), не поддерживаются. Тем не менее асинхронные операции поддерживаются в вызовах s.on() в *preread-фазе*.

js_set

Синтаксис	`js_set` *$переменная функция* | *модуль.функция*;
По умолчанию	—
Контекст	stream, server

Задает функцию njs для указанной переменной. Можно ссылаться на функцию модуля.

Функция вызывается в момент первого обращения к переменной для данного запроса. Точный момент вызова функции зависит от *фазы*, в которой происходит обращение к переменной. Это можно использовать для реализации дополнительной логики, не относящейся к вычислению переменной. Например, если переменная указана в директиве *log_format*, то ее обработчик не будет выполняться до фазы записи в лог. Этот обработчик также может использоваться для выполнения процедур непосредственно перед освобождением запроса.

Примечание

Так как обработчик *js_set* должен сразу возвращать результат, то поддерживаются только синхронные операции. Таким образом, асинхронные операции, например ngx.fetch() или setTimeout(), не поддерживаются.

js_shared_dict_zone

Синтаксис	`js_shared_dict_zone` zone=*имя:размер* [timeout=*время*] [type=string | number] [evict];
По умолчанию	—
Контекст	stream

Задает *имя* и *размер* зоны разделяемой памяти, в которой хранится словарь ключей и значений, разделяемый между рабочими процессами.

`type`	необязательный параметр, позволяет изменить тип значения на числовой (`number`), по умолчанию в качестве ключа и значения используется строка (`string`)
`timeout`	необязательный параметр, задает время, по завершении которого все записи в словаре удаляются из зоны
`evict`	необязательный параметр, удаляет самую старую пару ключ-значение при переполнении зоны

Пример:

```
example.conf:
# Создается словарь размером 1Мб со строковыми значениями,
# пары ключ-значение удаляются при отсутствии активности в течение 60 секунд:
```

```
js_shared_dict_zone zone=foo:1M timeout=60s;

# Создается словарь размером 512Кб со строковыми значениями,
# удаляется самая старая пара ключ-значение при переполнении зоны:
js_shared_dict_zone zone=bar:512K timeout=30s evict;

# Создается постоянный словарь размером 32Кб с числовыми значениями:
js_shared_dict_zone zone=num:32k type=number;
```

```
example.js:
    function get(r) {
        r.return(200, ngx.shared.foo.get(r.args.key));
    }

    function set(r) {
        r.return(200, ngx.shared.foo.set(r.args.key, r.args.value));
    }

    function delete(r) {
        r.return(200, ngx.shared.bar.delete(r.args.key));
    }

    function increment(r) {
        r.return(200, ngx.shared.num.incr(r.args.key, 2));
    }
```

js_var

Синтаксис	`js_var` *$переменная* [*значение*];
По умолчанию	—
Контекст	stream, server

Объявляет перезаписываемую переменную. В качестве значения можно использовать текст, переменные и их комбинации.

Свойства объекта сессии

Каждый stream-обработчик njs получает один аргумент, объект stream-сессии.

Limit Conn

Позволяет ограничить число соединений по заданному ключу, в частности, число соединений с одного IP-адреса.

Пример конфигурации

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

    ...

    server {

        ...

        limit_conn           addr 1;
        limit_conn_log_level error;
    }
}
```

Директивы

limit_conn

Синтаксис	`limit_conn` *зона число*;
По умолчанию	—
Контекст	stream, server

Задает зону разделяемой памяти и максимально допустимое число соединений для одного значения ключа. При превышении этого числа сервер закроет соединение. Например, директивы

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

server {
    ...
    limit_conn addr 1;
}
```

разрешают одновременно обрабатывать не более одного соединения с одного IP-адреса.

Допустимо одновременное указание нескольких директив *limit_ conn*, при этом будет срабатывать любое из ограничений.

Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *limit_ conn*.

limit_conn_dry_run

Синтаксис	`limit_conn_dry_run` on | off;
По умолчанию	`limit_conn_dry_run off;`
Контекст	stream, server

Включает режим пробного запуска. В данном режиме число соединений не ограничивается, однако в *зоне разделяемой памяти* текущее число избыточных соединений учитывается как обычно.

limit_conn_log_level

Синтаксис	`limit_conn_log_level` info | notice | warn | error;
По умолчанию	`limit_conn_log_level error;`
Контекст	stream, server

Задает желаемый уровень записи в лог случаев ограничения числа соединений.

limit_conn_zone

Синтаксис	`limit_conn_zone` *ключ* zone = *название:размер*;
По умолчанию	—
Контекст	stream

Задает параметры зоны разделяемой памяти, которая хранит состояние для разных значений ключа. Состояние в частности содержит текущее число соединений. В качестве ключа может использоваться текст, переменные и их комбинации. Запросы с пустым значением ключа не учитываются.

Пример использования:

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

Здесь в качестве ключа используется IP-адрес клиента, задаваемый переменной `$binary_remote_addr`.

Длина значения *$binary_remote_addr* равна 4 байтам для IPv4-адресов или 16 байтам для IPv6-адресов. При этом размер состояния всегда равен 32 или 64 байтам на 32-битных платформах и 64 байтам на 64-битных. В зоне размером 1 мегабайт может разместиться около 32 тысяч состояний размером 32 байта или 16 тысяч состояний размером 64 байта. При переполнении зоны сервер закроет соединение.

Встроенные переменные

`$limit_conn_status`

хранит результат ограничения числа соединений: *PASSED*, *REJECTED* или *REJECTED_DRY_RUN*

Log

Модуль записывает логи запросов в указанном формате.

Пример конфигурации

```
log_format basic '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time';

access_log /spool/logs/angie-access.log basic buffer=32k;
```

Директивы

access_log

Синтаксис	`access_log` *путь* [*формат* [buffer=*размер*] [gzip[=*степень*]] [flush=*время*] [if=*условие*]]; `access_log` off;
По умолчанию	`access_log off;`
Контекст	stream, server

Задает *путь*, *формат* и настройки буферизованной записи в лог. На одном уровне конфигурации может использоваться несколько логов. Запись в *syslog* настраивается указанием префикса *«syslog:»* в первом параметре. Специальное значение *off* отменяет все директивы *access_log* для текущего уровня.

Если задан размер буфера с помощью параметра *buffer* или указан параметр *gzip*, то запись будет буферизованной.

Осторожно

Размер буфера должен быть не больше размера атомарной записи в дисковый файл. Для FreeBSD этот размер неограничен.

При включенной буферизации данные записываются в файл:

- если очередная строка лога не помещается в буфер;
- если данные в буфере находятся дольше интервала времени, заданного параметром *flush*;
- при *переоткрытии лог-файла* или завершении рабочего процесса.

Если задан параметр *gzip*, то буфер будет сжиматься перед записью в файл. Степень сжатия может быть задана в диапазоне от *1* (быстрее, но хуже сжатие) до *9* (медленнее, но лучше сжатие). По умолчанию используются буфер размером *64K* байт и степень сжатия *1*. Данные сжимаются атомарными блоками, и в любой момент времени лог-файл может быть распакован или прочитан с помощью утилиты *«zcat»*.

Пример:

```
access_log /path/to/log.gz basic gzip flush=5m;
```

Важно

Для поддержки gzip-сжатия логов Angie PRO должен быть собран с библиотекой *zlib*.

В пути файла можно использовать переменные, но такие логи имеют некоторые ограничения:

- *пользователь*, с правами которого работают рабочие процессы, должен иметь права на создание файлов в каталоге с такими логами;
- не работает буферизация;
- файл открывается для каждой записи в лог и сразу же после записи закрывается. Следует однако иметь в виду, что поскольку дескрипторы часто используемых файлов могут храниться в кэше, то при ротации логов в течение времени, заданного параметром *valid* директивы *open_log_file_cache*, запись может продолжаться в старый файл.

Параметр *if* включает условную запись в лог. Сессия не будет записываться в лог, если результатом вычисления условия является *«0»* или пустая строка.

log_format

Синтаксис	`log_format` *имя* [escape=default|json|none] *строка* ...;
По умолчанию	—
Контекст	stream

Задает формат лога, например:

```
log_format proxy '$remote_addr [$time_local] '
                 '$protocol $status $bytes_sent $bytes_received '
                 '$session_time "$upstream_addr" '
                 '"$upstream_bytes_sent" "$upstream_bytes_received" "$upstream_
↪connect_time"';
```

Параметр *escape* позволяет задать экранирование символов *json* или *default* в переменных, по умолчанию используется *default*. Значение *none* отключает экранирование символов.

При использовании *default* символы «"», «\», а также символы со значениями меньше 32 или больше 126 экранируются как «\xXX». Если значение переменной не найдено, то в качестве значения в лог будет записываться дефис «-«.

При использовании *json* экранируются все символы, недопустимые в JSON строках: символы «"» и «\» экранируются как «\"» и «\\», символы со значениями меньше 32 экранируются как «\n», «\r», «\t», «\b», «\f» или «\u00XX».

open_log_file_cache

Синтаксис	`open_log_file_cache` max=*N* [inactive=*время*] [min_uses=*N*] [valid=*время*];
По умолчанию	`open_log_file_cache off;`
Контекст	http, server, location

Задает кэш, в котором хранятся дескрипторы файлов часто используемых логов, имена которых заданы с использованием переменных. Параметры:

`max`	задает максимальное число дескрипторов в кэше; при переполнении кэша наименее востребованные (LRU) дескрипторы закрываются
`inactive`	задает время, после которого кэшированный дескриптор закрывается, если к нему не было обращений в течение этого времени; по умолчанию 10 секунд
`min_uses`	задает минимальное число использований файла в течение времени, заданного параметром *inactive*, после которого дескриптор файла будет оставаться открытым в кэше; по умолчанию 1
`valid`	задает, через какое время нужно проверять, что файл еще существует под тем же именем; по умолчанию 60 секунд
`off`	запрещает кэш

Пример использования:

```
open_log_file_cache max=1000 inactive=20s valid=1m min_uses=2;
```

Map

Создает переменные, значения которых зависят от значений других переменных.

Пример конфигурации

```
map $remote_addr $limit {
    127.0.0.1    "";
    default      $binary_remote_addr;
}

limit_conn_zone $limit zone=addr:10m;
limit_conn addr 1;
```

Директивы

map

Синтаксис	`map` *строка $переменная* { ... };
По умолчанию	—
Контекст	stream

Создает новую переменную. Ее значение зависит от первого параметра, заданного строкой с переменными, например:

```
set $var1 "foo";
set $var2 "bar";

map $var1$var2 $new_variable {
    default "foobar_value";
}
```

Здесь переменная `$new_variable` будет иметь значение, составленное из двух переменных `$var1` и `$var2`, или значение по умолчанию, если эти переменные не определены.

Примечание

Поскольку переменные вычисляются только в момент использования, само по себе наличие даже большого числа объявлений переменных «map» не влечет за собой никаких дополнительных расходов на обработку запросов.

Параметры внутри блока *map* задают соответствие между исходными и результирующими значениями.

Исходные значения задаются строками или регулярными выражениями.

Строки проверяются без учета регистра.

Перед регулярным выражением ставится символ «~», если при сравнении следует учитывать регистр символов, либо символы «~*», если регистр символов учитывать не нужно. Регулярное выражение может содержать именованные и позиционные выделения, которые могут затем использоваться в других директивах совместно с результирующей переменной.

Если исходное значение совпадает с именем одного из специальных параметров, описанных ниже, перед ним следует поставить символ «\".

В качестве результирующего значения можно указать текст, переменную и их комбинации.

Также поддерживаются следующие специальные параметры:

`default` *значение*	задает результирующее значение, если исходное значение не совпадает ни с одним из перечисленных. Если параметр *default* не указан, результирующим значением по умолчанию будет пустая строка.
`hostnames`	указывает, что в качестве исходных значений можно использовать маску для первой или последней части имени хоста. Этот параметр следует указывать перед списком значений.

Например,

```
*.example.com 1;
example.*     1;
```

Вместо двух записей

```
example.com   1;
*.example.com 1;
```

можно использовать одну:

```
.example.com  1;
```

`include` *файл*	включает файл со значениями. Включений может быть несколько.
`volatile`	указывает, что переменная не кэшируется.

Если исходному значению соответствует несколько из указанных вариантов, например, одновременно подходят и маска, и регулярное выражение, будет выбран первый подходящий вариант в следующем порядке приоритета:

1. строковое значение без маски
2. самое длинное строковое значение с маской в начале, например «**.example.com*»
3. самое длинное строковое значение с маской в конце, например «*mail.**»
4. первое подходящее регулярное выражение (в порядке следования в конфигурационном файле)

5. значение по умолчанию (*default*)

map_hash_bucket_size

Синтаксис	`map_hash_bucket_size` *размер*;
По умолчанию	`map_hash_bucket_size 32|64|128;`
Контекст	stream

Задает размер корзины в хэш-таблицах для переменных *map*. Значение по умолчанию зависит от размера строки кэша процессора. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

map_hash_max_size

Синтаксис	`map_hash_max_size` *размер*;
По умолчанию	`map_hash_max_size 2048;`
Контекст	stream

Задает максимальный размер хэш-таблиц для переменных *map*. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

MQTT Preread

Позволяет извлекать идентификатор клиента и имя пользователя из пакетов `CONNECT` протокола Message Queuing Telemetry Transport (MQTT) версий 3.1.1 и 5.0.

При сборке из исходного кода модуль необходимо включить с помощью параметра сборки `--with-stream_mqtt_preread_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

Выбор сервера в группе по идентификатору клиента:

```
stream {

    mqtt_preread on;

    upstream mqtt {
        hash $mqtt_preread_clientid;
        # ...
    }
}
```

Директивы

mqtt_preread

Синтаксис	`mqtt_preread` on | off;
По умолчанию	`mqtt_preread off;`
Контекст	stream, server

Управляет извлечением информации из пакета `CONNECT` на этапе *предварительного чтения*. Если параметр включен (`on`), то в контексте, где он задан, заполняются перечисленные ниже переменные.

Встроенные переменные

Подробное описание семантики значений см. в спецификации протокола MQTT версий 3.1.1 и 5.0.

`$mqtt_preread_clientid`

Уникальный идентификатор клиента.

`$mqtt_preread_username`

Необязательное имя пользователя.

Pass

Позволяет передавать принятое соединение напрямую на любой настроенный слушающий сокет в модуль *HTTP*, *потоковый* или *почтовый* модули.

Пример конфигурации

После того, как модуль `stream` завершит обработку SSL/TLS, он передает соединение в модуль `http`:

```
http {
    server {
        listen 8000;

        location / {
            root html;
        }
    }
}

stream {
    server {
        listen 12345 ssl;

        ssl_certificate     domain.crt;
        ssl_certificate_key domain.key;
```

```
        pass 127.0.0.1:8000;
    }
}
```

Директивы

pass

Синтаксис	pass *адрес*;
По умолчанию	—
Контекст	server

Эта директива задает адрес сервера, на который должно быть передано клиентское соединение. *Адрес* можно указать как IP-адрес и порт:

```
pass 127.0.0.1:12345;
```

Или как путь к UNIX-сокету:

```
pass unix:/tmp/stream.socket;
```

Также *адрес* можно задать с помощью переменных:

```
pass $upstream;
```

Proxy

Позволяет проксировать потоки данных по TCP, UDP и UNIX-сокетам.

Пример конфигурации

```
server {
    listen 127.0.0.1:12345;
    proxy_pass 127.0.0.1:8080;
}

server {
    listen 12345;
    proxy_connect_timeout 1s;
    proxy_timeout 1m;
    proxy_pass example.com:12345;
}

server {
    listen 53 udp reuseport;
    proxy_timeout 20s;
    proxy_pass dns.example.com:53;
}

server {
    listen [::1]:12345;
```

```
    proxy_pass unix:/tmp/stream.socket;
}
```

Директивы

proxy_bind

Синтаксис	`proxy_bind` *адрес* [transparent] | off;
По умолчанию	—
Контекст	stream, server

Задает локальный IP-адрес, который будет использоваться в исходящих соединениях с проксируемым сервером. В значении параметра допустимо использование переменных. Специальное значение `off` отменяет действие унаследованной с предыдущего уровня конфигурации директивы *proxy_bind*, позволяя системе самостоятельно выбирать локальный IP-адрес.

Параметр `transparent` позволяет задать нелокальный IP-адрес, который будет использоваться в исходящих соединениях с проксируемым сервером, например, реальный IP-адрес клиента:

```
proxy_bind $remote_addr transparent;
```

Для работы параметра обычно требуется запустить рабочие процессы Angie PRO с привилегиями *суперпользователя*. В Linux этого не требуется, так как если указан параметр *transparent*, то рабочие процессы наследуют capability *CAP_NET_RAW* из главного процесса.

Важно

Необходимо настроить таблицу маршрутизации ядра для перехвата сетевого трафика с проксируемого сервера.

proxy_buffer_size

Синтаксис	`proxy_buffer_size` *размер*;
По умолчанию	`proxy_buffer_size 16k;`
Контекст	stream, server

Задает размер буфера, в который будут читаться данные, получаемые от проксируемого сервера. Также задает размер буфера, в который будут читаться данные, получаемые от клиента.

proxy_connect_timeout

Синтаксис	`proxy_connect_timeout` *время*;
По умолчанию	`proxy_connect_timeout 60s;`
Контекст	stream, server

Задает таймаут для установления соединения с проксируемым сервером.

proxy_connection_drop

Синтаксис	`proxy_connection_drop` *время* | on | off;
По умолчанию	`proxy_connection_drop off;`
Контекст	http, server, location

Настраивает завершение всех соединений с проксируемым сервером, если он был удален из группы или помечен как постоянно недоступный в результате процесса *reresolve* или *команды API* `DELETE`.

Сессия завершается, когда обрабатывается следующее событие чтения или записи для клиента или проксируемого сервера.

Установка *времени* включает *таймаут* до завершения сессии; при выборе значения `on` сессии завершаются немедленно.

proxy_download_rate

Синтаксис	`proxy_download_rate` *скорость*;
По умолчанию	`proxy_download_rate 0;`
Контекст	stream, server

Ограничивает скорость чтения данных от проксируемого сервера; `скорость` задается в байтах в секунду.

`0`	отключает ограничение скорости

Примечание

Ограничение устанавливается на соединение, поэтому, если Angie PRO одновременно откроет два соединения к проксируемому серверу, суммарная скорость будет вдвое выше заданного ограничения.

В значении параметра можно использовать переменные. Это может быть полезно в случаях, когда скорость нужно ограничивать в зависимости от какого-либо условия:

```
map $slow $rate {
    1     4k;
    2     8k;
}
```

```
proxy_download_rate $rate
```

proxy_half_close

Синтаксис	`proxy_half_close` on | off;
По умолчанию	`proxy_half_close off;`
Контекст	stream, server

Разрешает или запрещает независимое закрытие каждой из сторон проксируемого соединения TCP («TCP half-close»). Если разрешено, то проксирование по TCP будет продолжаться, пока обе стороны не закроют соединение.

proxy_next_upstream

Синтаксис	`proxy_next_upstream` on | off;
По умолчанию	`proxy_next_upstream on;`
Контекст	stream, server

При невозможности установить соединение с проксируемым сервером определяет, будет ли клиентское соединение передано *следующему серверу*.

Передача соединения следующему серверу может быть ограничена по *количеству попыток* и по *времени*.

proxy_next_upstream_timeout

Синтаксис	`proxy_next_upstream_timeout` *время*;
По умолчанию	`proxy_next_upstream_timeout 0;`
Контекст	stream, server

Ограничивает время, в течение которого возможна передача запроса *следующему* серверу.

0	отключает это ограничение

proxy_next_upstream_tries

Синтаксис	`proxy_next_upstream_tries` *число*;
По умолчанию	`proxy_next_upstream_tries 0;`
Контекст	stream, server

Ограничивает число допустимых попыток для передачи запроса *следующему* серверу.

0	отключает это ограничение

proxy_pass

Синтаксис	`proxy_pass` *адрес*;
По умолчанию	—
Контекст	server

Задает адрес проксируемого сервера; `адрес` может быть указан в виде доменного имени или IP-адреса, за которым следует порт:

```
proxy_pass localhost:12345;
```

или в виде пути UNIX-сокета:

```
proxy_pass unix:/tmp/stream.socket;
```

Если доменному имени соответствует несколько адресов, то все они будут использоваться по очереди (round-robin). Кроме того, в качестве адреса можно указать *группу серверов*. Если используется группа, указать порт невозможно; вместо этого укажите порт для каждого сервера внутри группы отдельно.

Адрес можно также задать с помощью переменных:

```
proxy_pass $upstream;
```

В этом случае имя сервера ищется среди описанных *групп серверов* и если не найдено, то определяется с помощью *resolver*'а.

proxy_protocol

Синтаксис	`proxy_protocol` on | off;
По умолчанию	`proxy_protocol off;`
Контекст	stream, server

Включает протокол PROXY для соединений с проксируемым сервером.

proxy_requests

Синтаксис	`proxy_requests` *число*;
По умолчанию	`proxy_requests 0;`
Контекст	stream, server

Задает число датаграмм, полученных от клиента, по достижении которого удаляется привязка между клиентом и существующей UDP-сессией. После получения указанного количества датаграмм следующая датаграмма, полученная от того же клиента, начинает новую сессию. Сессия завершится после отправки всех принятых датаграмм на проксируемый сервер и получения указанного количества *ответов* или после *таймаута*.

proxy_responses

Синтаксис	`proxy_responses` *число*;
По умолчанию	—
Контекст	stream, server

Задает количество датаграмм, ожидаемых от проксируемого сервера в ответ на датаграмму клиента в случае, если используется протокол *UDP*. Задаваемое число служит подсказкой для завершения сессии. По умолчанию количество датаграмм не ограничено.

Если указано нулевое значение, то ответ не ожидается. Однако если ответ получен и сессия еще не завершилась, то ответ будет обработан.

proxy_socket_keepalive

Синтаксис	`proxy_socket_keepalive` on | off;
По умолчанию	`proxy_socket_keepalive off;`
Контекст	stream, server

Конфигурирует поведение «TCP keepalive» для исходящих соединений к проксируемому серверу.

`""`	По умолчанию для сокета действуют настройки операционной системы.
`on`	для сокета включается параметр *SO_KEEPALIVE*

proxy_ssl

Синтаксис	`proxy_ssl` on | off;
По умолчанию	`proxy_ssl off;`
Контекст	stream, server

Включает протоколы SSL/TLS для соединений с проксируемым сервером.

proxy_ssl_certificate

Синтаксис	`proxy_ssl_certificate` *файл* [*файл*];
По умолчанию	—
Контекст	stream, server

Задает файл с сертификатом в формате PEM для аутентификации на проксируемом сервере. В имени файла можно использовать переменные.

Добавлено в версии 1.2.0.

При включенном *proxy_ssl_ntls* директива принимает два аргумента вместо одного:

```
server {
    proxy_ssl_ntls  on;

    proxy_ssl_certificate      sign.crt enc.crt;
    proxy_ssl_certificate_key  sign.key enc.key;

    proxy_ssl_ciphers "ECC-SM2-WITH-SM4-SM3:ECDHE-SM2-WITH-SM4-SM3:RSA";

    proxy_pass backend:12345;
}
```

proxy_ssl_certificate_key

Синтаксис	`proxy_ssl_certificate_key` *файл* [*файл*];
По умолчанию	—
Контекст	stream, server

Задает файл с секретным ключом в формате PEM для аутентификации на проксируемом сервере. В имени файла можно использовать переменные.

Добавлено в версии 1.2.0.

При включенном *proxy_ssl_ntls* директива принимает два аргумента вместо одного:

```
server {
    proxy_ssl_ntls  on;

    proxy_ssl_certificate      sign.crt enc.crt;
    proxy_ssl_certificate_key  sign.key enc.key;

    proxy_ssl_ciphers "ECC-SM2-WITH-SM4-SM3:ECDHE-SM2-WITH-SM4-SM3:RSA";

    proxy_pass backend:12345;
}
```

proxy_ssl_ciphers

Синтаксис	`proxy_ssl_ciphers` *шифры*;
По умолчанию	`proxy_ssl_ciphers DEFAULT;`
Контекст	stream, server

Описывает разрешенные шифры для запросов к проксируемому серверу. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL.

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

proxy_ssl_conf_command

Синтаксис	`proxy_ssl_conf_command` *имя значение*;
По умолчанию	—
Контекст	stream, server

Задает произвольные конфигурационные команды OpenSSL при установлении соединения с проксируемым сервером.

Важно

Директива поддерживается при использовании OpenSSL 1.0.2 и выше.

На одном уровне может быть указано несколько директив *proxy_ssl_conf_command*. Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *proxy_ssl_conf_command*.

Осторожно

Следует учитывать, что изменение настроек OpenSSL напрямую может привести к неожиданному поведению.

proxy_ssl_crl

Синтаксис	`proxy_ssl_crl` *файл*;
По умолчанию	—
Контекст	stream, server

Указывает файл с отозванными сертификатами (CRL) в формате PEM, используемыми при *проверке* сертификата проксируемого сервера.

proxy_ssl_name

Синтаксис	`proxy_ssl_name` *имя*;
По умолчанию	`proxy_ssl_name` *хост из* `proxy_pass;`
Контекст	stream, server

Позволяет переопределить имя сервера, используемое при *проверке* сертификата проксируемого сервера, а также для *передачи его через SNI* при установлении соединения с проксируемым сервером. Имя сервера можно также задать с помощью переменных.

По умолчанию используется имя хоста из адреса, заданного директивой *proxy_pass*.

proxy_ssl_ntls

Добавлено в версии 1.2.0.

Синтаксис	`proxy_ssl_ntls on | off;`
По умолчанию	`proxy_ssl_ntls off;`
Контекст	stream, server

Включает клиентскую поддержку NTLS при использовании TLS библиотеки TongSuo.

```
server {
    proxy_ssl_ntls  on;

    proxy_ssl_certificate      sign.crt enc.crt;
    proxy_ssl_certificate_key  sign.key enc.key;

    proxy_ssl_ciphers "ECC-SM2-WITH-SM4-SM3:ECDHE-SM2-WITH-SM4-SM3:RSA";

    proxy_pass backend:12345;
}
```

Важно

Angie PRO необходимо собрать с использованием параметра конфигурации *–with-ntls*, с соответствующей SSL библиотекой с поддержкой NTLS

```
./configure --with-openssl=../Tongsuo-8.3.0 \
            --with-openssl-opt=enable-ntls  \
            --with-ntls
```

proxy_ssl_password_file

Синтаксис	`proxy_ssl_password_file` *файл*;
По умолчанию	—
Контекст	stream, server

Задает файл с паролями от *секретных ключей*, где каждый пароль указан на отдельной строке. Пароли применяются по очереди в момент загрузки ключа.

proxy_ssl_protocols

Синтаксис	`proxy_ssl_protocols` [SSLv2] [SSLv3] [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`proxy_ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;`
Контекст	stream, server

Изменено в версии 1.2.0: Параметр `TLSv1.3` добавлен к используемым по умолчанию.

Разрешает указанные протоколы для соединений с проксируемым сервером.

proxy_ssl_server_name

Синтаксис	`proxy_ssl_server_name` on | off;
По умолчанию	`proxy_ssl_server_name off;`
Контекст	stream, server

Разрешает или запрещает передачу имени сервера, заданного директивой *proxy_ssl_name*, через расширение Server Name Indication протокола TLS (SNI, RFC 6066) при установлении соединения с проксируемым сервером.

proxy_ssl_session_reuse

Синтаксис	`proxy_ssl_session_reuse` on | off;
По умолчанию	`proxy_ssl_session_reuse on;`
Контекст	stream, server

Определяет, использовать ли повторно SSL-сессии при работе с проксируемым сервером. Если в логах появляются ошибки «*SSL3_GET_FINISHED:digest check failed*», то можно попробовать выключить повторное использование сессий.

proxy_ssl_trusted_certificate

Синтаксис	`proxy_ssl_trusted_certificate` *файл*;
По умолчанию	—
Контекст	stream, server

Задает файл с доверенными сертификатами CA в формате PEM, используемыми при *проверке* сертификата проксируемого HTTPS-сервера.

proxy_ssl_verify

Синтаксис	`proxy_ssl_verify` on | off;
По умолчанию	`proxy_ssl_verify off;`
Контекст	stream, server

Разрешает или запрещает проверку сертификата проксируемого сервера.

proxy_ssl_verify_depth

Синтаксис	`proxy_ssl_verify_depth` *число*;
По умолчанию	`proxy_ssl_verify_depth 1;`
Контекст	stream, server

Устанавливает глубину проверки в цепочке сертификатов проксируемого сервера.

proxy_timeout

Синтаксис	`proxy_timeout` *время*;
По умолчанию	`proxy_timeout 10m;`
Контекст	stream, server

Задает таймаут между двумя идущими подряд операциями чтения или записи на клиентском соединении или соединении с проксируемым сервером. Если по истечении этого времени данные не передавались, соединение закрывается.

upstream_probe_timeout (PRO)

Добавлено в версии 1.4.0: PRO

Синтаксис	`upstream_probe_timeout` *время*;
По умолчанию	`upstream_probe_timeout 50s;`
Контекст	server

Задает максимальное *время* бездействия установленного с сервером соединения для проверок, настроенных с помощью директивы *upstream_probe (PRO)*; при превышении этого предела соединение будет закрыто.

proxy_upload_rate

Синтаксис	`proxy_upload_rate` *скорость*;
По умолчанию	`proxy_upload_rate 0;`
Контекст	stream, server

Ограничивает скорость чтения данных от клиента. Скорость задается в байтах в секунду.

0	отключает ограничение скорости

Примечание

Ограничение устанавливается на соединение, поэтому, если клиент одновременно откроет два соединения, суммарная скорость будет вдвое выше заданного ограничения.

В значении параметра можно использовать переменные. Это может быть полезно в случаях, когда скорость нужно ограничивать в зависимости от какого-либо условия:

proxy_upload_rate $rate;

```
map $slow $rate {
    1     4k;
    2     8k;
}

proxy_upload_rate $rate;
```

RDP Preread

При использовании протокола RDP позволяет извлекать cookie, которые используются для идентификации и управления сессиями, до момента принятия решения о балансировке.

При сборке из исходного кода модуль необходимо включить с помощью параметра сборки `--with-stream_rdp_preread_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

Привязка к выдавшему cookie серверу

Конфигурация использует режим `learn` директивы *sticky*:

```
stream {

    rdp_preread on;

    upstream rdp {

        server 127.0.0.1:3390 sid=a;
        server 127.0.0.1:3391 sid=b;

        sticky learn lookup=$rdp_cookie create=$rdp_cookie zone=sessions:1m;
    }
}
```

Директивы

rdp_preread

Синтаксис	`rdp_preread` on | off;
По умолчанию	`rdp_preread off;`
Контекст	stream, server

Управляет извлечением информации из cookie протокола RDP на этапе *предварительного чтения*. Если параметр включен (`on`), то в контексте, где он задан, заполняются перечисленные ниже переменные.

Встроенные переменные

Семантика значений в составе cookie зависит от версии протокола RDP.

`$rdp_cookie`

Значение cookie целиком.

`$rdp_cookie_` ***имя***

Значение поля cookie с заданным именем.

RealIP

Позволяет менять адрес и порт клиента на переданные в заголовке протокола PROXY. Протокол PROXY должен быть предварительно включен при помощи установки параметра *proxy_protocol* в директиве *listen*.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-stream_realip_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
listen 12345 proxy_protocol;

set_real_ip_from  192.168.1.0/24;
set_real_ip_from  192.168.2.1;
set_real_ip_from  2001:0db8::/32;
```

Директивы

set_real_ip_from

Синтаксис	`set_real_ip_from` *адрес* | *CIDR* | unix:;
По умолчанию	—
Контекст	stream, server

Задает доверенные адреса, которые передают верный адрес для замены. Если указано специальное значение `unix:`, доверенными будут считаться все UNIX-сокеты.

Встроенные переменные

`$realip_remote_addr`

хранит исходный адрес клиента

`$realip_remote_port`

хранит исходный порт клиента

Return

Позволяет отправить заданное значение клиенту и после этого закрыть соединение.

Пример конфигурации

```
server {
    listen 12345;
    return $time_iso8601;
}
```

Директивы

return

Синтаксис	`return` *значение*;
По умолчанию	—
Контекст	server

Задает значение, отправляемое клиенту. В качестве значения можно использовать текст, переменные и их комбинации.

Set

Позволяет устанавливать значение переменной.

Пример конфигурации

```
server {
    listen 12345;
    set    $true 1;
}
```

Директивы

set

Синтаксис	`set` *$переменная значение*;
По умолчанию	—
Контекст	server

Устанавливает значение указанной переменной. В качестве значения можно использовать текст, переменные и их комбинации.

Split Clients

Модуль генерирует переменные для A/B-тестирования, канареечных релизов и других сценариев, которые направляют определенный процент клиентов на один сервер или конфигурацию, а остальных — куда-то еще.

Пример конфигурации

```
stream {
    # ...
    split_clients "${remote_addr}AAA" $upstream {
                  0.5%                feature_test1;
                  2.0%                feature_test2;
                  *                   production;
    }

    server {
        # ...
        proxy_pass $upstream;
    }
}
```

Директивы

split_clients

Синтаксис	`split_clients` *строка $переменная* { ... }
По умолчанию	—
Контекст	stream

Создает *$переменную*, хэшируя *строку*; переменные в *строке* подставляются, результат хэшируется, затем по значению хэша выбирается строковое значение *$переменной*.

Функция хэширования использует MurmurHash2 (32 бит), и весь диапазон ее значений (с 0 по 4294967295) сопоставляется с корзинами в порядке появления; процентные величины определяют размер корзин. В конце может стоять метасимвол (`*`); хэши, не попавшие в другие корзины, сопоставляются с приданным ему значением.

Пример:

```
split_clients "${remote_addr}AAA" $variant {
               0.5%               .one;
               2.0%               .two;
               *                  "";
}
```

Здесь после подстановки в строке `$remote_addrAAA` значения хэша распределяются следующим образом:

- значения от 0 до 21474835 (0,5%) дают `.one`;
- значения от 21474836 до 107374180 (2%) дают `.two`;
- значения от 107374181 до 4294967295 (все остальные) дают `""` (пустую строку).

SSL

Обеспечивает необходимую поддержку для работы прокси-сервера по протоколу SSL/TLS.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-stream_ssl_module`.

В пакетах и образах из наших репозиториев модуль включен в сборку.

> **Важно**
>
> Для этого модуля нужна библиотека OpenSSL.

Пример конфигурации

Для уменьшения загрузки процессора рекомендуется

- установить число *рабочих процессов* равным числу процессоров,
- включить *разделяемый кэш* сессий,
- выключить *встроенный кэш* сессий
- и, возможно, увеличить *время жизни* сессии (по умолчанию 5 минут):

```
worker_processes auto;

stream {

    #...

    server {
        listen              12345 ssl;

        ssl_protocols       TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
        ssl_ciphers         AES128-SHA:AES256-SHA:RC4-SHA:DES-CBC3-SHA:RC4-MD5;
        ssl_certificate     /usr/local/angie/conf/cert.pem;
        ssl_certificate_key /usr/local/angie/conf/cert.key;
        ssl_session_cache   shared:SSL:10m;
        ssl_session_timeout 10m;

    #    ...
    }
```

Директивы

ssl_alpn

Синтаксис	`ssl_alpn` *протокол* ...;
По умолчанию	—
Контекст	stream, server

Задает список поддерживаемых протоколов ALPN. Один из протоколов должен быть *согласован*, если клиент использует ALPN:

```
map $ssl_alpn_protocol $proxy {
    h2                  127.0.0.1:8001;
    http/1.1            127.0.0.1:8002;
}

server {
    listen      12346;
    proxy_pass  $proxy;
    ssl_alpn    h2 http/1.1;
}
```

ssl_certificate

Синтаксис	`ssl_certificate` *файл*;
По умолчанию	—
Контекст	stream, server

Указывает файл с сертификатом в формате PEM для данного сервера. Если вместе с основным сертификатом нужно указать промежуточные, то они должны находиться в этом же файле в следующем порядке — сначала основной сертификат, а затем промежуточные. В этом же файле может находиться секретный ключ в формате PEM.

Директива может быть указана несколько раз для загрузки сертификатов разных типов, например RSA и ECDSA:

```
server {
    listen              12345 ssl;

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

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

#    ...
}
```

Возможность задавать отдельные цепочки сертификатов для разных сертификатов есть только в OpenSSL 1.0.2 и выше. Для более старых версий следует указывать только одну цепочку сертификатов.

Важно

В имени файла можно использовать переменные при использовании OpenSSL 1.0.2 и выше:

```
ssl_certificate     $ssl_server_name.crt;
ssl_certificate_key $ssl_server_name.key;
```

При использовании переменных сертификат загружается при каждой операции SSL-рукопожатия, что может отрицательно влиять на производительность.

Вместо `файла` можно указать значение «data:*$переменная*», при котором сертификат загружается из переменной без использования промежуточных файлов.

Ненадлежащее использование подобного синтаксиса может быть небезопасно, например данные секретного ключа могут попасть в *лог ошибок*.

ssl_certificate_key

Синтаксис	`ssl_certificate_key` *файл*;
По умолчанию	—
Контекст	stream, server

Указывает файл с секретным ключом в формате PEM для данного виртуального сервера.

Важно

В имени файла можно использовать переменные при использовании OpenSSL 1.0.2 и выше.

Вместо `файла` можно указать значение «engine:*имя*:id», которое загружает ключ с указанным *id* из OpenSSL engine с заданным именем.

Вместо `файла` также можно указать значение «data:*$переменная*», при котором секретный ключ загружается из переменной без использования промежуточных файлов. При этом следует учитывать, что ненадлежащее использование подобного синтаксиса может быть небезопасно, например данные секретного ключа могут попасть в *лог ошибок*.

ssl_ciphers

Синтаксис	`ssl_ciphers` *шифры*;
По умолчанию	`ssl_ciphers HIGH:!aNULL:!MD5;`
Контекст	stream, server

Описывает разрешенные шифры. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL, например:

```
ssl_ciphers ALL:!aNULL:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
```

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

ssl_client_certificate

Синтаксис	`ssl_client_certificate` *файл*;
По умолчанию	—
Контекст	stream, server

Указывает файл с доверенными сертификатами CA в формате PEM, которые используются для *проверки* клиентских сертификатов.

Список сертификатов будет отправляться клиентам. Если это нежелательно, можно воспользоваться директивой *ssl_trusted_certificate*.

ssl_conf_command

Синтаксис	`ssl_conf_command` *имя значение*;
По умолчанию	—
Контекст	stream, server

Задает произвольные конфигурационные команды OpenSSL.

Важно

Директива поддерживается при использовании OpenSSL 1.0.2 и выше.

На одном уровне может быть указано несколько директив *ssl_ conf_ command*:

```
ssl_conf_command Options PrioritizeChaCha;
ssl_conf_command Ciphersuites TLS_CHACHA20_POLY1305_SHA256;
```

Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *ssl_ conf_ command*.

Осторожно

Изменение настроек OpenSSL напрямую может привести к неожиданному поведению.

ssl_crl

Синтаксис	`ssl_crl` *файл*;
По умолчанию	—
Контекст	stream, server

Указывает файл с отозванными сертификатами (CRL) в формате PEM, используемыми для *проверки* клиентских сертификатов.

ssl_dhparam

Синтаксис	`ssl_dhparam` *файл*;
По умолчанию	—
Контекст	stream, server

Указывает файл с параметрами для DHE-шифров.

Осторожно

По умолчанию параметры не заданы, и соответственно DHE-шифры не будут использоваться.

ssl_ecdh_curve

Синтаксис	`ssl_ecdh_curve` *кривая*;
По умолчанию	`ssl_ecdh_curve auto;`
Контекст	stream, server

Задает кривую для ECDHE-шифров.

Важно

При использовании OpenSSL 1.0.2 и выше можно указывать несколько кривых, например:

```
ssl_ecdh_curve prime256v1:secp384r1;
```

Специальное значение `auto` соответствует встроенному в библиотеку OpenSSL списку кривых для OpenSSL 1.0.2 и выше, или *prime256v1* для более старых версий.

Важно

При использовании OpenSSL 1.0.2 и выше директива задает список кривых, поддерживаемых сервером. Поэтому для работы ECDSA-сертификатов важно, чтобы список включал кривые, используемые в сертификатах.

ssl_handshake_timeout

Синтаксис	`ssl_handshake_timeout` *время*;
По умолчанию	`ssl_handshake_timeout 60s;`
Контекст	stream, server

Задает таймаут для завершения операции SSL-рукопожатия.

ssl_ntls

Добавлено в версии 1.2.0.

Синтаксис	`ssl_ntls` on | off;
По умолчанию	`ssl_ntls off;`
Контекст	stream, server

Включает серверную поддержку NTLS при использовании TLS библиотеки TongSuo

```
listen ... ssl;
ssl_ntls  on;
```

Важно

Angie PRO необходимо собрать с использованием параметра конфигурации *–with-ntls*, с соответствующей SSL библиотекой с поддержкой NTLS

```
./configure --with-openssl=../Tongsuo-8.3.0 \
            --with-openssl-opt=enable-ntls  \
            --with-ntls
```

ssl_password_file

Синтаксис	`ssl_password_file` *файл*;
По умолчанию	—
Контекст	stream, server

Задает файл с паролями от *секретных ключей*, где каждый пароль указан на отдельной строке. Пароли применяются по очереди в момент загрузки ключа.

Пример:

```
stream {
    ssl_password_file /etc/keys/global.pass;
    ...

    server {
        listen 127.0.0.1:12345;
        ssl_certificate_key /etc/keys/first.key;
    }

    server {
        listen 127.0.0.1:12346;

        # вместо файла можно указать именованный канал
        ssl_password_file /etc/keys/fifo;
        ssl_certificate_key /etc/keys/second.key;
    }
}
```

ssl_prefer_server_ciphers

Синтаксис	`ssl_prefer_server_ciphers` on | off;
По умолчанию	`ssl_prefer_server_ciphers off;`
Контекст	stream, server

При использовании протоколов SSLv3 и TLS устанавливает приоритет серверных шифров над клиентскими.

ssl_protocols

Синтаксис	`ssl_protocols` [SSLv2] [SSLv3] [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;`
Контекст	stream, server

Изменено в версии 1.2.0: Параметр `TLSv1.3` добавлен к используемым по умолчанию.

Разрешает указанные протоколы.

Важно

Параметры TLSv1.1 и TLSv1.2 работают только при использовании OpenSSL 1.0.1 и выше.

Параметр TLSv1.3 работает только при использовании OpenSSL 1.1.1 и выше.

ssl_session_cache

Синтаксис	`ssl_session_cache` off | none | [builtin[:*размер*]] [shared:*название*:*размер*];
По умолчанию	`ssl_session_cache none;`
Контекст	stream, server

Задает тип и размеры кэшей для хранения параметров сессий. Тип кэша может быть следующим:

`off`	жесткое запрещение использования кэша сессий: Angie PRO явно сообщает клиенту, что сессии не могут использоваться повторно.
`none`	мягкое запрещение использования кэша сессий: Angie PRO сообщает клиенту, что сессии могут использоваться повторно, но на самом деле не хранит параметры сессии в кэше.
`builtin`	встроенный в OpenSSL кэш, используется в рамках только одного рабочего процесса. Размер кэша задается в сессиях. Если размер не задан, то он равен 20480 сессиям. Использование встроенного кэша может вести к фрагментации памяти.
`shared`	кэш, разделяемый между всеми рабочими процессами. Размер кэша задается в байтах, в 1 мегабайт может поместиться около 4000 сессий. У каждого разделяемого кэша должно быть произвольное название. Кэш с одинаковым названием может использоваться в нескольких серверах. Также он используется для автоматического создания, хранения и периодического обновления ключей TLS session tickets, если они не указаны явно с помощью директивы *ssl_session_ticket_key*.

Можно использовать одновременно оба типа кэша, например:

```
ssl_session_cache builtin:1000 shared:SSL:10m;
```

однако использование только разделяемого кэша без встроенного должно быть более эффективным.

ssl_session_ticket_key

Синтаксис	`ssl_session_ticket_key` *файл*;
По умолчанию	—
Контекст	stream, server

Задает файл с секретным ключом, применяемым при шифровании и расшифровании TLS session tickets. Директива необходима, если один и тот же ключ нужно использовать на нескольких серверах. По умолчанию используется случайно сгенерированный ключ.

Если указано несколько ключей, то только первый ключ используется для шифрования TLS session tickets. Это позволяет настроить ротацию ключей, например:

```
ssl_session_ticket_key current.key;
ssl_session_ticket_key previous.key;
```

Файл должен содержать 80 или 48 байт случайных данных и может быть создан следующей командой:

```
openssl rand 80 > ticket.key
```

В зависимости от размера файла для шифрования будет использоваться либо AES256 (для 80-байтных ключей), либо AES128 (для 48-байтных ключей).

ssl_session_tickets

Синтаксис	`ssl_session_tickets` on | off;
По умолчанию	`ssl_session_tickets on;`
Контекст	stream, server

Разрешает или запрещает возобновление сессий при помощи TLS session tickets.

ssl_session_timeout

Синтаксис	`ssl_session_timeout` *время*;
По умолчанию	`ssl_session_timeout 5m;`
Контекст	stream, server

Задает время, в течение которого клиент может повторно использовать параметры сессии.

ssl_trusted_certificate

Синтаксис	`ssl_trusted_certificate` *файл*;
По умолчанию	—
Контекст	stream, server

Задает файл с доверенными сертификатами CA в формате PEM, которые используются для *проверки* клиентских сертификатов.

В отличие от *ssl_client_certificate*, список этих сертификатов не будет отправляться клиентам.

ssl_verify_client

Синтаксис	`ssl_verify_client` on | off | optional | optional_no_ca;
По умолчанию	`ssl_verify_client off;`
Контекст	stream, server

Разрешает проверку клиентских сертификатов. Результат проверки доступен через переменную *$ssl_client_verify*. Если при проверке клиентского сертификата произошла ошибка или клиент не предоставил требуемый сертификат, соединение закрывается.

`optional`	запрашивает клиентский сертификат, и если сертификат был предоставлен, проверяет его
`optional_no_ca`	запрашивает сертификат клиента, но не требует, чтобы он был подписан доверенным сертификатом CA. Это предназначено для случаев, когда фактическая проверка сертификата осуществляется внешним по отношению к Angie PRO сервисом.

ssl_verify_depth

Синтаксис	`ssl_verify_depth` *число*;
По умолчанию	`ssl_verify_depth 1;`
Контекст	stream, server

Устанавливает глубину проверки в цепочке клиентских сертификатов.

Встроенные переменные

Модуль *stream_ssl* поддерживает встроенные переменные:

`$ssl_alpn_protocol`

возвращает протокол, выбранный при помощи ALPN во время SSL-рукопожатия, либо пустую строку.

`$ssl_cipher`

возвращает название используемого шифра для установленного SSL-соединения.

`$ssl_ciphers`

возвращает список шифров, поддерживаемых клиентом. Известные шифры указаны по имени, неизвестные указаны в шестнадцатеричном виде, например:

AES128-SHA:AES256-SHA:0x00ff

Важно

Переменная полностью поддерживается при использовании OpenSSL версии 1.0.2 и выше. При использовании более старых версий переменная доступна только для новых сессий и может содержать только известные шифры.

`$ssl_client_cert`

возвращает клиентский сертификат для установленного SSL-соединения в формате PEM перед каждой строкой которого, кроме первой, вставляется символ табуляции.

`$ssl_client_fingerprint`

возвращает SHA1-отпечаток клиентского сертификата для установленного SSL-соединения.

`$ssl_client_i_dn`

возвращает строку «issuer DN» клиентского сертификата для установленного SSL-соединения согласно RFC 2253.

`$ssl_client_raw_cert`

возвращает клиентский сертификат для установленного SSL-соединения в формате PEM.

`$ssl_client_s_dn`

возвращает строку «subject DN» клиентского сертификата для установленного SSL-соединения согласно RFC 2253.

`$ssl_client_serial`

возвращает серийный номер клиентского сертификата для установленного SSL-соединения.

`$ssl_client_v_end`

возвращает дату окончания срока действия клиентского сертификата.

`$ssl_client_v_remain`

возвращает число дней, оставшихся до истечения срока действия клиентского сертификата.

`$ssl_client_v_start`

возвращает дату начала срока действия клиентского сертификата.

`$ssl_client_verify`

возвращает результат проверки клиентского сертификата: `SUCCESS`, «*FAILED:reason*» и, если сертификат не был предоставлен, `NONE`.

`$ssl_curve`

возвращает согласованную кривую, использованную для обмена ключами во время SSL-рукопожатия. Известные кривые указаны по имени, неизвестные указаны в шестнадцатеричном виде, например:

prime256v1

Важно

Переменная поддерживается при использовании OpenSSL версии 3.0 и выше. При использовании более старых версий значением переменной будет пустая строка.

`$ssl_curves`

возвращает список кривых, поддерживаемых клиентом. Известные кривые указаны по имени, неизвестные указаны в шестнадцатеричном виде, например:

0x001d:prime256v1:secp521r1:secp384r1

Важно

Переменная поддерживается при использовании OpenSSL версии 1.0.2 и выше. При использовании более старых версий значением переменной будет пустая строка.

Переменная доступна только для новых сессий.

`$ssl_protocol`

возвращает протокол установленного SSL-соединения.

`$ssl_server_cert_type`

принимает значения `RSA`, `DSA`, `ECDSA`, `ED448`, `ED25519`, `SM2`, `RSA-PSS` или `unknown` в зависимости от типа сертификата и ключа сервера.

`$ssl_server_name`

возвращает имя сервера, запрошенное через SNI.

`$ssl_session_id`

возвращает идентификатор сессии установленного SSL-соединения.

`$ssl_session_reused`

возвращает `r`, если сессия была использована повторно, иначе «.».

SSL Preread

Позволяет извлекать информацию из сообщения ClientHello без терминирования SSL/TLS, например имя сервера, запрошенное через SNI, или протоколы, указанные в ALPN.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-stream_ssl_preread_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

Выбор апстрима по имени сервера

```
map $ssl_preread_server_name $name {
    backend.example.com      backend;
    default                  backend2;
}

upstream backend {
    server 192.168.0.1:12345;
    server 192.168.0.2:12345;
}

upstream backend2 {
    server 192.168.0.3:12345;
    server 192.168.0.4:12345;
}

server {
    listen      12346;
    proxy_pass  $name;
```

```
    ssl_preread on;
}
```

Выбор сервера по протоколу

```
map $ssl_preread_alpn_protocols $proxy {
    ~\bh2\b           127.0.0.1:8001;
    ~\bhttp/1.1\b     127.0.0.1:8002;
    ~\bxmpp-client\b  127.0.0.1:8003;
}

server {
    listen      9000;
    proxy_pass  $proxy;
    ssl_preread on;
}
```

Выбор сервера по версии протокола SSL

```
map $ssl_preread_protocol $upstream {
    ""        ssh.example.com:22;
    "TLSv1.2" new.example.com:443;
    default   tls.example.com:443;
}

# ssh и https на одном порту
server {
    listen      192.168.0.1:443;
    proxy_pass  $upstream;
    ssl_preread on;
}
```

Директивы

ssl_preread

Синтаксис	`ssl_preread` on | off;
По умолчанию	`ssl_preread off;`
Контекст	stream, server

Разрешает извлекать информацию из сообщения ClientHello на этапе *предварительного чтения*.

Встроенные переменные

`$ssl_preread_protocol`

Максимальная версия протокола SSL, поддерживаемая клиентом.

`$ssl_preread_server_name`

Имя сервера, запрошенное через SNI.

`$ssl_preread_alpn_protocols`

Список протоколов, переданный клиентом через ALPN. Значения разделяются запятыми.

Upstream

Предоставляет контекст для описания группы серверов, которые могут использоваться в директиве *proxy_pass*.

Пример конфигурации

```
upstream backend {
    hash $remote_addr consistent;
    zone backend 1m;

    server backend1.example.com:1935  weight=5;
    server unix:/tmp/backend3;
    server backend3.example.com       service=_example._tcp resolve;

    server backup1.example.com:1935   backup;
    server backup2.example.com:1935   backup;
}

resolver 127.0.0.53 status_zone=resolver;

server {
    listen 1936;
    proxy_pass backend;
}
```

Директивы

upstream

Синтаксис	`upstream` *имя* { ... }
По умолчанию	—
Контекст	stream

Описывает группу серверов. Серверы могут слушать на разных портах. Кроме того, можно одновременно использовать серверы, слушающие на TCP- и UNIX-сокетах.

Пример:

```
upstream backend {
    server backend1.example.com:1935 weight=5;
    server 127.0.0.1:1935            max_fails=3 fail_timeout=30s;
    server unix:/tmp/backend2;
    server backend3.example.com:1935 resolve;

    server backup1.example.com:1935  backup;
}
```

По умолчанию соединения распределяются по серверам циклически (в режиме round-robin) с учетом весов серверов. В вышеприведенном примере каждые 7 соединений будут распределены так: 5 соединений на backend1.example.com:1935 и по одному соединению на второй и третий серверы.

Если при попытке работы с сервером происходит ошибка, то соединение передается следующему серверу, и так далее до тех пор, пока не будут опробованы все работающие серверы. Если связь с серверами не удалась, соединение будет закрыто.

server

Синтаксис	`server` *адрес* [*параметры*];
По умолчанию	—
Контекст	upstream

Задает адрес и другие параметры сервера. Адрес может быть указан в виде доменного имени или IP-адреса, и обязательного порта, или в виде пути UNIX-сокета, который указывается после префикса `unix:`. Доменное имя, которому соответствует несколько IP-адресов, задает сразу несколько серверов.

Могут быть заданы следующие параметры:

`weight=`*число*	задает вес сервера по умолчанию 1.
`max_conns=`*число*	ограничивает максимальное число одновременных активных соединений к проксируемому серверу. Значение по умолчанию равно `0` и означает, что ограничения нет. Если группа не находится в *зоне* разделяемой памяти, то ограничение работает отдельно для каждого рабочего процесса.

`max_fails=`*число* — задает число неудачных попыток связи с сервером, которые должны произойти в течение заданного *fail_ timeout* времени для того, чтобы сервер считался недоступным; после этого он будет повторно проверен через то же самое время.

В данном случае неудачной попыткой считается ошибка или таймаут при установке соединения с сервером.

Примечание

Если директива `server` в группе разрешается в несколько серверов, ее настройка `max_fails` применяется к каждому серверу отдельно.

Если после разрешения всех директив `server` в апстриме остается только один сервер, настройка `max_fails` не действует и будет проигнорирована.

`max_fails=1`	число попыток по умолчанию
`max_fails=0`	отключает учет попыток

`fail_timeout=`*время* — задает:

`fail_timeout=`*время* — задает период времени, в течение которого должно произойти определенное число неудачных попыток связи с сервером (*max_fails*), чтобы сервер считался недоступным. Затем сервер остается недоступным в течение того же самого времени, прежде чем будет проверен повторно.

Значение по умолчанию — 10 секунд.

Примечание

Если директива `server` в группе разрешается в несколько серверов, ее настройка `fail_timeout` применяется к каждому серверу отдельно.

Если после разрешения всех директив `server` в апстриме остается только один сервер, настройка `fail_timeout` не действует и будет проигнорирована.

`backup`	помечает сервер как запасной. На него будут передаваться запросы в случае, если не работают основные серверы.
`down`	помечает сервер как постоянно недоступный.
`drain`	помечает сервер как разгружаемый (draining); это значит, что он получает только запросы сессий, привязанных ранее через *sticky*. В остальном поведение такое же, как в режиме `down`.

Осторожно

Параметр `backup` нельзя использовать совместно с методами балансировки нагрузки *hash* и *random*.

Параметры `down` и `drain` взаимно исключающие.

Добавлено в версии 1.3.0.

`resolve`	Позволяет отслеживать изменения списка IP-адресов, соответствующего доменному имени, и обновлять его без перезагрузки конфигурации. При этом группа должна находиться в *зоне разделяемой памяти*; также должен быть определен *преобразователь имен в адреса*.
`service=`*имя*	Включает преобразование SRV-записей DNS и задает имя сервиса. При указании этого параметра необходимо также задать параметр *resolve*, не указывая порт сервера при имени хоста. Если в имени службы нет точек, формируется имя по стандарту RFC: к имени службы добавляется префикс `_`, затем через точку добавляется `_tcp`. Так, имя службы `http` даст в результате `_http._tcp`. Angie PRO разрешает SRV-записи, объединяя нормализованное имя службы и имя хоста и получая список серверов для полученной комбинации через DNS, вместе с их приоритетами и весами. • SRV-записи с наивысшим приоритетом (те, которые имеют минимальное значение приоритета) разрешаются как основные серверы, а прочие записи становятся запасными серверами. Если `backup` установлено с `server`, SRV-записи с наивысшим приоритетом разрешаются как запасные серверы, а прочие записи игнорируются. • Вес аналогичен параметру `weight` директивы `server`. Если вес задан как в самой директиве, так и в SRV-записи, используется вес, установленный в директиве.

В этом примере выполняется поиск записи `_http._tcp.backend.example.com`:

```
server backend.example.com service=http resolve;
```

Добавлено в версии 1.4.0.

`slow_start=`*время*	задает *время* восстановления веса сервера, возвращающегося к работе при балансировке нагрузки методом *round-robin* или *least_conn*. Если параметр задан и сервер после сбоя снова считается работающим с точки зрения *max_fails* и *upstream_probe (PRO)*, то такой сервер равномерно набирает указанный для него вес в течение заданного времени. Если параметр не задан, то в аналогичной ситуации сервер сразу начинает работу с указанным для него весом.

Примечание

Если в апстриме задан только один `server`, `slow_start` не работает и будет игнорироваться.

state (PRO)

Добавлено в версии 1.4.0: PRO

Синтаксис	`state` *файл*;
По умолчанию	—
Контекст	upstream

Указывает *файл*, где постоянно хранится список серверов апстрима. При установке из наших пакетов для хранения таких файлов специально создается каталог `/var/lib/angie/state/` (`/var/`

`db/angie/state/` во FreeBSD) с соответствующими правами доступа, и в конфигурации остается добавить лишь имя файла:

```
upstream backend {

    zone backend 1m;
    state /var/lib/angie/state/<ИМЯ ФАЙЛА>;
}
```

Список серверов здесь имеет формат, аналогичный `s_server`. Содержимое файла изменяется при любом изменении серверов в разделе */config/stream/upstreams/* через API конфигурации. Файл считывается при запуске Angie PRO или перезагрузке конфигурации.

Осторожно

Чтобы использовать директиву `state` в блоке `upstream`, в нем не должно быть директив `server`, но нужна зона разделяемой памяти (*zone*).

zone

Синтаксис	`zone` *имя* [*размер*];
По умолчанию	—
Контекст	upstream

Задает имя и размер зоны разделяемой памяти, в которой хранятся конфигурация группы и ее рабочее состояние, разделяемые между рабочими процессами. В одной и той же зоне могут быть сразу несколько групп. В этом случае достаточно указать размер только один раз.

feedback (PRO)

Добавлено в версии 1.7.0: PRO

Синтаксис	`feedback` *переменная* [inverse] [factor=*число*] [account=*условная_ переменная*];
По умолчанию	—
Контекст	upstream

Задает в `upstream` механизм балансировки нагрузки по обратной связи. Он динамически корректирует решения при балансировке, умножая вес каждого проксируемого сервера на среднее значение обратной связи, которое меняется с течением времени в зависимости от значения *переменной* и подчиняется необязательному условию.

Могут быть заданы следующие параметры:

`переменная`	Переменная, из которой берется значение обратной связи. Она должна представлять собой метрику производительности или состояния; предполагается, что ее передает сервер. Значение оценивается при каждом ответе от сервера и учитывается в скользящем среднем согласно настройкам `inverse` и `factor`.
`inverse`	Если параметр задан, значение обратной связи интерпретируется наоборот: более низкие значения указывают на лучшую производительность.
`factor`	Коэффициент, по которому значение обратной связи учитывается при расчете среднего. Допустимы целые числа от 0 до 99. По умолчанию — `90`. Среднее рассчитывается по формуле экспоненциального сглаживания. Чем больше коэффициент, тем меньше новые значения влияют на среднее; если указать `90`, то будет взято 90 % от предыдущего значения и лишь 10 % от нового.
`account`	Указывает условную переменную, которая контролирует, как соединения учитываются при расчете. Среднее значение обновляется с учетом значения обратной связи, только если условная переменная не равна `""` или `"0"`. **Примечание** По умолчанию трафик от *активных проверок* не включается в расчет; комбинация переменной *$upstream_probe* с `account` позволяет включить и их или даже исключить все остальное.

Пример:

```
upstream backend {

    zone backend 1m;

    feedback $feedback_value factor=80 account=$condition_value;

    server backend1.example.com:1935  weight=1;
    server backend2.example.com:1935  weight=2;
}

map $protocol $feedback_value {
    "TCP"                       100;
    "UDP"                       75;
    default                     10;
}

map $upstream_probe $condition_value {
    "high_priority" "1";
    "low_priority"  "0";
    default         "1";
}
```

Эта конфигурация категоризирует серверы по уровням обратной связи на основе протоколов, используемых в отдельных сессиях, а также добавляет условие на *$upstream_probe*, чтобы учитывать только активную проверку `high_priority` или обычные клиентские сессии.

hash

Синтаксис	`hash` *ключ* [consistent];
По умолчанию	—
Контекст	upstream

Задает метод балансировки нагрузки для группы, при котором соответствие клиента серверу определяется при помощи хэшированного значения ключа. В качестве ключа может использоваться текст, переменные и их комбинации. Пример использования:

```
hash $remote_addr;
```

Метод совместим с библиотекой Perl Cache::Memcached.

Если задан параметр `consistent`, то вместо вышеописанного метода будет использоваться метод консистентного хэширования ketama. Метод гарантирует, что при добавлении сервера в группу или его удалении на другие серверы будет перераспределено минимальное число ключей. Применение метода для кэширующих серверов обеспечивает больший процент попаданий в кэш. Метод совместим с библиотекой Perl Cache::Memcached::Fast при значении параметра ketama_points равным 160.

least_conn

Синтаксис	`least_conn`;
По умолчанию	—
Контекст	upstream

Задает для группы метод балансировки нагрузки, при котором соединение передается серверу с наименьшим числом активных соединений, с учетом весов серверов. Если подходит сразу несколько серверов, они выбираются циклически (в режиме round-robin) с учетом их весов.

least_time (PRO)

Синтаксис	`least_time` connect | first_byte | last_byte [factor=*number*] [account=*condition_variable*];
По умолчанию	—
Контекст	upstream

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

`connect`	Директива учитывает среднее время установки соединения.
`first_byte`	Директива использует среднее время получения первого байта ответа.
`last_byte`	Директива использует среднее время получения полного ответа.

Добавлено в версии 1.7.0: PRO

`factor`	Выполняет ту же функцию, что и *response_time_factor (PRO)*, и переопределяет его, если параметр задан.
`account`	Указывает условную переменную, которая контролирует, какие соединения учитываются при расчете. Среднее значение обновляется, только если условная переменная соединения не равна `""` или `"0"`. **Примечание** По умолчанию *активные проверки* не включаются в расчет; комбинация переменной *$upstream_probe* с `account` позволяет включить их или даже исключить все остальное.

Текущие средние значения, вычисленные с учетом `factor` и `account`, представлены также как `connect_time`, `first_byte_time` и `last_byte_time` в объекте `health` сервера среди *метрик апстрима* в API.

random

Синтаксис	`random` [two];
По умолчанию	—
Контекст	upstream

Задает для группы метод балансировки нагрузки, при котором соединение передается случайно выбранному серверу, с учетом весов серверов.

Если указан необязательный параметр `two`, Angie PRO случайным образом выбирает два сервера, из которых выбирает сервер, используя указанный метод. Методом по умолчанию является *least_conn*, при котором соединение передается на сервер с наименьшим количеством активных соединений.

response_time_factor (PRO)

Синтаксис	`response_time_factor` *число*;
По умолчанию	`response_time_factor 90;`
Контекст	upstream

Задает для метода балансировки нагрузки *least_time (PRO)* коэффициент сглаживания **предыдущего** значения при вычислении среднего времени ответа по формуле экспоненциально взвешенного скользящего среднего.

Чем больше указанное *число*, тем меньше новые значения влияют на среднее; если указать `90`, то будет взято 90 % от предыдущего значения и лишь 10 % от нового. Допустимые значения — от 0 до 99 включительно.

Текущие средние значения представлены как `connect_time` (время установления соединения), `first_byte_time` (время получения первого байта ответа) и `last_byte_time` (время получения ответа целиком) в объекте `health` сервера среди *метрик апстрима* в API.

Примечание

При подсчете учитываются только успешные ответы; что считать неуспешным ответом, определяют директивы *proxy_next_upstream*.

sticky

Добавлено в версии 1.6.0: Angie

Добавлено в версии 1.6.0: Angie PRO

Синтаксис	`sticky` route *$variable*...; `sticky` learn zone=*zone* create=*$create_var1*... lookup=*$lookup_var1*... [connect] [timeout=*time*];
По умолчанию	—
Контекст	upstream

Настраивает привязку клиентских сессий к проксируемым серверам в режиме, заданном первым параметром; для разгрузки серверов, у которых задана директива `sticky`, можно использовать опцию `drain` в блоке *server*.

Внимание

Директива `sticky` должна использоваться после всех директив, задающих тот или иной метод балансировки нагрузки, иначе она не будет работать.

Режим `route`

Этот режим использует предопределенные идентификаторы маршрутов, которые могут быть встроены в свойства соединения, доступные Angie PRO. Он менее гибок, так как зависит от предопределенных значений, но лучше подходит, если такие идентификаторы уже используются.

Здесь при установлении соединения проксируемый сервер может назначить клиенту маршрут и вернуть его идентификатор способом, известным им обоим. В качестве идентификатора маршрута должно использоваться значение параметра *sid* директивы *server*. Учтите, что параметр дополнительно хэшируется, если задана директива *sticky_secret*.

Последующие соединения от клиентов, желающих использовать этот маршрут, должны содержать выданный сервером идентификатор, причем так, чтобы он попал в переменные Angie PRO.

В параметрах директивы указываются переменные для маршрутизации. Чтобы выбрать сервер, куда направляется входящее соединение, используется первая непустая переменная; она затем сравнивается с параметром *sid* директивы *server*. Если выбрать сервер не удается или выбранный сервер не может принять соединение, то будет выбран другой сервер согласно настроенному методу балансировки.

Здесь Angie PRO ищет идентификатор маршрута в переменной `$route`, получающей значение на основе *$ssl_preread_server_name* (обратите внимание, что нужно включить *ssl_preread*):

```
stream {

    map $ssl_preread_server_name $route {

        a.example.com           a;
        b.example.com           b;
```

```
        default                   "";
    }

    upstream backend {

        server 127.0.0.1:8081 sid=a;
        server 127.0.0.1:8082 sid=b;

        sticky route $route;
    }

    server {

        listen 127.0.0.1:8080;

        ssl_preread on;

        proxy_pass backend;
    }
}
```

Режим `learn` (PRO)

В этом режиме для привязки клиента к конкретному проксируемому серверу используется динамически генерируемый ключ; он более гибок, так как назначает серверы на ходу, хранит сеансы в зоне общей памяти и поддерживает различные способы передачи идентификаторов сессий.

Здесь сессия создается на основе свойств соединения, идущих от проксируемого сервера. С параметрами `create` и `lookup` перечисляются переменные, указывающие, как создаются новые и ищутся существующие сессии. Оба параметра можно использовать по нескольку раз.

Идентификатором сессии служит значение первой непустой переменной, указанной с `create`; например, это может быть *имя проксируемого сервера*.

Сессии хранятся в зоне общей памяти; ее имя и размер задаются параметром `zone`. Если к сессии не было обращений в течение *времени* `timeout`, она удаляется. Значение по умолчанию — 1 час.

Последующие соединения от клиентов, желающих использовать сессию, должны содержать ее идентификатор, причем так, чтобы он попал в непустую переменную, указанную с `lookup`; тогда его значение будет сопоставлено с сессиями в общей памяти. Если выбрать сервер не удается или выбранный сервер не может обработать соединение, то будет выбран другой сервер согласно настроенному методу балансировки.

Параметр `connect` позволяет создать сессию сразу после получения заголовков ответа от проксируемого сервера. Без него сессия создается только после завершения обработки со.

В примере Angie PRO создает и ищет сессии, используя переменную *$rdp_ cookie*:

```
stream {

    upstream backend {

        server 127.0.0.1:3390 sid=a;
        server 127.0.0.1:3391 sid=b;

        sticky learn lookup=$rdp_cookie create=$rdp_cookie zone=sessions:1m;
    }

    server {

        listen 127.0.0.1:3389;
```

```
        ssl_preread on;

        proxy_pass backend;
    }
}
```

sticky_strict

Добавлено в версии 1.6.0: Angie

Добавлено в версии 1.6.0: Angie PRO

Синтаксис	`sticky_strict` on | off;
По умолчанию	`sticky_strict off;`
Контекст	upstream

При включении Angie PRO будет возвращать клиенту ошибку соединения, если желаемый сервер недоступен, вместо использования любого другого доступного сервера, как это происходит, когда в группе нет доступных серверов.

sticky_secret

Добавлено в версии 1.6.0: Angie

Добавлено в версии 1.6.0: Angie PRO

Синтаксис	`sticky_secret` *строка*;
По умолчанию	—
Контекст	upstream

Добавляет *строку* как соль в функцию MD5-хэширования для директивы *sticky* в режиме `route`. *Строка* может содержать переменные, например *$remote_addr*:

```
upstream backend {
    server 127.0.0.1:8081 sid=a;
    server 127.0.0.1:8082 sid=b;

    sticky route $route;
    sticky_secret my_secret.$remote_addr;
}
```

Соль добавляется после хэшируемого значения; чтобы независимо проверить механизм хэширования:

```
$ echo -n "<VALUE><SALT>" | md5sum
```

Встроенные переменные

Модуль `stream_upstream` поддерживает следующие встроенные переменные:

`$upstream_addr`

хранит IP-адрес и порт или путь к UNIX-сокету сервера группы. Если при проксировании были сделаны обращения к нескольким серверам, то их адреса разделяются запятой, например:

192.168.1.1:1935, 192.168.1.2:1935, unix:/tmp/sock»

Если сервер не может быть выбран, то переменная хранит *имя группы серверов*.

`$upstream_bytes_received`

число байт, полученных от сервера группы. Значения нескольких соединений разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_ addr*.

`$upstream_bytes_sent`

число байт, переданных на сервер группы. Значения нескольких соединений разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_ addr*.

`$upstream_connect_time`

хранит время, затраченное на установление соединения с сервером группы; время хранится в секундах с точностью до миллисекунд. Времена нескольких соединений разделяются запятыми и двоеточиями подобно адресам в переменной *$upstream_ addr*.

`$upstream_first_byte_time`

время получения первого байта данных; время хранится в секундах с точностью до миллисекунд. Времена нескольких соединений разделяются запятыми подобно адресам в переменной *$upstream_ addr*.

`$upstream_session_time`

длительность сессии в секундах с точностью до миллисекунд. Времена нескольких соединений разделяются запятыми подобно адресам в переменной *$upstream_ addr*.

`$upstream_sticky_status`

Статус соединений с привязкой.

`""`	Соединение направлено в группу серверов, где привязка не используется.
`NEW`	Соединение не содержит информации о привязке к серверу.
`HIT`	Соединение с привязкой направлено на желаемый сервер.
`MISS`	Соединение с привязкой направлено на сервер, выбранный по алгоритму балансировки.

Статусы из нескольких соединений разделяются запятыми и двоеточиями аналогично адресам в переменной *$upstream_addr*.

Upstream Probe

Реализует активные проверки работоспособности (health probes) для *Upstream*.

Пример конфигурации

```
server {
    listen ...;

    # ...
    proxy_pass backend;
    upstream_probe_timeout 1s;

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

Директивы

upstream_probe (PRO)

Добавлено в версии 1.4.0: PRO

Синтаксис	`upstream_probe` *имя* [port=*число*] [interval=*время*] [test=*условие*] [essential] [fails=*число*] [passes=*число*] [max_response=*размер*] [mode=always|idle|onfail] [udp] [send=*строка*];
По умолчанию	—
Контекст	server

Задает активную проверку работоспособности серверов *апстрима*, указанного в директиве *proxy_pass* в том же контексте `server`, где находится директива `upstream_probe`.

Сервер проходит проверку, если запрос к нему успешно выполняется с учетом всех параметров самой директивы `upstream_probe` и всех параметров, влияющих на использование апстримов тем контекстом `server`, где она задана, в том числе директивы *proxy_next_upstream*.

Чтобы использовать проверки, в апстриме необходима зона разделяемой памяти (*zone*). Для одного апстрима можно определить несколько проверок.

Могут быть заданы следующие параметры:

`имя`	Обязательное имя проверки.
`port`	Альтернативный порт для запроса.
`interval`	*Интервал* между проверками. По умолчанию — `5s`.
`test`	Проверяемое при запросе условие; задается строкой из переменных. Если результат подстановки всех переменных — `""` или `"0"`, проверка не пройдена.
`essential`	Если параметр задан, то изначально состояние сервера подлежит уточнению и клиентские запросы не передаются ему, пока проверка не будет пройдена.
`persistent`	Установка этого параметра требует сначала включить `essential`; серверы с `persistent`, работавшие до *перезагрузки конфигурации*, начинают получать запросы без необходимости сначала пройти эту проверку.
`fails`	Число последовательных неуспешных запросов, при котором проверка считает сервер неработающим. По умолчанию — 1.
`passes`	Число последовательных успешных запросов, при котором проверка считает сервер работающим. По умолчанию — 1.
`max_response`	Максимальный объем памяти для ответа. Если задано нулевое *значение*, ожидание ответа отключается. По умолчанию — `256k`.
`mode`	Режим проверки в зависимости от работоспособности серверов: • `always` — серверы проверяются независимо от состояния; • `idle` — проверяются неработающие серверы, а также серверы, где с последнего клиентского запроса прошло время `interval`. • `onfail` — проверяются серверы только в неработающем состоянии. По умолчанию — `always`.
`udp`	Если параметр указан, используется протокол UDP. По умолчанию для проверок используется TCP.
`send`	Отправляемые для проверки данные; это может быть строка с префиксом `data:` или имя файла с данными (задается абсолютно или относительно каталога `/usr/local/angie/`).

Пример:

```
upstream backend {
    zone backend 1m;

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

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

server {
    listen ...;

    # ...
    proxy_pass backend;
    upstream_probe_timeout 1s;

    upstream_probe backend_probe
        port=12345
        interval=5s
        test=$good
        essential
        persistent
        fails=3
        passes=3
```

```
        max_response=512k
        mode=onfail
        "send=data:GET / HTTP/1.0\n\n";
}
```

Детали работы:

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

Встроенные переменные

Модуль `stream_upstream` поддерживает следующие встроенные переменные:

`$upstream_probe` (PRO)

Имя активной сейчас проверки *upstream_probe*.

`$upstream_probe_response` (PRO)

Содержимое ответа, полученного в ходе активной проверки *upstream_probe*.

Базовый потоковый модуль реализует основную функциональность для обработки TCP- и UDP-соединений: это определение серверных блоков, маршрутизация трафика, настройка проксирования, поддержка SSL/TLS и управление подключениями для потоковых сервисов, таких как базы данных, DNS и другие протоколы, работающие на основе TCP и UDP.

Остальные модули этого раздела расширяют эту функциональность, позволяя гибко настраивать и оптимизировать работу потокового сервера под различные сценарии и требования.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-stream`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
worker_processes auto;

error_log /var/log/angie/error.log info;

events {
    worker_connections  1024;
}

stream {
    upstream backend {
        hash $remote_addr consistent;
```

```
        server backend1.example.com:12345 weight=5;
        server 127.0.0.1:12345            max_fails=3 fail_timeout=30s;
        server unix:/tmp/backend3;
    }

    upstream dns {
       server 192.168.0.1:53535;
       server dns.example.com:53;
    }

    server {
        listen 12345;
        proxy_connect_timeout 1s;
        proxy_timeout 3s;
        proxy_pass backend;
    }

    server {
        listen 127.0.0.1:53 udp reuseport;
        proxy_timeout 20s;
        proxy_pass dns;
    }

    server {
        listen [::1]:12345;
        proxy_pass unix:/tmp/stream.socket;
    }
}
```

Директивы

listen

Синтаксис	`listen` *адрес*[:*порт*] [ssl] [udp] [proxy_protocol] [setfib=*число*] [fastopen=*число*] [backlog=*число*] [rcvbuf=*размер*] [sndbuf=*размер*] [accept_filter=*фильтр*] [deferred] [bind] [ipv6only=on|off] [reuseport] [so_keepalive=on|off|[keepidle]:[keepintvl]:[keepcnt]];
По умолчанию	—
Контекст	server

Задает *адрес* и *порт* для сокета, на котором сервер будет принимать соединения. Можно указать только *порт*. Кроме того, *адрес* может быть именем хоста, например:

```
listen 127.0.0.1:12345;
listen *:12345;
listen 12345;      # то же, что и *:12345
listen localhost:12345;
```

IPv6-адреса задаются в квадратных скобках:

```
listen [::1]:12345;
listen [::]:12345;
```

UNIX-сокеты задаются префиксом `unix:`

```
listen unix:/var/run/angie.sock;
```

Диапазоны портов задаются при помощи указания первого и последнего порта через дефис:

```
listen 127.0.0.1:12345-12399;
listen 12345-12399;
```

Важно

Разные серверы должны слушать на разных парах *адрес:порт*.

`ssl`	указывает на то, что все соединения, принимаемые на данном слушающем сокете, должны работать в режиме SSL.
`udp`	конфигурирует слушающий сокет для работы с датаграммами. Для обработки пакетов с одного адреса и порта в рамках одной сессии необходимо также указывать параметр *reuseport*.
`proxy_protocol`	указывает на то, что все соединения, принимаемые на данном порту, должны использовать протокол PROXY.

В директиве *listen* можно также указать несколько дополнительных параметров, специфичных для связанных с сокетами системных вызовов.

`setfib=`*число*	устанавливает связанную таблицу маршрутизации, FIB (параметр `SO_SETFIB`) для слушающего сокета. Пока это работает только на FreeBSD.
`fastopen=`*число*	включает «TCP Fast Open» для слушающего сокета и ограничивает максимальную длину очереди соединений, которые еще не завершили процесс трехстороннего рукопожатия.

Осторожно

Не включайте «TCP Fast Open», не убедившись, что сервер может адекватно обрабатывать многократное получение одного и того же SYN-пакета с данными.

`backlog=`*число*	задает параметр *backlog* в вызове *listen()*, который ограничивает максимальный размер очереди ожидающих приема соединений. По умолчанию *backlog* устанавливается равным *-1* для FreeBSD, DragonFly BSD и macOS, и *511* для других платформ.
`rcvbuf=`*размер*	задает размер буфера приема (параметр *SO_RCVBUF*) для слушающего сокета.
`sndbuf=`*размер*	задает размер буфера передачи (параметр *SO_SNDBUF*) для слушающего сокета.
`accept_filter=`*фильтр*	задает имя принимающего фильтра (параметр `SO_ACCEPTFILTER`) для слушающего сокета, который фильтрует входящие соединения перед их передачей в `accept()`. Работает только на FreeBSD и NetBSD 5.0+. Допустимые значения: `dataready` и `httpready`.
`deferred`	указывает использовать отложенный `accept()` (параметр `TCP_DEFER_ACCEPT`) на Linux.
`bind`	указывает, что для данного слушающего сокета нужно делать *bind()* отдельно. Это нужно потому, что если описаны несколько директив *listen* с одинаковым портом, но разными адресами, и одна из директив *listen* слушает на всех адресах для данного *порта* (**:порт*), то Angie PRO сделает *bind()* только на **:порт*. Необходимо заметить, что в этом случае для определения адреса, на который пришло соединение, делается системный вызов *getsockname()*. Если же используются параметры *setfib*, *fastopen*, *backlog*, *rcvbuf*, *sndbuf*, *accept_filter*, *deferred*, *ipv6only*, *reuseport* или *so_keepalive*, то для данной пары *адрес:порт* всегда делается отдельный вызов *bind()*.
`ipv6only=on` | `off`	определяет (через параметр сокета *IPV6_V6ONLY*), будет ли слушающий на wildcard-адресе [::] IPv6-сокет принимать только IPv6-соединения, или же одновременно IPv6- и IPv4-соединения. По умолчанию параметр включен. Установить его можно только один раз на старте.
`reuseport`	указывает, что нужно создавать отдельный слушающий сокет для каждого рабочего процесса (через параметр сокета *SO_REUSEPORT* для Linux 3.9+ и DragonFly BSD или *SO_REUSEPORT_LB* для FreeBSD 12+), позволяя ядру распределять входящие соединения между рабочими процессами. В настоящий момент это работает только на Linux 3.9+, DragonFly BSD и FreeBSD 12+.

Осторожно

Ненадлежащее использование параметра *reuseport* может быть небезопасно.

`so_keepalive=on` | `off` | `[keepidle]:[keepintvl]:[keepcnt]` конфигурирует для слушающего сокета поведение «TCP keepalive».

`''`	если параметр опущен, для сокета будут действовать настройки операционной системы
`on`	для сокета включается параметр *SO_KEEPALIVE*
`off`	для сокета параметр *SO_KEEPALIVE* выключается

Некоторые операционные системы поддерживают настройку параметров «TCP keepalive» на уровне сокета посредством параметров *TCP_KEEPIDLE*, *TCP_KEEPINTVL* и *TCP_KEEPCNT*. На таких системах их можно сконфигурировать с помощью параметров *keepidle*, *keepintvl* и *keepcnt*. Один или два параметра могут быть опущены, в таком случае для соответствующего параметра сокета будут действовать стандартные системные настройки.

Например,

```
so_keepalive=30m::10
```

установит таймаут бездействия (*TCP_KEEPIDLE*) в 30 минут, для интервала проб (*TCP_KEEPINTVL*) будет действовать стандартная системная настройка, а счетчик проб (*TCP_KEEPCNT*) будет равен 10.

preread_buffer_size

Синтаксис	`preread_buffer_size` *размер*;
По умолчанию	`preread_buffer_size 16k;`
Контекст	stream, server

Задает размер буфера *предварительного чтения*.

preread_timeout

Синтаксис	`preread_timeout` *время*;
По умолчанию	`preread_timeout 30s;`
Контекст	stream, server

Задает время фазы *предварительного чтения*.

proxy_protocol_timeout

Синтаксис	`proxy_protocol_timeout` *время*;
По умолчанию	`proxy_protocol_timeout 30s;`
Контекст	stream, server

Задает время для завершения операции чтения заголовка протокола PROXY. Если по истечении этого времени заголовок полностью не получен, соединение закрывается.

resolver

Синтаксис	`resolver` *адрес* ... [valid=*время*] [ipv4=on|off] [ipv6=on|off] [status_zone=*зона*];
По умолчанию	—
Контекст	stream, server, upstream

Задает серверы DNS, используемые для преобразования имен вышестоящих серверов в адреса, например:

```
resolver 127.0.0.53 [::1]:5353;
```

Адрес может быть указан в виде доменного имени или IP-адреса, и необязательного порта. Если порт не указан, используется порт 53. Серверы DNS опрашиваются циклически.

По умолчанию Angie PRO кэширует ответы, используя значение TTL из ответа. Необязательный параметр valid позволяет это переопределить:

`valid`	*необязательный* параметр, позволяет переопределить срок кэширования ответа

```
resolver 127.0.0.53 [::1]:5353 valid=30s;
```

По умолчанию Angie PRO будет искать как IPv4-, так и IPv6-адреса при преобразовании имен в адреса.

`ipv4=off`	запрещает поиск IPv4-адресов
`ipv6=off`	запрещает поиск IPv6-адресов

`status_zone`	*необязательный* параметр; включает сбор метрик запросов и ответов DNS-сервера (*/status/resolvers/<zone>*) в указанной зоне

Совет

Для предотвращения DNS-спуфинга рекомендуется использовать DNS-серверы в защищенной доверенной локальной сети.

resolver_timeout

Синтаксис	`resolver_timeout` *время;*
По умолчанию	`resolver_timeout 30s;`
Контекст	stream, server, upstream

Задает таймаут для преобразования имени в адрес, например:

```
resolver_timeout 5s;
```

server

Синтаксис	`server { ... }`
По умолчанию	—
Контекст	stream

Задает конфигурацию для сервера.

server_name

Синтаксис	`server_name` *имя ...*;
По умолчанию	`server_name "";`
Контекст	server

Задает имена виртуального сервера, например:

```
server {
    server_name example.com www.example.com;
}
```

Первое имя становится основным именем сервера.

Имена серверов могут включать звездочку (*), заменяющую первую или последнюю часть имени:

```
server {
    server_name example.com *.example.com www.example.*;
}
```

Такие имена называются шаблонными именами.

Первые два примера, приведенные выше, можно объединить в один:

```
server {
    server_name .example.com;
}
```

Также можно использовать регулярные выражения в именах серверов, предваряя имя тильдой (~):

```
server {
    server_name www.example.com ~^www\d+\.example\.com$;
}
```

Регулярные выражения могут включать захваты, которые можно использовать в других директивах:

```
server {
    server_name ~^(www\.)?(.+)$;

    proxy_pass www.$2:12345;
}
```

Именованные захваты в регулярных выражениях создают переменные, которые можно использовать в других директивах:

```
server {
    server_name ~^(www\.)?(?<domain>.+)$;

    proxy_pass www.$domain:12345;
}
```

Если параметр директивы установлен на `$hostname`, будет вставлено имя хоста машины.

При поиске виртуального сервера по имени, если имя совпадает с более чем одним из указанных вариантов (например, совпадают и шаблонное имя, и регулярное выражение), будет выбрано первое совпавшее имя в следующем порядке приоритета:

- Точное имя

- Самое длинное шаблонное имя, начинающееся с звездочки, например, `*.example.com`
- Самое длинное шаблонное имя, заканчивающееся звездочкой, например, `mail.*`
- Первое совпавшее регулярное выражение (в порядке появления в конфигурационном файле)

> **Внимание**
>
> Для TLS-соединений используйте модуль *SSL Preread*.

server_names_hash_bucket_size

Синтаксис	`server_names_hash_bucket_size` *размер*;
По умолчанию	`server_names_hash_bucket_size 32|64|128;`
Контекст	stream

Задает размер корзины для хэш-таблиц имен серверов. Значение по умолчанию зависит от размера кэш-линии процессора.

server_names_hash_max_size

Синтаксис	`server_names_hash_max_size` *размер*;
По умолчанию	`server_names_hash_max_size 512;`
Контекст	stream

Задает максимальный размер хэш-таблиц имен серверов.

status_zone

Синтаксис	`status_zone` *зона*;
По умолчанию	—
Контекст	*server*

Выделяет зону разделяемой памяти для сбора метрик */status/stream/server_zones/<zone>*.

Несколько контекстов `server` могут совместно использовать одну и ту же зону для сбора данных.

stream

Синтаксис	`stream { ... }`
По умолчанию	—
Контекст	main

Предоставляет контекст конфигурационного файла, в котором указываются директивы stream-сервера.

tcp_nodelay

Синтаксис	`tcp_nodelay` on | off;
По умолчанию	`tcp_nodelay on;`
Контекст	stream, server

Разрешает или запрещает использование параметра *TCP_NODELAY*. Параметр включается как для клиентских соединений, так и для соединений с проксируемыми серверами.

variables_hash_bucket_size

Синтаксис	`variables_hash_bucket_size` *размер*;
По умолчанию	`variables_hash_bucket_size 64;`
Контекст	stream

Задает размер корзины в хэш-таблице переменных. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

variables_hash_max_size

Синтаксис	`variables_hash_max_size` *размер*;
По умолчанию	`variables_hash_max_size 1024;`
Контекст	stream

Задает максимальный размер хэш-таблиц переменных. Подробнее настройка хэш-таблиц обсуждается *отдельно*.

Встроенные переменные

Модуль *stream core* поддерживает встроенные переменные:

`$angie_version`

версия Angie PRO

`$binary_remote_addr`

адрес клиента в бинарном виде, длина значения всегда 4 байта для IPv4-адресов или 16 байт для IPv6-адресов

`$bytes_received`

число байт, полученных от клиента

`$bytes_sent`

число байт, переданных клиенту

`$connection`

порядковый номер соединения

`$hostname`

имя хоста

`$msec`

текущее время в секундах с точностью до миллисекунд

`$pid`

номер (PID) рабочего процесса

`$protocol`

протокол, используемый для работы с клиентом: *TCP* или *UDP*

`$proxy_protocol_addr`

адрес клиента, полученный из заголовка протокола PROXY Протокол PROXY должен быть предварительно включен при помощи установки параметра proxy_protocol в директиве *listen*.

`$proxy_protocol_port`

порт клиента, полученный из заголовка протокола PROXY Протокол PROXY должен быть предварительно включен при помощи установки параметра proxy_protocol в директиве *listen*.

`$proxy_protocol_server_addr`

адрес сервера, полученный из заголовка протокола PROXY Протокол PROXY должен быть предварительно включен при помощи установки параметра proxy_protocol в директиве *listen*.

`$proxy_protocol_server_port`

порт сервера, полученный из заголовка протокола PROXY Протокол PROXY должен быть предварительно включен при помощи установки параметра proxy_protocol в директиве *listen*.

`$proxy_protocol_tlv_` ***имя***

TLV, полученный из заголовка протокола PROXY. *Имя* может быть именем типа TLV или его числовым значением. В последнем случае значение задается в шестнадцатеричном виде и должно начинаться с *0x*:

$proxy_protocol_tlv_alpn $proxy_protocol_tlv_0x01

SSL TLV могут также быть доступны как по имени типа TLV, так и по его числовому значению, оба должны начинаться с *ssl_*:

$proxy_protocol_tlv_ssl_version $proxy_protocol_tlv_ssl_0x21

Поддерживаются следующие имена типов TLV:

- *alpn (0x01)* - протокол более высокого уровня, используемый поверх соединения
- *authority (0x02)* - значение имени хоста, передаваемое клиентом
- *unique_id (0x05)* - уникальный идентификатор соединения
- *netns (0x30)* - имя пространства имен
- *ssl (0x20)* - структура SSL TLV в бинарном виде

Поддерживаются следующие имена типов SSL TLV:

- *ssl_version (0x21)* - версия SSL, используемая в клиентском соединении
- *ssl_cn (0x22)* - Common Name сертификата
- *ssl_cipher (0x23)* - имя используемого шифра
- *ssl_sig_alg (0x24)* - алгоритм, используемый для подписи сертификата
- *ssl_key_alg (0x25)* - алгоритм публичного ключа

Также поддерживается следующее специальное имя типа SSL TLV:

- *ssl_verify* - результат проверки клиентского сертификата: 0, если клиент предоставил сертификат и он был успешно верифицирован, либо ненулевое значение

Протокол PROXY должен быть предварительно включен при помощи установки параметра proxy_protocol в директиве *listen*.

`$remote_addr`

адрес клиента

`$remote_port`

порт клиента

`$server_addr`

адрес сервера, принявшего соединение Получение значения этой переменной обычно требует одного системного вызова. Чтобы избежать системного вызова, в директивах *listen* следует указывать адреса и использовать параметр *bind*.

`$server_port`

порт сервера, принявшего соединение

`$session_time`

длительность сессии в секундах с точностью до миллисекунд

`$status`

статус сессии, может принимать одно из следующих значений:

200	сессия завершена успешно
400	невозможно разобрать данные, полученные от клиента, например заголовок протокола PROXY
403	доступ запрещен, например при ограничении доступа для *определенных адресов клиентов*
500	внутренняя ошибка сервера
502	плохой шлюз, например если невозможно выбрать сервер группы или сервер недоступен
503	сервис недоступен, например при ограничении по *числу соединений*

`$time_iso8601`

локальное время в формате по стандарту ISO 8601

`$time_local`

локальное время в Common Log Format

Почтовый модуль

Auth HTTP

Директивы

auth_http

Синтаксис	`auth_http` URL;
По умолчанию	—
Контекст	mail, server

Задает URL HTTP-сервера аутентификации. Протокол описан *ниже*.

auth_http_header

Синтаксис	`auth_http_header` *заголовок значение*;
По умолчанию	—
Контекст	mail, server

Добавляет указанный заголовок к запросам, посылаемым на сервер аутентификации. Заголовок можно использовать в качестве shared secret для проверки, что запрос поступил от Angie PRO. Например:

```
auth_http_header X-Auth-Key "secret_string";
```

auth_http_pass_client_cert

Синтаксис	`auth_http_pass_client_cert` on | off;
По умолчанию	`auth_http_pass_client_cert off;`
Контекст	mail, server

Добавляет заголовок «Auth-SSL-Cert» с *клиентским сертификатом* в формате PEM (закодирован в формате *urlencode*) к запросам, посылаемым на сервер аутентификации.

auth_http_timeout

Синтаксис	`auth_http_timeout` *время*;
По умолчанию	`auth_http_timeout 60s;`
Контекст	mail, server

Задает таймаут общения с сервером аутентификации.

Протокол

Для общения с сервером аутентификации используется протокол HTTP. Данные в теле ответа игнорируются, информация передается только в заголовках.

Примеры запросов и ответов:

Запрос:

```
GET /auth HTTP/1.0
Host: localhost
Auth-Method: plain # plain/apop/cram-md5/external
Auth-User: user
Auth-Pass: password
Auth-Protocol: imap # imap/pop3/smtp
Auth-Login-Attempt: 1
Client-IP: 192.0.2.42
Client-Host: client.example.org
```

Хороший ответ:

```
HTTP/1.0 200 OK
Auth-Status: OK
Auth-Server: 198.51.100.1
Auth-Port: 143
```

Плохой ответ:

```
HTTP/1.0 200 OK
Auth-Status: Invalid login or password
Auth-Wait: 3
```

Если заголовка «Auth-Wait» нет, то после выдачи ошибки соединение будет закрыто. В текущей реализации на каждую попытку аутентификации выделяется память, которая освобождается только при завершении сессии. Поэтому число неудачных попыток аутентификации в рамках одной сессии должно быть ограничено — после 10-20 попыток (номер попытки передается в заголовке «Auth-Login-Attempt») сервер должен выдать ответ без заголовка «Auth-Wait».

При использовании APOP или CRAM-MD5 запрос и ответ будут выглядеть так:

```
GET /auth HTTP/1.0
Host: localhost
Auth-Method: apop
Auth-User: user
Auth-Salt: <238188073.1163692009@mail.example.com>
Auth-Pass: auth_response
```

```
Auth-Protocol: imap
Auth-Login-Attempt: 1
Client-IP: 192.0.2.42
Client-Host: client.example.org
```

Хороший ответ:

```
HTTP/1.0 200 OK
Auth-Status: OK
Auth-Server: 198.51.100.1
Auth-Port: 143
Auth-Pass: plain-text-pass
```

Если в ответе есть заголовок «Auth-User», то он переопределяет имя пользователя, используемое для аутентификации с бэкендом.

Для SMTP в ответе дополнительно учитывается заголовок «Auth-Error-Code» — если он есть, то используется как код ответа в случае ошибки. Если его нет, то по умолчанию к «Auth-Status» будет добавлен код *535 5.7.0*.

Например, если от сервера аутентификации будет получен ответ:

```
HTTP/1.0 200 OK
Auth-Status: Temporary server problem, try again later
Auth-Error-Code: 451 4.3.0
Auth-Wait: 3
```

то по SMTP клиенту будет выдана ошибка

```
451 4.3.0 Temporary server problem, try again later
```

Если при проксировании SMTP не требуется аутентификация, запрос будет выглядеть так:

```
GET /auth HTTP/1.0
Host: localhost
Auth-Method: none
Auth-User:
Auth-Pass:
Auth-Protocol: smtp
Auth-Login-Attempt: 1
Client-IP: 192.0.2.42
Client-Host: client.example.org
Auth-SMTP-Helo: client.example.org
Auth-SMTP-From: MAIL FROM: <>
Auth-SMTP-To: RCPT TO: <postmaster@mail.example.com>
```

Для клиентского соединения по протоколу SSL/TLS добавляется заголовок «Auth-SSL», и если директива *ssl_verify_client* включена, заголовок «Auth-SSL-Verify» содержит результат проверки клиентского сертификата: `SUCCESS`, «*FAILED:reason*» и, если сертификат не был предоставлен, `NONE`.

Если клиентский сертификат был предоставлен, информация о нем передается в следующих заголовках запроса: «Auth-SSL-Subject», «Auth-SSL-Issuer», «Auth-SSL-Serial» и «Auth-SSL-Fingerprint». Если директива *auth_http_pass_client_cert* включена, сам сертификат передается в заголовке «Auth-SSL-Cert». Протокол и шифр установленного соединения передаются в заголовках «Auth-SSL-Protocol» и «Auth-SSL-Cipher». Запрос будет выглядеть так:

```
GET /auth HTTP/1.0
Host: localhost
Auth-Method: plain
```

```
Auth-User: user
Auth-Pass: password
Auth-Protocol: imap
Auth-Login-Attempt: 1
Client-IP: 192.0.2.42
Auth-SSL: on
Auth-SSL-Protocol: TLSv1.3
Auth-SSL-Cipher: TLS_AES_256_GCM_SHA384
Auth-SSL-Verify: SUCCESS
Auth-SSL-Subject: /CN=example.com
Auth-SSL-Issuer: /CN=example.com
Auth-SSL-Serial: C07AD56B846B5BFF
Auth-SSL-Fingerprint: 29d6a80a123d13355ed16b4b04605e29cb55a5ad
```

При использовании *протокола PROXY*, информация о нем передается в следующих заголовках запроса: «Proxy-Protocol-Addr», «Proxy-Protocol-Port», «Proxy-Protocol-Server-Addr» и «Proxy-Protocol-Server-Port».

IMAP

Директивы

imap_auth

Синтаксис	`imap_auth` *метод* ...;
По умолчанию	`imap_auth plain;`
Контекст	mail, server

Задает разрешенные методы аутентификации IMAP-клиентов. Поддерживаемые методы:

`plain`	LOGIN, AUTH=PLAIN
`login`	AUTH=LOGIN
`cram-md5`	AUTH=CRAM-MD5. Для работы этого метода пароль должен храниться в незашифрованном виде.
`external`	AUTH=EXTERNAL

Методы аутентификации с передачей пароля открытым текстом (команда *LOGIN*, *AUTH=PLAIN* и *AUTH=LOGIN*) включены всегда, однако если методы `plain` и `login` не указаны, то *AUTH=PLAIN* и *AUTH=LOGIN* не будут автоматически добавляться в *imap_capabilities*.

imap_capabilities

Синтаксис	`imap_capabilities` *расширение* ...;
По умолчанию	`imap_capabilities IMAP4 IMAP4rev1 UIDPLUS;`
Контекст	mail, server

Позволяет указать список расширений протокола IMAP, выдаваемый клиенту по команде CAPABILITY. В зависимости от значения директивы *starttls* к этому списку автоматически добавляются методы аутентификации, указанные в директиве *imap_auth*, и STARTTLS.

В данной директиве имеет смысл указать расширения, поддерживаемые IMAP-серверами, на которые проксируются клиенты (если эти расширения относятся к командам, используемым после аутентификации, когда Angie PRO прозрачно проксирует подключение клиента на бэкенд).

imap_client_buffer

Синтаксис	`imap_client_buffer` *размер*;
По умолчанию	`imap_client_buffer 4k|8k;`
Контекст	mail, server

Задает размер буфера для чтения IMAP-команд. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

POP3

Директивы

pop3_auth

Синтаксис	`pop3_auth` *метод* ...;
По умолчанию	`ipop3_auth plain;`
Контекст	mail, server

Задает разрешенные методы аутентификации POP3-клиентов. Поддерживаемые методы:

`plain`	USER/PASS, AUTH PLAIN, AUTH LOGIN
`apop`	APOP. Для работы этого метода пароль должен храниться в незашифрованном виде.
`cram-md5`	AUTH=CRAM-MD5. Для работы этого метода пароль должен храниться в незашифрованном виде.
`external`	AUTH=EXTERNAL

Методы аутентификации с передачей пароля открытым текстом (*USER/PASS*, *AUTH PLAIN* и *AUTH LOGIN*) включены всегда, однако если метод `plain` не указан, то *AUTH PLAIN* и *AUTH LOGIN* не будут автоматически добавляться в *pop3_capabilities*.

pop3_capabilities

Синтаксис	`pop3_capabilities` *расширение* ...;
По умолчанию	`pop3_capabilities TOP USER UIDL;`
Контекст	mail, server

Позволяет указать список расширений протокола POP3, выдаваемый клиенту по команде CAPA. В зависимости от значения директивы *starttls* к этому списку автоматически добавляются методы аутентификации, указанные в директиве *pop3_auth* (расширение SASL), и STLS.

В данной директиве имеет смысл указать расширения, поддерживаемые POP3-серверами, на которые проксируются клиенты (если эти расширения относятся к командам, используемым после аутентификации, когда Angie PRO прозрачно проксирует подключение клиента на бэкенд).

Proxy

Директивы

proxy_buffer

Синтаксис	`proxy_buffer` *размер*;
По умолчанию	`proxy_buffer 4k|8k;`
Контекст	mail, server

Задает размер буфера, используемого при проксировании. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

proxy_pass_error_message

Синтаксис	`proxy_buffer` on | off;
По умолчанию	`proxy_pass_error_message off;`
Контекст	mail, server

Определяет, передавать ли клиенту сообщение об ошибке, полученное при аутентификации на бэкенде.

Обычно, если аутентификация в Angie PRO прошла успешно, бэкенд не может вернуть ошибку. Если же он все-таки возвращает ошибку, это значит, что произошла ошибка внутри системы. В таких случаях сообщение бэкенда может содержать информацию, которую нельзя показывать клиенту. Однако для некоторых POP3-серверов ошибка в ответ на правильный пароль является штатным поведением. В этом случае директиву стоит включить.

proxy_protocol

Синтаксис	`proxy_protocol` on | off;
По умолчанию	`proxy_protocol off;`
Контекст	mail, server

Включает протокол PROXY для соединений с бэкендом.

proxy_smtp_auth

Синтаксис	`proxy_smtp_auth` on | off;
По умолчанию	`proxy_smtp_auth off;`
Контекст	mail, server

Разрешает или запрещает аутентификацию пользователей на SMTP-бэкенде при помощи команды *AUTH*.

Если также включен *XCLIENT*, то команда *XCLIENT* не будет отправлять параметр *LOGIN*.

proxy_smtp_auth

Синтаксис	`proxy_timeout` *время*;
По умолчанию	`proxy_timeout 24h;`
Контекст	mail, server

Задает таймаут между двумя идущими подряд операциями чтения или записи на клиентском соединении или соединении с проксируемым сервером. Если по истечении этого времени данные не передавались, соединение закрывается.

xclient

Синтаксис	`xclient` on | off;
По умолчанию	`xclient on;`
Контекст	mail, server

Разрешает или запрещает передачу команды XCLIENT с параметрами клиента при подключении к SMTP-бэкенду.

При помощи *XCLIENT* MTA может писать в лог информацию о клиенте и применять различные ограничения на основе этих данных.

Если команда *XCLIENT* разрешена, то при подключении к бэкенду Angie PRO посылает ему следующие команды:

- *EHLO* с *именем сервера*
- *XCLIENT*
- *EHLO* или *HELO*, как ее передал клиент

Если *найденное* по IP-адресу клиента имя указывает на тот же адрес, оно передается в параметре *NAME* команды *XCLIENT*. Если имя не может быть найдено, указывает на другой адрес, или не задан *resolver*, то в параметре *NAME* передается *[UNAVAILABLE]*. Если же в процессе поиска имени или адреса произошла ошибка, передается *[TEMPUNAVAIL]*.

Если команда *XCLIENT* запрещена, то при подключении к бэкенду Angie PRO передает команду *EHLO* с *именем сервера*, если клиент передал *EHLO*, иначе *HELO* с именем сервера.

RealIP

Позволяет менять адрес и необязательный порт клиента на переданные в указанном поле заголовка адрес и порт клиента на переданные в заголовке протокола PROXY. Протокол PROXY должен быть предварительно включен при помощи установки параметра *proxy_protocol* в директиве *listen*.

Пример конфигурации

```
listen 110 proxy_protocol;

set_real_ip_from  192.168.1.0/24;
set_real_ip_from  192.168.2.1;
set_real_ip_from  2001:0db8::/32;
```

Директивы

set_real_ip_from

Синтаксис	`set_real_ip_from` *адрес* | *CIDR* | unix:;
По умолчанию	—
Контекст	mail, server

Задает доверенные адреса, которые передают верный адрес для замены. Если указано специальное значение `unix:`, доверенными будут считаться все UNIX-сокеты.

SMTP

Директивы

smtp_auth

Синтаксис	`smtp_auth` *метод* ...;
По умолчанию	`smtp_auth plain login;`
Контекст	mail, server

Задает разрешенные методы аутентификации SASL-аутентификации SMTP-клиентов. Поддерживаемые методы:

`plain`	AUTH PLAIN
`login`	AUTH LOGIN
`cram-md5`	AUTH CRAM-MD5. Для работы этого метода пароль должен храниться в незашифрованном виде.
`external`	AUTH EXTERNAL
`none`	Аутентификация не требуется

Методы аутентификации с передачей пароля открытым текстом (*AUTH PLAIN* и *AUTH LOGIN*) включены всегда, однако если методы `plain` и `login` не указаны, то *AUTH PLAIN* и *AUTH LOGIN* не будут автоматически добавляться в *smtp_capabilities*.

smtp_capabilities

Синтаксис	`smtp_capabilities` *расширение* ...;
По умолчанию	—
Контекст	mail, server

Позволяет указать список расширений протокола SMTP, выдаваемый клиенту в ответе на команду EHLO. В зависимости от значения директивы *starttls* к этому списку автоматически добавляются методы аутентификации, указанные в директиве *smtp_auth*, и STARTTLS.

В данной директиве имеет смысл указать расширения, поддерживаемые MTA, на который проксируются клиенты (если эти расширения относятся к командам, используемым после аутентификации, когда Angie PRO прозрачно проксирует подключение клиента на бэкенд).

smtp_client_buffer

Синтаксис	`smtp_client_buffer` *размер*;
По умолчанию	`smtp_client_buffer 4k|8k;`
Контекст	mail, server

Задает размер буфера для чтения SMTP-команд. По умолчанию размер одного буфера равен размеру страницы. В зависимости от платформы это или 4K, или 8K.

smtp_greeting_delay

Синтаксис	`smtp_greeting_delay` *размер*;
По умолчанию	`smtp_greeting_delay 0;`
Контекст	mail, server

Позволяет задать задержку перед отправкой SMTP-приветствия, чтобы отклонить клиентов, не дожидающихся приветствия до начала отправки SMTP-команд.

SSL

Обеспечивает работу почтового прокси-сервера по протоколу SSL/TLS.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-mail_ssl_module`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Важно

Для этого модуля нужна библиотека OpenSSL.

Пример конфигурации

Для уменьшения загрузки процессора рекомендуется

- установить число *рабочих процессов* равным числу процессоров,
- включить *разделяемый кэш* сессий,
- выключить *встроенный кэш* сессий
- и, возможно, увеличить *время жизни* сессии (по умолчанию 5 минут):

```
worker_processes auto;

mail {

    ...

    server {
        listen              993 ssl;

        ssl_protocols       TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
        ssl_ciphers         AES128-SHA:AES256-SHA:RC4-SHA:DES-CBC3-SHA:RC4-MD5;
        ssl_certificate     /usr/local/angie/conf/cert.pem;
        ssl_certificate_key /usr/local/angie/conf/cert.key;
        ssl_session_cache   shared:SSL:10m;
        ssl_session_timeout 10m;

    #    ...
    }
```

Директивы

ssl_certificate

Синтаксис	`ssl_certificate` *файл*;
По умолчанию	—
Контекст	mail, server

Указывает файл с сертификатом в формате PEM для данного сервера. Если вместе с основным сертификатом нужно указать промежуточные, то они должны находиться в этом же файле в следующем порядке — сначала основной сертификат, а затем промежуточные. В этом же файле может находиться секретный ключ в формате PEM.

Директива может быть указана несколько раз для загрузки сертификатов разных типов, например RSA и ECDSA:

```
server {
    listen              993 ssl;

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

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

```
#    ...
}
```

Возможность задавать отдельные цепочки сертификатов для разных сертификатов есть только в OpenSSL 1.0.2 и выше. Для более старых версий следует указывать только одну цепочку сертификатов.

Вместо `файла` можно указать значение «data:*сертификат*», при котором сертификат загружается без использования промежуточных файлов.

Ненадлежащее использование подобного синтаксиса может быть небезопасно, например данные секретного ключа могут попасть в *лог ошибок*.

ssl_certificate_key

Синтаксис	`ssl_certificate_key` *файл*;
По умолчанию	—
Контекст	mail, server

Указывает файл с секретным ключом в формате PEM для данного виртуального сервера.

Вместо `файла` можно указать значение «engine:*имя*:id», которое загружает ключ с указанным *id* из OpenSSL engine с заданным именем.

Вместо `файла` также можно указать значение «data:*ключ*», при котором секретный ключ загружается без использования промежуточных файлов. При этом следует учитывать, что ненадлежащее использование подобного синтаксиса может быть небезопасно, например данные секретного ключа могут попасть в *лог ошибок*.

ssl_ciphers

Синтаксис	`ssl_ciphers` *шифры*;
По умолчанию	`ssl_ciphers HIGH:!aNULL:!MD5;`
Контекст	mail, server

Описывает разрешенные шифры. Шифры задаются в формате, поддерживаемом библиотекой OpenSSL, например:

```
ssl_ciphers ALL:!aNULL:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
```

Полный список можно посмотреть с помощью команды «*openssl ciphers*».

ssl_client_certificate

Синтаксис	`ssl_client_certificate` *файл*;
По умолчанию	—
Контекст	mail, server

Указывает файл с доверенными сертификатами CA в формате PEM, которые используются для *проверки* клиентских сертификатов.

Список сертификатов будет отправляться клиентам. Если это нежелательно, можно воспользоваться директивой *ssl_trusted_certificate*.

ssl_conf_command

Синтаксис	`ssl_conf_command` *имя значение*;
По умолчанию	—
Контекст	mail, server

Задает произвольные конфигурационные команды OpenSSL.

Важно

Директива поддерживается при использовании OpenSSL 1.0.2 и выше.

На одном уровне может быть указано несколько директив *ssl_conf_command*:

```
ssl_conf_command Options PrioritizeChaCha;
ssl_conf_command Ciphersuites TLS_CHACHA20_POLY1305_SHA256;
```

Директивы наследуются с предыдущего уровня конфигурации при условии, что на данном уровне не описаны свои директивы *ssl_conf_command*.

Осторожно

Изменение настроек OpenSSL напрямую может привести к неожиданному поведению.

ssl_crl

Синтаксис	`ssl_crl` *файл*;
По умолчанию	—
Контекст	mail, server

Указывает файл с отозванными сертификатами (CRL) в формате PEM, используемыми для *проверки* клиентских сертификатов.

ssl_dhparam

Синтаксис	`ssl_dhparam` *файл*;
По умолчанию	—
Контекст	mail, server

Указывает файл с параметрами для DHE-шифров.

Осторожно

По умолчанию параметры не заданы, и соответственно DHE-шифры не будут использоваться.

ssl_ecdh_curve

Синтаксис	`ssl_ecdh_curve` *кривая*;
По умолчанию	`ssl_ecdh_curve auto;`
Контекст	mail, server

Задает кривую для ECDHE-шифров.

Важно

При использовании OpenSSL 1.0.2 и выше можно указывать несколько кривых, например:

```
ssl_ecdh_curve prime256v1:secp384r1;
```

Специальное значение `auto` соответствует встроенному в библиотеку OpenSSL списку кривых для OpenSSL 1.0.2 и выше, или *prime256v1* для более старых версий.

Важно

При использовании OpenSSL 1.0.2 и выше директива задает список кривых, поддерживаемых сервером. Поэтому для работы ECDSA-сертификатов важно, чтобы список включал кривые, используемые в сертификатах.

ssl_password_file

Синтаксис	`ssl_password_file` *файл*;
По умолчанию	—
Контекст	mail, server

Задает файл с паролями от *секретных ключей*, где каждый пароль указан на отдельной строке. Пароли применяются по очереди в момент загрузки ключа.

Пример:

```
mail {
    ssl_password_file /etc/keys/global.pass;
    ...

    server {
        server_name mail1.example.com;
        ssl_certificate_key /etc/keys/first.key;
    }

    server {
        server_name mail2.example.com;

        # вместо файла можно указать именованный канал
        ssl_password_file /etc/keys/fifo;
        ssl_certificate_key /etc/keys/second.key;
    }
}
```

ssl_prefer_server_ciphers

Синтаксис	`ssl_prefer_server_ciphers` on | off;
По умолчанию	`ssl_prefer_server_ciphers off;`
Контекст	mail, server

При использовании протоколов SSLv3 и TLS устанавливает приоритет серверных шифров над клиентскими.

ssl_protocols

Синтаксис	`ssl_protocols` [SSLv2] [SSLv3] [TLSv1] [TLSv1.1] [TLSv1.2] [TLSv1.3];
По умолчанию	`ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;`
Контекст	mail, server

Изменено в версии 1.2.0: Параметр `TLSv1.3` добавлен к используемым по умолчанию.

Разрешает указанные протоколы.

Важно

Параметры TLSv1.1 и TLSv1.2 работают только при использовании OpenSSL 1.0.1 и выше.

Параметр TLSv1.3 работает только при использовании OpenSSL 1.1.1 и выше.

ssl_session_cache

Синтаксис	`ssl_session_cache` off | none | [builtin[:*размер*]] [shared:*название*:*размер*];
По умолчанию	`ssl_session_cache none;`
Контекст	mail, server

Задает тип и размеры кэшей для хранения параметров сессий. Тип кэша может быть следующим:

`off`	жесткое запрещение использования кэша сессий: Angie PRO явно сообщает клиенту, что сессии не могут использоваться повторно.
`none`	мягкое запрещение использования кэша сессий: Angie PRO сообщает клиенту, что сессии могут использоваться повторно, но на самом деле не хранит параметры сессии в кэше.
`builtin`	встроенный в OpenSSL кэш, используется в рамках только одного рабочего процесса. Размер кэша задается в сессиях. Если размер не задан, то он равен 20480 сессиям. Использование встроенного кэша может вести к фрагментации памяти.
`shared`	кэш, разделяемый между всеми рабочими процессами. Размер кэша задается в байтах, в 1 мегабайт может поместиться около 4000 сессий. У каждого разделяемого кэша должно быть произвольное название. Кэш с одинаковым названием может использоваться в нескольких серверах. Также он используется для автоматического создания, хранения и периодического обновления ключей TLS session tickets, если они не указаны явно с помощью директивы *ssl_session_ticket_key*.

Можно использовать одновременно оба типа кэша, например:

```
ssl_session_cache builtin:1000 shared:SSL:10m;
```

однако использование только разделяемого кэша без встроенного должно быть более эффективным.

ssl_session_ticket_key

Синтаксис	`ssl_session_ticket_key` *файл*;
По умолчанию	—
Контекст	mail, server

Задает файл с секретным ключом, применяемым при шифровании и расшифровании TLS session tickets. Директива необходима, если один и тот же ключ нужно использовать на нескольких серверах. По умолчанию используется случайно сгенерированный ключ.

Если указано несколько ключей, то только первый ключ используется для шифрования TLS session tickets. Это позволяет настроить ротацию ключей, например:

```
ssl_session_ticket_key current.key;
ssl_session_ticket_key previous.key;
```

Файл должен содержать 80 или 48 байт случайных данных и может быть создан следующей командой:

```
openssl rand 80 > ticket.key
```

В зависимости от размера файла для шифрования будет использоваться либо AES256 (для 80-байтных ключей), либо AES128 (для 48-байтных ключей).

ssl_session_tickets

Синтаксис	`ssl_session_tickets` on | off;
По умолчанию	`ssl_session_tickets on;`
Контекст	mail, server

Разрешает или запрещает возобновление сессий при помощи TLS session tickets.

ssl_session_timeout

Синтаксис	`ssl_session_timeout` *время*;
По умолчанию	`ssl_session_timeout 5m;`
Контекст	mail, server

Задает время, в течение которого клиент может повторно использовать параметры сессии.

ssl_trusted_certificate

Синтаксис	`ssl_trusted_certificate` *файл*;
По умолчанию	—
Контекст	mail, server

Задает файл с доверенными сертификатами CA в формате PEM, которые используются для *проверки* клиентских сертификатов.

В отличие от *ssl_client_certificate*, список этих сертификатов не будет отправляться клиентам.

ssl_verify_client

Синтаксис	`ssl_verify_client` on | off | optional | optional_no_ca;
По умолчанию	`ssl_verify_client off;`
Контекст	mail, server

Разрешает проверку клиентских сертификатов. Результат проверки передается в заголовке «Auth-SSL-Verify» в запросе *аутентификации*. Если при проверке клиентского сертификата произошла ошибка или клиент не предоставил требуемый сертификат, соединение закрывается.

`optional`	запрашивает клиентский сертификат, и если сертификат был предоставлен, проверяет его
`optional_no_ca`	запрашивает сертификат клиента, но не требует, чтобы он был подписан доверенным сертификатом CA. Это предназначено для случаев, когда фактическая проверка сертификата осуществляется внешним по отношению к Angie PRO сервисом. Содержимое сертификата доступно в запросах, *посылаемых* на сервер аутентификации.

ssl_verify_depth

Синтаксис	`ssl_verify_depth` *число*;
По умолчанию	`ssl_verify_depth 1;`
Контекст	mail, server

Устанавливает глубину проверки в цепочке клиентских сертификатов.

starttls

Синтаксис	`starttls` on | off | only;
По умолчанию	`starttls off;`
Контекст	mail, server

`on`	разрешить использование команд STLS для POP3 и STARTTLS для IMAP и SMTP;
`off`	запретить использование команд STLS и STARTTLS;
`only`	требовать предварительного перехода на TLS.

Базовый почтовый модуль реализует основную функциональность почтового прокси-сервера: это поддержка протоколов SMTP, IMAP и POP3, настройка серверных блоков, маршрутизация почтовых запросов, аутентификация пользователей и поддержка SSL/TLS для защиты почтовых соединений.

Остальные модули этого раздела расширяют эту функциональность, позволяя гибко настраивать и оптимизировать работу почтового сервера под различные сценарии и требования.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-mail`. В пакетах и образах из наших репозиториев модуль включен в сборку.

Пример конфигурации

```
worker_processes auto;

error_log /var/log/angie/error.log info;

events {
    worker_connections  1024;
}

mail {
    server_name       mail.example.com;
    auth_http         localhost:9000/cgi-bin/auth.cgi;

    imap_capabilities IMAP4rev1 UIDPLUS IDLE LITERAL+ QUOTA;

    pop3_auth         plain apop cram-md5;
    pop3_capabilities LAST TOP USER PIPELINING UIDL;

    smtp_auth         login plain cram-md5;
    smtp_capabilities "SIZE 10485760" ENHANCEDSTATUSCODES 8BITMIME DSN;
    xclient           off;

    server {
        listen   25;
        protocol smtp;
    }
    server {
        listen   110;
        protocol pop3;
        proxy_pass_error_message on;
    }
    server {
        listen   143;
        protocol imap;
    }
    server {
        listen   587;
        protocol smtp;
    }
}
```

Директивы

listen

Синтаксис	`listen` *адрес*[:*порт*] [ssl] [proxy_protocol] [backlog=*число*] [rcvbuf=*размер*] [sndbuf=*размер*] [bind] [ipv6only=on|off] [reuseport] [so_keepalive=on|off|[keepidle]:[keepintvl]:[keepcnt]];
По умолчанию	—
Контекст	server

Задает *адрес* и *порт* для сокета, на котором сервер будет принимать соединения. Можно указать

только *порт*. Кроме того, *адрес* может быть именем хоста, например:

```
listen 127.0.0.1:110;
listen *:110;
listen 110;      # то же, что и *:110
listen localhost:110;
```

IPv6-адреса задаются в квадратных скобках:

```
listen [::1]:110;
listen [::]:110;
```

UNIX-сокеты задаются префиксом `unix:`

```
listen unix:/var/run/angie.sock;
```

Важно

Разные серверы должны слушать на разных парах *адрес:порт*.

`ssl`	указывает на то, что все соединения, принимаемые на данном слушающем сокете, должны работать в режиме SSL.
`proxy_protocol`	указывает на то, что все соединения, принимаемые на данном порту, должны использовать протокол PROXY. Полученная информация передается *серверу аутентификации* и может быть использована для *изменения адреса клиента*.

В директиве *listen* можно также указать несколько дополнительных параметров, специфичных для связанных с сокетами системных вызовов.

`backlog=`*число*	задает параметр *backlog* в вызове *listen()*, который ограничивает максимальный размер очереди ожидающих приема соединений. По умолчанию *backlog* устанавливается равным *-1* для FreeBSD, DragonFly BSD и macOS, и *511* для других платформ.
`rcvbuf=`*размер*	задает размер буфера приема (параметр *SO_RCVBUF*) для слушающего сокета.
`sndbuf=`*размер*	задает размер буфера передачи (параметр *SO_SNDBUF*) для слушающего сокета.
`bind`	указывает, что для данного слушающего сокета нужно делать *bind()* отдельно. Это нужно потому, что если описаны несколько директив *listen* с одинаковым портом, но разными адресами, и одна из директив *listen* слушает на всех адресах для данного *порта* (**:порт*), то Angie PRO сделает *bind()* только на **:порт*. Необходимо заметить, что в этом случае для определения адреса, на который пришло соединение, делается системный вызов *getsockname()*. Если же используются параметры *backlog*, *rcvbuf*, *sndbuf*, *ipv6only*, *reuseport* или *so_keepalive*, то для данной пары *адрес:порт* всегда делается отдельный вызов *bind()*.
`ipv6only=on` | `off`	определяет (через параметр сокета *IPV6_V6ONLY*), будет ли слушающий на wildcard-адресе [::] IPv6-сокет принимать только IPv6-соединения, или же одновременно IPv6- и IPv4-соединения. По умолчанию параметр включен. Установить его можно только один раз на старте.

`so_keepalive=on` | `off` | `[keepidle]:[keepintvl]:[keepcnt]` конфигурирует для слушающего сокета поведение «TCP keepalive».

`''`	если параметр опущен, для сокета будут действовать настройки операционной системы
`on`	для сокета включается параметр *SO_KEEPALIVE*
`off`	для сокета параметр *SO_KEEPALIVE* выключается

Некоторые операционные системы поддерживают настройку параметров «TCP keepalive» на уровне сокета посредством параметров *TCP_KEEPIDLE*, *TCP_KEEPINTVL* и *TCP_KEEPCNT*. На таких системах их можно сконфигурировать с помощью параметров *keepidle*, *keepintvl* и *keepcnt*. Один или два параметра могут быть опущены, в таком случае для соответствующего параметра сокета будут действовать стандартные системные настройки.

Например,

```
so_keepalive=30m::10
```

установит таймаут бездействия (*TCP_KEEPIDLE*) в 30 минут, для интервала проб (*TCP_KEEPINTVL*) будет действовать стандартная системная настройка, а счетчик проб (*TCP_KEEPCNT*) будет равен 10.

Разные серверы должны слушать на разных парах *адрес:порт*.

mail

Синтаксис	`mail { ... }`
По умолчанию	—
Контекст	main

Предоставляет контекст конфигурационного файла, в котором указываются директивы почтового сервера.

max_commands

Добавлено в версии 1.7.0.

Синтаксис	`max_commands` *число*;
По умолчанию	`max_commands 1000;`
Контекст	mail, server

Задает максимальное количество команд, отправляемых во время аутентификации, для усиления защиты от DoS-атак.

max_errors

Синтаксис	`max_errors` *число*;
По умолчанию	`max_errors 5;`
Контекст	mail, server

Задает число ошибок протокола, по достижении которого соединение закрывается.

protocol

Синтаксис	`protocol` *imap* | *pop3* | *smtp;*
По умолчанию	—
Контекст	server

Задает протокол проксируемого сервера. Поддерживаются протоколы *IMAP*, *POP3* и *SMTP*.

Если директива не указана, то протокол может быть определен автоматически по общеизвестному порту, указанному в директиве *listen*:

```
imap: 143, 993
pop3: 110, 995
smtp: 25, 587, 465
```

При сборке из исходного кода поддержку ненужных протоколов можно отключить с помощью параметров сборки `--without-mail_imap_module`, `--without-mail_pop3_module` и `--without-mail_smtp_module`.

resolver

Синтаксис	`resolver` *адрес* ... [valid=*время*] [ipv4=on|off] [ipv6=on|off] [status_zone=*зона*];
По умолчанию	`resolver off;`
Контекст	mail, server

Задает серверы DNS, используемые для преобразования имени хоста клиента для передачи его на *сервер аутентификации* и в команде *XCLIENT* при проксировании SMTP, например:

```
resolver 127.0.0.53 [::1]:5353;
```

Адрес может быть указан в виде доменного имени или IP-адреса, и необязательного порта. Если порт не указан, используется порт 53. Серверы DNS опрашиваются циклически.

По умолчанию Angie PRO кэширует ответы, используя значение TTL из ответа. Необязательный параметр valid позволяет это переопределить:

`valid`	*необязательный* параметр, позволяет переопределить срок кэширования ответа

```
resolver 127.0.0.53 [::1]:5353 valid=30s;
```

По умолчанию Angie PRO будет искать как IPv4-, так и IPv6-адреса при преобразовании имен в адреса.

`ipv4=off`	запрещает поиск IPv4-адресов
`ipv6=off`	запрещает поиск IPv6-адресов
`status_zone`	*необязательный* параметр, включает сбор информации о запросах и ответах сервера DNS в указанной зоне

Совет

Для предотвращения DNS-спуфинга рекомендуется использовать DNS-серверы в защищенной доверенной локальной сети.

resolver_timeout

Синтаксис	`resolver_timeout` *время;*
По умолчанию	`resolver_timeout 30s;`
Контекст	mail, server

Задает таймаут для преобразования имени в адрес, например:

```
resolver_timeout 5s;
```

server

Синтаксис	`server { ... }`
По умолчанию	—
Контекст	mail

Задает конфигурацию для сервера.

server_name

Синтаксис	`server_name` *имя*;
По умолчанию	`server_name hostname;`
Контекст	mail, server

Задает имя сервера, используемое:

- в начальном приветствии POP3/SMTP-сервера;
- в salt при аутентификации SASL-методом CRAM-MD5;

- в команде EHLO при подключении к SMTP-бэкенду, если разрешена передача команды *XCLIENT*.

Если директива не указана, используется имя хоста (*hostname*) машины.

timeout

Синтаксис	`timeout` *время;*
По умолчанию	`timeout 60s;`
Контекст	mail, server

Задает таймаут, который используется до начала проксирования на бэкенд.

Модуль Google PerfTools

Включает поддержку профилирования рабочих процессов Angie PRO при помощи Google Performance Tools. Модуль предназначен для разработчиков Angie PRO и позволяет им анализировать и оптимизировать производительность сервера, предоставляя подробную информацию об использовании памяти, загрузке процессора и других метриках производительности.

При сборке из исходного кода модуль не собирается по умолчанию; его необходимо включить с помощью параметра сборки `--with-google_perftools_module`.

> **Важно**
>
> Для этого модуля нужна библиотека gperftools.

Пример конфигурации

```
google_perftools_profiles /var/log/angie/perftools;
```

Профили будут сохраняться в файлах вида `/var/log/angie/perftools.<PID рабочего процесса>`.

Директивы

google_perftools_profiles

Синтаксис	`google_perftools_profiles` *префикс файла*;
По умолчанию	—
Контекст	main

Задает префикс имени файла, где будет храниться информация о профилировании рабочего процесса Angie PRO. Идентификатор рабочего процесса добавляется в конце имени через точку, например: `/var/log/angie/perftools.1234`.

Основной модуль

Основной модуль	Управление служебными файлами, процессами и другими модулями Angie PRO.

HTTP-модули

HTTP	Основная функциональность для обработки HTTP-запросов и ответов, управления HTTI
Access	Контроль доступа на основе IP-адресов и диапазонов CIDR.
ACME	Автоматическое получение SSL-сертификатов по протоколу ACME.
Addition	Вставка заданного фрагмента до или после тела ответа.
API	RESTful HTTP-интерфейс для получения базовой информации о веб-сервере и его статис
Auth Basic	Базовая HTTP-аутентификация для контроля доступа по имени пользователя и паролю.
Auth Request	Авторизация с помощью подзапроса к внешнему HTTP-сервису.
AutoIndex	Автоматический листинг директорий без индексного файла.
Browser (устарел)	Определение браузера на основе заголовка `User-Agent`.
Charset	Настройка и преобразование кодировки ответа.
DAV	Управление файлами на сервере по протоколу WebDAV.
Empty GIF	Отдача однопиксельного прозрачного GIF.
FastCGI	Проксирование запроса к FastCGI-серверу.
FLV	Псевдо-стриминг файлов в формате Flash Video (FLV).
Geo	Преобразование IP-адресов в заданные значения переменных.
GeoIP	Получение данных об IP-адресах на основе геолокации по базам MaxMind GeoIP.
gRPC	Проксирование запроса к gRPC-серверу.
GunZIP	Распаковка сжатых GZip-ответов для их модификации и в случаях, когда клиент не подд
GZip	Сжатие ответов методом GZip для экономии трафика.
GZip Static	Отдача статических файлов, предварительно сжатых методом GZip.
Headers	Изменение полей заголовка ответа.
HTTP2	Обработка запросов по протоколу HTTP/2.
HTTP3	Обработка запросов по протоколу HTTP/3.
Image Filter	Преобразование изображений.
Index	Настройка индексных файлов, обслуживающих запросы с косой чертой в конце (`/`).
JS	Обработчики для расширения функциональности путем задания дополнительной логики
Limit Conn	Ограничение числа одновременных запросов (активных соединений) для защиты от пере
Limit Req	Ограничение частоты запросов для защиты от перегрузки и подбора паролей.
Log	Настройка журнала запросов для отслеживания обращений к ресурсам с целью монитор
Map	Преобразование переменных на основе предопределенных пар «ключ-значение».
Memcached	Получение ответов от Memcached-сервера.
Mirror	Зеркалирование запросов на другие серверы.
MP4	Псевдо-стриминг файлов в формате MP4.
Perl	Обработчики для расширения функциональности путем задания дополнительной логики
Prometheus	Метрики сервера в формате, совместимом с Prometheus, для мониторинга и сбора статис
Proxy	Реверсивное проксирование запросов к другим HTTP-серверам.
Random Index	Случайный выбор индексного файла для запросов, оканчивающихся косой чертой (`/`).
RealIP	Определение адреса и порта клиента при работе за другим прокси-сервером.
Referer	Валидация значений заголовка `Referer`.
Rewrite	Модификация URI запроса, перенаправления, установка переменных и выбор конфигура
SCGI	Проксирование запроса к SCGI-серверу.
Secure Link	Создание защищенных ссылок с возможностью ограничения срока доступа.
Slice	Разделение запроса на множество подзапросов к отдельным фрагментам для лучшего кэ
Split Clients	Создание переменных для A/B-тестирования, канареечных релизов, шардинга и других с
SSI	Обработка команд SSI (Server Side Includes) в ответах.
SSL	Настройка SSL/TLS для обработки запросов по протоколу HTTPS.
Stub Status (устарел)	Глобальные счетчики соединений и запросов в текстовом формате.

Таблица 1 – продолжение с предыдущей с

Sub	Поиск и замена фрагментов в теле ответа.
Upstream	Настройка групп проксируемых серверов для балансировки нагрузки.
Upstream Probe	Настройка активных проверок работоспособности для групп проксируемых серверов.
UserID	Выдача и обработка cookie с уникальным идентификатором клиента для отслеживания с
uWSGI	Проксирование запроса к uWSGI-серверу.
XSLT	Преобразование XML-документов с помощью языка XSLT.

Потоковые модули

Stream	Основная функциональность потокового сервера для балансировки протоколов TCP и UDP на уровне L4.
Access	Контроль доступа на основе IP-адресов и диапазонов CIDR.
Geo	Преобразование IP-адресов в заданные значения переменных.
GeoIP	Получение данных об IP-адресах на основе геолокации по базам MaxMind GeoIP.
JS	Обработчики для расширения функциональности путем задания дополнительной логики на njs, подмножестве языка JavaScript.
Limit Conn	Ограничение числа одновременных соединений для защиты от перегрузки.
Log	Настройка журнала сессий для отслеживания обращений к ресурсам с целью мониторинга и анализа.
Map	Преобразование переменных на основе предопределенных пар «ключ-значение».
MQTT Preread	Чтение идентификатора клиента и имени пользователя из соединения по протоколу MQTT до момента принятия решения о балансировке.
Pass	Передача принятых соединений напрямую в настроенный слушающий сокет.
Proxy	Настройка проксирования к другим серверам.
RDP Preread	Чтение cookie из соединения по протоколу RDP до момента принятия решения о балансировке.
RealIP	Определение адреса и порта клиента при работе за другим прокси-сервером.
Return	Отправка в ответ клиенту при его подключении заданного значения без дальнейшего проксирования.
Set	Установка заданных значений переменных.
Split Clients	Создание переменных для A/B-тестирования, канареечных релизов, шардинга и других сценариев, требующих разделения по пропорциональным группам.
SSL	Терминирование протоколов SSL/TLS и DTLS.
SSL Preread	Извлечение информации из сообщения `ClientHello` без терминирования SSL/TLS и до момента принятия решения о балансировке.
Upstream	Настройка групп проксируемых серверов для балансировки нагрузки.
Upstream	Настройка активных проверок работоспособности для групп проксируемых серверов.

Почтовые модули

Mail	Основная функциональность почтового прокси-сервера.
Auth HT	Аутентификация пользователей и выбор сервера для последующего проксирования с помощью HTTP-запросов к внешнему серверу.
IMAP	Поддержка протокола IMAP.
POP3	Поддержка протокола POP3.
Proxy	Настройка проксирования к другим серверам.
RealIP	Определение адреса и порта клиента при работе за другим прокси-сервером.
SMTP	Поддержка протокола SMTP.
SSL	Поддержка протоколов SSL/TLS и StartTLS.

Модуль Google PerfTools

Google Perf.	Отвечает за интеграцию с библиотекой Google Performance Tools для профилирования и анализа производительности приложений.

3.2.2 Встроенные переменные

HTTP-модули	*Потоковые модули*
$ancient_browser	
$angie_version	*$angie_version*
$arg_имя	
$args	
$binary_remote_addr	*$binary_remote_addr*
$body_bytes_sent	
	$bytes_received
$bytes_sent	*$bytes_sent*
$connection	*$connection*
$connection_requests	
$connection_time	
$connections_active	
$connections_reading	
$connections_writing	
$connections_waiting	
$content_length	
$content_type	
$cookie_имя	
$date_local	
$date_gmt	
$document_root	
$document_uri	
$fastcgi_script_name	
$fastcgi_path_info	
$gzip_ratio	
$host	
$hostname	*$hostname*
$http2	
$http3	
$http_имя	
$https	
$invalid_referer	
$is_args	
$limit_conn_status	*$limit_conn_status*
$limit_rate	
$limit_req_status	
$memcached_key	
$modern_browser	
	$mqtt_preread_clientid
	$mqtt_preread_username
$msec	*$msec*
$msie	
$p8s_value	
$pid	*$pid*
$pipe	

продолжается на следующей странице

Таблица 2 – продолжение с предыдущей страницы

HTTP-модули	*Потоковые модули*
$proxy_add_x_forwarded_for	
$proxy_host	
$proxy_port	
	$protocol
$proxy_protocol_addr	*$proxy_protocol_addr*
$proxy_protocol_port	*$proxy_protocol_port*
$proxy_protocol_server_addr	*$proxy_protocol_server_addr*
$proxy_protocol_server_port	*$proxy_protocol_server_port*
$proxy_protocol_tlv_имя	*$proxy_protocol_tlv_имя*
$query_string	
$quic_connection	
	$rdp_cookie, *$rdp_cookie_имя*
$realip_remote_addr	*$realip_remote_addr*
$realip_remote_port	*$realip_remote_port*
$realpath_root	
$remote_addr	*$remote_addr*
$remote_port	*$remote_port*
$remote_user	
$request	
$request_body	
$request_body_file	
$request_completion	
$request_filename	
$request_id	
$request_length	
$request_method	
$request_time	
$request_uri	
$scheme	
$secure_link	
$secure_link_expires	
$sent_http_имя	
$sent_trailer_имя	
$server_addr	*$server_addr*
$server_name	
$server_port	*$server_port*
$server_protocol	
	$session_time
$slice_range	
$ssl_alpn_protocol	*$ssl_alpn_protocol*
$ssl_cipher	*$ssl_cipher*
$ssl_ciphers	
$ssl_client_escaped_cert	
	$ssl_client_cert
$ssl_client_fingerprint	*$ssl_client_fingerprint*
$ssl_client_i_dn	*$ssl_client_i_dn*
$ssl_client_i_dn_legacy	
$ssl_client_raw_cert	*$ssl_client_raw_cert*
$ssl_client_s_dn	*$ssl_client_s_dn*
$ssl_client_s_dn_legacy	
$ssl_client_serial	*$ssl_client_serial*
$ssl_client_v_end	*$ssl_client_v_end*
$ssl_client_v_remain	*$ssl_client_v_remain*
$ssl_client_v_start	*$ssl_client_v_start*
$ssl_client_verify	*$ssl_client_verify*

продолжается на следующей странице

Таблица 2 – продолжение с предыдущей страницы

HTTP-модули	*Потоковые модули*
$ssl_curve	*$ssl_curve*
$ssl_curves	*$ssl_curves*
$ssl_early_data	
	$ssl_preread_alpn_protocols
	$ssl_preread_protocol
	$ssl_preread_server_name
$ssl_protocol	*$ssl_protocol*
$ssl_server_name	*$ssl_server_name*
$ssl_session_id	*$ssl_session_id*
$ssl_session_reused	*$ssl_session_reused*
$status	*$status*
$time_iso8601	*$time_iso8601*
$time_local	*$time_local*
$tcpinfo_rtt, *$tcpinfo_rttvar*, *$tcpinfo_snd_cwnd*, *$tcpinfo_rcv_space*	
$uid_got	
$uid_reset	
$uid_set	
$upstream_addr	*$upstream_addr*
$upstream_bytes_received	*$upstream_bytes_received*
$upstream_bytes_sent	*$upstream_bytes_sent*
$upstream_cache_status	
$upstream_connect_time	*$upstream_connect_time*
$upstream_cookie_имя	
	$upstream_first_byte_time
$upstream_header_time	
$upstream_http_имя	
$upstream_probe (PRO)	*$upstream_probe (PRO)*
$upstream_probe_body (PRO)	
	$upstream_probe_response (PRO)
$upstream_response_length	
$upstream_response_time	
	$upstream_session_time
$upstream_status	
$upstream_sticky_status	*$upstream_sticky_status*
$upstream_trailer_имя	
$uri	

3.3 Инструкции

Здесь приведены инструкции по отдельным аспектам настройки Angie PRO.

3.3.1 Миграция с nginx на Angie

Если вы переходите с nginx на Angie, поздравляем! У нас есть руководство для вас.

Имейте в виду, что оно предназначено для базового сценария замены, который полагается на пакетную версию Angie. Если вы работаете с контейнерами, виртуальными машинами, нестандартными путями или модулями, вам потребуется дополнительная подстройка.

Установка Angie

Рекомендуем использовать официальные пакеты из наших репозиториев; см. шаги по установке Angie для вашего дистрибутива. Пока не запускайте сервер; вместо этого проверьте его командой `sudo angie -V`:

```
$ sudo angie -V

  Angie version: Angie/1.7.0
  nginx version: nginx/1.25.4
  built by gcc 11.4.0
  configure arguments: --prefix=/etc/angie --conf-path=/etc/angie/angie.conf ...
```

Как следует отсюда, *конфигурация* находится в `/etc/angie/`, когда Angie устанавливается из пакета.

Обновление конфигурации Angie

Angie обычно требует минимальных изменений в существующей конфигурации nginx.

1. Скопируйте конфигурацию nginx в `/etc/angie/` целиком:

   ```
   $ sudo rsync -a --no-links /etc/nginx/ /etc/angie/
   ```

   Предположим, конфигурация nginx хранится в `/etc/nginx/`; измените шаги, если у вас другой путь.

2. Переименуйте основной файл конфигурации так, как ожидает Angie:

   ```
   $ sudo mv /etc/angie/nginx.conf /etc/angie/angie.conf
   ```

3. Поправьте пути во всей конфигурации Angie, начиная с основного файла конфигурации. Детали зависят от того, как был установлен nginx, но, по крайней мере, необходимо обновить следующее.

   Любые пути *include*, которые пока указывают на `/etc/nginx/`:

   ```
   # include /etc/nginx/conf.d/*.conf;
   # include /etc/nginx/default.d/*.conf;
   # include /etc/nginx/http.d/*.conf;
   # include /etc/nginx/stream.d/*.conf;
   include /etc/angie/conf.d/*.conf;
   include /etc/angie/default.d/*.conf;
   include /etc/angie/http.d/*.conf;
   include /etc/angie/stream.d/*.conf;

   # include /etc/nginx/sites-enabled/*;
   include /etc/angie/sites-enabled/*;

   # include /etc/nginx/modules-enabled/*;
   include /etc/angie/modules-enabled/*;
   ```

```
# include /etc/nginx/mime.types;
include /etc/angie/mime.types;
```

Файл *PID*, который важен для управления процессами Angie:

```
# pid /var/run/nginx.pid;
# -- или --
# pid /run/nginx.pid;
pid /run/angie.pid;
```

Наконец, *журнал обращений* и *журнал ошибок*:

```
# access_log /var/log/nginx/access.log;
access_log /var/log/angie/access.log;

# error_log /var/log/nginx/error.log;
error_log /var/log/angie/error.log;
```

Виртуальные хосты

Если для включения виртуальных хостов используется директория `sites-enabled/`, поправьте и ее:

```
# include /etc/nginx/sites-enabled/*;
include /etc/angie/sites-enabled/*;
```

Затем воссоздайте символические ссылки в `/etc/angie/sites-enabled/`, чтобы все работало.

Перечислите исходные файлы виртуальных хостов, например:

```
$ ls -l /etc/nginx/sites-enabled/

  default -> /etc/nginx/sites-available/default
```

Обратите внимание на их фактическое расположение; здесь это `/etc/nginx/sites-available/`.

Если вы не копировали их ранее в `/etc/angie/`, скопируйте сейчас:

```
$ sudo rsync -a /etc/nginx/sites-available/ /etc/angie/sites-available/
```

Наконец, воссоздайте каждую символическую ссылку:

```
$ sudo ln -s /etc/angie/sites-available/default \
             /etc/angie/sites-enabled/default
```

Динамические модули

Найдите и установите используемые в Angie аналоги для всех динамических модулей, упомянутых в конфигурации nginx, например:

```
$ sudo nginx -T | grep load_module

  load_module modules/ngx_http_geoip2_module.so;
  load_module modules/ngx_stream_geoip2_module.so;
  ...
```

Это означает, что вам нужно установить пакет `angie-module-geoip2`, и так далее.

Есть два популярных способа включения конфигурации динамических модулей:

`/usr/share/nginx/modules/`

Если динамические модули включены через `/usr/share/nginx/modules/`, поправьте путь:

```
# Load dynamic modules. See /usr/share/doc/nginx/README.dynamic.
# include /usr/share/nginx/modules/*.conf;

include /usr/share/angie/modules/*.conf;
```

Затем скопируйте файлы конфигурации модулей:

```
$ sudo rsync -a /usr/share/nginx/modules/ /usr/share/angie/modules/
```

Наконец, измените путь *load_ module* в каждом файле:

```
# load_module "/usr/lib64/nginx/modules/ngx_http_geoip2_module.so";
load_module "/usr/lib64/angie/modules/ngx_http_geoip2_module.so";
```

`/etc/nginx/modules-enabled/`

Если динамические модули включены через `/etc/nginx/modules-enabled/`, поправьте путь:

```
# include /etc/nginx/modules-enabled/*.conf;
include /etc/angie/modules-enabled/*.conf;
```

Затем воссоздайте символические ссылки в `/etc/angie/modules-enabled/`, чтобы все работало.

Перечислите исходные файлы конфигурации модулей, например:

```
$ ls -l /etc/nginx/modules-enabled/

  mod-http-geoip2.conf -> /usr/share/nginx/modules-available/mod-http-geoip2.conf
```

Обратите внимание на их фактическое расположение; здесь это `/usr/share/nginx/modules-available/`.

Скопируйте их в `/usr/share/angie/`:

```
$ sudo rsync -a /usr/share/nginx/modules-available/ /usr/share/angie/modules-
↪available/
```

Наконец, воссоздайте каждую символическую ссылку:

```
$ sudo ln -s /usr/share/angie/modules-available/mod-http-geoip2.conf \
             /etc/angie/modules-enabled/mod-http-geoip2.conf
```

Корневая директория (необязательно)

Если *root* указывает на директорию `/usr/share/nginx/html/`, можно изменить директиву, указав на Angie.

Скопируйте директорию и исправьте значение `root` в конфигурации Angie:

```
$ sudo rsync -a /usr/share/nginx/html/ /usr/share/angie/html/
```

```
# root /usr/share/nginx/html;
root /usr/share/angie/html;
```

Пользователь и группа (необязательно)

Хотя директиву *user* достаточно оставить как есть, для гибкости можно использовать учетные записи Angie.

Поправьте настройки `user` в конфигурации Angie:

```
# user www-data www-data;
user angie angie;
```

Измените владельца *всех* файлов конфигурации, включая файлы в `/usr/share/angie/`, например:

```
$ sudo chown -R angie:angie /etc/angie/
$ sudo chown -R angie:angie /usr/share/angie/
```

Если в конфигурации Angie есть директивы *root*, измените владельца указанных там директорий, например:

```
$ sudo chown -R angie:angie /var/www/html/
```

Завершение

Чтобы ничего не пропустить, найдите и исправьте оставшиеся упоминания `nginx` в конфигурации Angie:

```
$ grep -rn --include='*.conf' 'nginx' /etc/angie/
```

Тестирование и переключение

Обновив конфигурацию Angie, следующим шагом проверьте ее синтаксис, чтобы убедиться, что Angie может с ней работать, а затем переключиться. Проверьте, что Angie воспринимает новую конфигурацию:

```
$ sudo angie -t
```

Эта команда анализирует конфигурацию и сообщает об ошибках, которые блокируют запуск Angie; исправьте все проблемы и перезапустите команду.

Остановка nginx, запуск Angie

Чтобы минимизировать простой, запустите Angie сразу после остановки nginx:

```
$ sudo systemctl stop nginx && sudo systemctl start angie
```

При необходимости включите службу Angie для запуска после перезагрузки:

```
$ sudo systemctl enable angie
```

Миграция завершена! На этом все; вы великолепны.

Отключение nginx

Убедившись, что Angie работает стабильно, можно отключить или удалить nginx, чтобы избежать конфликтов.

Минимум того, что вы можете сделать, — это отключить службу:

```
$ sudo systemctl disable nginx
```

Настройка функций Angie

Можно предположить, что миграция нужна вам не просто так. Почему бы не пойти дальше и не настроить некоторые из дополнительных функций, которые есть в Angie, но нет в nginx?

3.3.2 Настройка модуля ModSecurity

После установки модуля ModSecurity из пакета его необходимо настроить.

1. Чтобы включить установленный модуль в *конфигурации*, загрузите его с помощью директивы *load_module*:

   Список 1: /etc/angie/angie.conf

   ```
   load_module modules/ngx_http_modsecurity_module.so;
   ```

2. Укажите директивы `modsecurity` и `modsecurity_rules_file` в соответствующем контексте, например `server`:

   Список 2: /etc/angie/http.d/default.conf

   ```
   server {
       modsecurity on;
       modsecurity_rules_file /etc/angie/modsecurity/rules.conf;
       # ...
   }
   ```

3. Скопируйте в каталог `/var/lib/angie/modsecurity/` базовый набор правил OWASP для ModSecurity (CRS):

   ```
   $ cd /var/lib/angie/modsecurity/
   $ sudo git clone -b v4.1.0 https://github.com/coreruleset/coreruleset
   ```

   Совет

   Уточните актуальный номер выпуска здесь: https://github.com/coreruleset/coreruleset/releases

4. В каталоге с базовыми правилами скопируйте минимально необходимые примеры конфигурации ModSecurity:

   ```
   $ sudo cp coreruleset/crs-setup.conf.example coreruleset/crs-setup.conf
   $ sudo cp coreruleset/rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example \
       coreruleset/rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf
   $ sudo cp coreruleset/rules/RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf.example \
       coreruleset/rules/RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf
   ```

5. Раскомментируйте приведенные ниже директивы `Include` в файле `/etc/angie/modsecurity/rules.conf`:

```
Include /var/lib/angie/modsecurity/coreruleset/crs-setup.conf
Include /var/lib/angie/modsecurity/coreruleset/rules/*.conf
```

6. Перезагрузите конфигурацию Angie PRO, чтобы изменения вступили в силу:

```
$ sudo angie -t && sudo service angie reload
```

3.3.3 Настройка SSL

Чтобы настроить HTTPS-сервер, необходимо включить параметр *ssl* на слушающих сокетах в блоке *server*, а также указать местоположение файлов с сертификатом сервера и секретным ключом:

```
server {
    listen              443 ssl;
    server_name         www.example.com;
    ssl_certificate     www.example.com.crt;
    ssl_certificate_key www.example.com.key;
    ssl_protocols       TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
    ssl_ciphers         HIGH:!aNULL:!MD5;
#...
}
```

Сертификат сервера является публичным. Он посылается каждому клиенту, соединяющемуся с сервером. Секретный ключ следует хранить в файле с ограниченным доступом (права доступа должны позволять главному процессу Angie PRO читать этот файл). Секретный ключ можно также хранить в одном файле с сертификатом.

```
ssl_certificate     www.example.com.cert;
ssl_certificate_key www.example.com.cert;
```

При этом права доступа к файлу следует также ограничить. Несмотря на то, что и сертификат, и ключ хранятся в одном файле, клиенту посылается только сертификат.

С помощью директив *ssl_protocols* и *ssl_ciphers* можно ограничить соединения использованием только «сильных» версий и шифров SSL/TLS. По умолчанию Angie PRO использует:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
ssl_ciphers HIGH:!aNULL:!MD5;
```

Поэтому их явная настройка в общем случае не требуется.

Оптимизация HTTPS-сервера

SSL-операции потребляют дополнительные ресурсы процессора. На мультипроцессорных системах следует запускать несколько *рабочих процессов*, не меньше числа доступных процессорных ядер. Наиболее ресурсоемкой для процессора является операция SSL-рукопожатия, в рамках которой формируются криптографические параметры сессии. Существует два способа уменьшения числа этих операций, производимых для каждого клиента: использование постоянных (*keepalive*) соединений, позволяющих в рамках одного соединения обрабатывать сразу несколько запросов, и повторное использование параметров SSL-сессии для предотвращения необходимости выполнения SSL-рукопожатия для параллельных и последующих соединений. Сессии хранятся в кэше SSL-сессий, разделяемом между рабочими процессами и настраиваемом директивой *ssl_session_cache*. В 1 мегабайт кэша помещается около 4000 сессий. Таймаут кэша по умолчанию равен 5 минутам. Он может быть увеличен с помощью директивы *ssl_session_timeout*. Вот пример конфигурации, оптимизированной под многоядерную систему с 10-мегабайтным разделяемым кэшем сессий:

```
worker_processes auto;

http {
    ssl_session_cache   shared:SSL:10m;
    ssl_session_timeout 10m;

    server {
        listen              443 ssl;
        server_name         www.example.com;
        keepalive_timeout   70;

        ssl_certificate     www.example.com.crt;
        ssl_certificate_key www.example.com.key;
        ssl_protocols       TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
        ssl_ciphers         HIGH:!aNULL:!MD5;
    #...
```

Цепочки SSL-сертификатов

Некоторые браузеры могут выдавать предупреждение о сертификате, подписанном общеизвестным центром сертификации, в то время как другие браузеры без проблем принимают этот же сертификат. Так происходит потому, что центр, выдавший сертификат, подписал его промежуточным сертификатом, которого нет в базе данных сертификатов общеизвестных доверенных центров сертификации, распространяемой вместе с браузером. В подобном случае центр сертификации предоставляет «связку» сертификатов, которую следует присоединить к сертификату сервера. Сертификат сервера следует разместить перед связкой сертификатов в скомбинированном файле:

```
$ cat www.example.com.crt bundle.crt > www.example.com.chained.crt
```

Полученный файл следует указать в директиве *ssl_certificate*:

```
server {
    listen              443 ssl;
    server_name         www.example.com;
    ssl_certificate     www.example.com.chained.crt;
    ssl_certificate_key www.example.com.key;
#...
}
```

Если сертификат сервера и связка сертификатов были соединены в неправильном порядке, Angie PRO не запустится и выдаст сообщение об ошибке:

> **SSL_CTX_use_PrivateKey_file(» ... /www.example.com.key») failed**
> (SSL: error:0B080074:x509 certificate routines: X509_check_private_key:key values mismatch)

Поскольку Angie PRO попытается использовать секретный ключ с первым сертификатом из связки вместо сертификата сервера.

Браузеры обычно сохраняют полученные промежуточные сертификаты, подписанные доверенными центрами сертификации, поэтому активно используемые браузеры уже могут иметь требуемые промежуточные сертификаты и не выдать предупреждение о сертификате, присланном без связанной с ним цепочки сертификатов. Убедиться в том, что сервер присылает полную цепочку сертификатов, можно при помощи утилиты командной строки `openssl`, например:

```
$ openssl s_client -connect www.godaddy.com:443

Certificate chain
```

```
 0 s:/C=US/ST=Arizona/L=Scottsdale/1.3.6.1.4.1.311.60.2.1.3=US
     /1.3.6.1.4.1.311.60.2.1.2=AZ/O=GoDaddy.com, Inc
     /OU=MIS Department/CN=www.GoDaddy.com
     /serialNumber=0796928-7/2.5.4.15=V1.0, Clause 5.(b)
   i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc.
     /OU=http://certificates.godaddy.com/repository
     /CN=Go Daddy Secure Certification Authority
     /serialNumber=07969287
 1 s:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc.
     /OU=http://certificates.godaddy.com/repository
     /CN=Go Daddy Secure Certification Authority
     /serialNumber=07969287
   i:/C=US/O=The Go Daddy Group, Inc.
     /OU=Go Daddy Class 2 Certification Authority
 2 s:/C=US/O=The Go Daddy Group, Inc.
     /OU=Go Daddy Class 2 Certification Authority
   i:/L=ValiCert Validation Network/O=ValiCert, Inc.
     /OU=ValiCert Class 2 Policy Validation Authority
     /CN=http://www.valicert.com//emailAddress=info@valicert.com
```

Совет

При тестировании конфигураций с *SNI* необходимо указывать опцию *-servername*, так как *openssl* по умолчанию не использует SNI.

В этом примере субъект («s») сертификата №0 сервера www.GoDaddy.com подписан издателем («i»), который в свою очередь является субъектом сертификата №1, подписанного издателем, который в свою очередь является субъектом сертификата №2, подписанного общеизвестным издателем ValiCert, Inc., чей сертификат хранится во встроенной в браузеры базе данных сертификатов.

Если связку сертификатов не добавили, будет показан только сертификат сервера под номером 0.

Единый HTTP/HTTPS сервер

Можно настроить единый сервер, который обслуживает как HTTP-, так и HTTPS-запросы:

```
server {
    listen              80;
    listen              443 ssl;
    server_name         www.example.com;
    ssl_certificate     www.example.com.crt;
    ssl_certificate_key www.example.com.key;
#...
}
```

Выбор HTTPS-сервера по имени

Типичная проблема возникает при настройке двух и более HTTPS-серверов, слушающих на одном и том же IP-адресе:

```
server {
    listen          443 ssl;
    server_name     www.example.com;
    ssl_certificate www.example.com.crt;
#...
}

server {
    listen          443 ssl;
    server_name     www.example.org;
    ssl_certificate www.example.org.crt;
#...
}
```

В такой конфигурации браузер получит сертификат сервера по умолчанию, т.е. *www.example.com*, независимо от запрашиваемого имени сервера. Это связано с поведением протокола SSL. SSL-соединение устанавливается до того, как браузер посылает HTTP-запрос, и Angie PRO не знает имени запрашиваемого сервера. Следовательно, он лишь может предложить сертификат сервера по умолчанию.

Наиболее старым и надежным способом решения этой проблемы является назначение каждому HTTPS-серверу своего IP-адреса:

```
server {
    listen          192.168.1.1:443 ssl;
    server_name     www.example.com;
    ssl_certificate www.example.com.crt;
#...
}

server {
    listen          192.168.1.2:443 ssl;
    server_name     www.example.org;
    ssl_certificate www.example.org.crt;
#...
}
```

SSL-сертификат с несколькими именами

Существуют и другие способы, позволяющие использовать один и тот же IP-адрес сразу для нескольких HTTPS-серверов. Все они, однако, имеют свои недостатки. Одним из таких способов является использование сертификата с несколькими именами в поле *SubjectAltName* сертификата, например *www.example.com* и *www.example.org*. Однако, длина поля *SubjectAltName* ограничена.

Другим способом является использование wildcard-сертификата, например **.example.org*. Такой сертификат защищает все поддомены указанного домена, но только на заданном уровне. Под такой сертификат подходит *www.example.org*, но не подходят *example.org* и *www.sub.example.org*. Эти два метода также могут быть объединены. Сертификат может содержать как точные, так и wildcard-имена в поле *SubjectAltName*, например *example.org* и **.example.org*.

Лучше всего разместить файл сертификата с несколькими именами и его секретный ключ на уровне конфигурации *http*, чтобы все серверы унаследовали их единственную копию в памяти.

```
ssl_certificate     common.crt;
ssl_certificate_key common.key;

server {
    listen          443 ssl;
    server_name     www.example.com;
#...
}

server {
    listen          443 ssl;
    server_name     www.example.org;
#...
}
```

Указание имени сервера

Более общее решение для работы нескольких HTTPS-серверов на одном IP-адресе — расширение Server Name Indication протокола TLS (SNI, RFC 6066), которое позволяет браузеру передать запрашиваемое имя сервера во время SSL-рукопожатия, а значит, сервер будет знать, какой сертификат ему следует использовать для соединения. Сейчас SNI поддерживается большинством современных браузеров, однако может не использоваться некоторыми старыми или специализированными клиентами.

> **Совет**
>
> В SNI можно передавать только доменные имена, однако некоторые браузеры могут ошибочно передавать IP-адрес сервера в качестве его имени, если в запросе указан IP-адрес. На этом не следует полагаться.

Чтобы использовать SNI в Angie PRO, соответствующая поддержка должна присутствовать как в библиотеке OpenSSL, использованной при сборке бинарного файла Angie PRO, так и в библиотеке, подгружаемой в момент работы. OpenSSL поддерживает SNI начиная с версии 0.9.8f, если она была собрана с опцией конфигурации *--enable-tlsext*. Начиная с OpenSSL 0.9.8j эта опция включена по умолчанию. Если Angie PRO был собран с поддержкой SNI, то при запуске Angie PRO с ключом «-V» об этом сообщается:

```
$ angie -V
...
TLS SNI support enabled
...
```

Однако если Angie PRO, собранный с поддержкой SNI, в процессе работы подгружает библиотеку OpenSSL, в которой нет поддержки SNI, Angie PRO выдает предупреждение:

> Angie PRO was built with SNI support, however, now it is linked dynamically to an OpenSSL library which has no tlsext support, therefore SNI is not available

3.3.4 Веб-панель мониторинга Console Light

Angie PRO предоставляет широкий спектр возможностей мониторинга своей работы; помимо *метрик* в API и модуля *Prometheus*, можно использовать визуальную консоль, устанавливаемую в дополнение к серверу.

Console Light

Console Light — это облегченный интерфейс мониторинга активности в реальном времени, который отображает ключевые показатели нагрузки и производительности сервера. Консоль основана на возможностях *API-интерфейса* Angie PRO; данные мониторинга активности генерируются в реальном времени. Кроме того, консоль позволяет динамически *изменять* конфигурацию Angie PRO там, где эту возможность предоставляет сам API.

Пример развернутой и настроенной консоли: https://console.angie.software/

Установка и настройка

Console Light публикуется в виде пакетов `angie-console-light` (Angie) и `angie-pro-console-light` (Angie PRO) в наших репозиториях и устанавливается так же, как и любой другой пакет; кроме того, можно скачать исходный код с нашего веб-сайта или GitHub. Текущая версия — 1.4.0.

После установки настройте консоль, добавив в *файл конфигурации* следующий фрагмент:

```
location /console/ {

    # Только локальный доступ
    allow 127.0.0.1;
    deny all;

    auto_redirect on;

    alias /usr/share/angie-console-light/html/;
    index index.html;

    location /console/api/ {
        api /status/;
    }

    # Чтобы после аутентификации работали функции редактирования (только PRO)
    location /console/api/config/ {

        auth_basic           "Защищенный сайт";
        auth_basic_user_file conf/htpasswd;

        api /config/;
    }
}
```

Не забудьте применить измененную конфигурацию:

```
$ sudo angie -t && sudo service angie reload
```

Включить аутентификацию аналогично примеру выше можно для произвольного раздела API, например:

```
location /console/server_zones/ {
    auth_basic           "Защищенный сайт";
    auth_basic_user_file conf/htpasswd;
}
```

Можно также запретить доступ к произвольному разделу настроенного таким образом `location` для консоли, например:

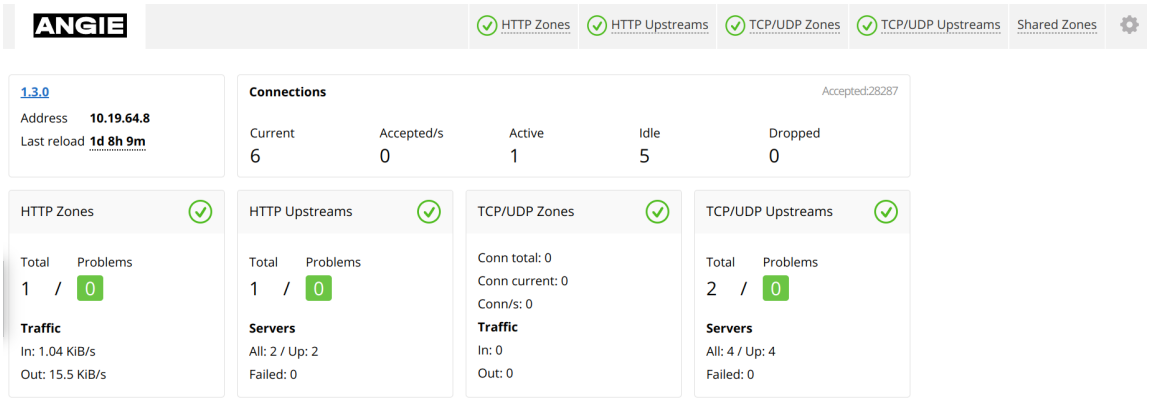
```
location /console/api/resolvers/ {
    deny all;
}
```

Интерфейс

Консоль представляет собой единый экран с набором вкладок, каждая из которых содержит ряд виджетов с данными мониторинга.

> **Подсказка**
>
> В разделах ниже описания элементов интерфейса даны в порядке слева направо.

Вкладка *Angie PRO*



Это основная вкладка, где в сводном виде отображаются основные показатели мониторинга Angie PRO, сведенные на основе данных из нескольких разделов API.

Виджет *About*

Здесь выводится номер версии Angie PRO со ссылкой на соответствующую документацию, а также адрес сервера и время последней *перезагрузки конфигурации*.

Кроме того, если включена директива *api_config_files*, ссылка *Configs* открывает список файлов конфигурации, загруженных на сервере. Затем каждый файл можно просмотреть в компактном виде с подсветкой синтаксиса.

Виджет *Connections*

Здесь представлена основная статистика серверных соединений, формируемая на основе раздела API */status/connections/*:

Current	Текущее количество соединений
Accepted/s	Число принимаемых за секунду соединений
Active	Число активных соединений
Idle	Число соединений в состоянии ожидания
Dropped	Количество сброшенных соединений

Также доступно:

Accepted	Общее число соединений, принятых с последней перезагрузки сервера

Виджет *HTTP Zones*

Внимание

Требует задать директиву *status_zone* в контексте `server` или `location`.

Здесь представлена статистика зон разделяемой памяти контекста `http`, формируемая на основе раздела API */status/http/server_zones/*:

Total	Общее количество зон
Problems	Количество зон с какими-либо проблемами
Traffic	Общий объем входящего и исходящего трафика

Виджет *HTTP Upstreams*

Внимание

Требует задать директиву *upstream* в контексте `http`.

Здесь представлена статистика апстримов контекста `http`, формируемая на основе раздела API */status/http/upstreams/*:

Total	Общее количество апстримов
Problems	Количество апстримов с какими-либо проблемами
Servers	Статистика серверов с разделением по состоянию

Виджет *TCP/UDP Zones*

Внимание

Требует задать следующие директивы:

- `status_zone` в контексте *server* или *stream*;
- `limit_conn` в контексте *server* или *stream*;
- *limit_conn_zone* в контексте `stream`.

Пример:

```
stream {

    # ...
    limit_conn_zone $connection zone=limit-conn-stream:10m;

    server {

        # ...
        limit_conn limit-conn-stream 1;
        status_zone foo;
    }
}
```

Здесь представлена статистика зон разделяемой памяти контекста `stream`, формируемая на основе раздела API */status/stream/server_zones/*:

Conn total	Общее количество клиентских соединений
Conn current	Текущее количество клиентских соединений
Conn/s	Количество обрабатываемых в секунду соединений

Виджет *TCP/UDP Upstreams*

Внимание

Требует задать директиву *upstream* в контексте `stream`.

Здесь представлена статистика апстримов контекста `stream`, формируемая на основе раздела API */status/stream/upstreams/*:

Total	Общее количество апстримов
Problems	Количество апстримов с какими-либо проблемами
Servers	Статистика серверов с разделением по состоянию

Вкладка *HTTP Zones*

Внимание

Требует задать директиву *status_zone* в контексте `server` или `location`.

Раздел *Server Zones*

Server Zones

Zone	Requests			Responses						Traffic				SSL			
	Current	Total	Req/s	1xx	2xx	3xx	4xx	5xx	Total	Sent/s	Rcvd/s	Sent	Rcvd	Handshaked	Reuses	Timedout	Failed
Brazil	1	1518366	3	0	1336935	2452	4880	174098	1518189	108 KiB	288 B	41.1 GiB	84.4 MiB	784	0	0	0
Russia	4	1382189	5	0	1373385	2504	5017	1279	1382010	61.4 KiB	228 B	42.1 GiB	73.7 MiB	836	0	0	0
India	4	1426856	4	0	1417678	2619	5266	1289	1426654	133 KiB	223 B	43.5 GiB	77.1 MiB	742	0	0	0
China	8	781161	2	0	729192	1375	3072	47514	780711	117 KiB	227 B	22.4 GiB	41.9 MiB	521	0	0	0
South Africa	5	1401366	6	0	1392465	2478	5113	1305	1401198	130 KiB	262 B	42.7 GiB	85.4 MiB	760	0	0	0
Argentina	4	1478295	7	0	1468815	2753	5449	1274	1478107	243 KiB	498 B	45.1 GiB	87.5 MiB	846	0	0	0
Egypt	2	1409034	3	0	1399957	2588	5155	1332	1408853	266 KiB	331 B	42.9 GiB	74.3 MiB	756	0	0	0
Ethiopia	2	1287945	5	0	1279661	2426	4676	1180	1287767	211 KiB	358 B	39.2 GiB	74.1 MiB	718	0	0	0
Iran	6	1414692	10	0	1405419	2564	5350	1353	1414478	391 KiB	754 B	43.1 GiB	73.0 MiB	830	0	0	0
Saudi Arabia	4	1469922	9	0	1460600	2605	5401	1312	1469717	367 KiB	617 B	44.8 GiB	87.0 MiB	818	0	0	0
UAE	1	1459720	2	0	1450440	2705	5258	1316	1459506	50.8 KiB	106 B	44.5 GiB	74.5 MiB	838	0	0	0

Здесь в сводном виде отображается статистика мониторинга зон разделяемой памяти для контекста `server` в `http`, формируемая на основе раздела API */status/http/server_zones/*. Для каждой зоны представлены следующие данные:

Zone	Имя зоны

Подсказка

Щелкните стрелку рядом с пунктом *Zone*, чтобы отсортировать зоны по алфавиту или порядку в конфигурации.

Requests	Общее количество запросов, а также число запросов в секунду
Responses	Количество ответов с разбиением по кодам статуса, а также их общее количество
Traffic	Скорость исходящего и входящего трафика, а также общие объемы исходящего и входящего трафика
SSL	Суммарные показатели количества: - успешных SSL-рукопожатий; - повторных использований SSL-сессий; - SSL-рукопожатий с истекшим таймаутом; - неуспешных SSL-рукопожатий.

Раздел *Location Zones*

Location Zones

Zone	Requests		Responses						Traffic			
	Total	Req/s	1xx	2xx	3xx	4xx	5xx	Total	Sent/s	Rcvd/s	Sent	Rcvd
Brasilia	308043	0	0	271399	509	955	35180	308005	38.9 KiB	57.0 B	8.33 GiB	17.0 MiB
Diadema	302843	0	0	266569	501	997	34776	302812	58.9 KiB	56.0 B	8.20 GiB	16.4 MiB
Porto Alegre	298320	2	0	262673	462	974	34211	298284	40.7 KiB	184 B	8.07 GiB	17.6 MiB
Salvador	303063	0	0	266622	487	954	35000	303026	0	0	8.18 GiB	16.7 MiB
Vitoria	306162	0	0	269732	493	1000	34937	306128	0	0	8.28 GiB	16.6 MiB
Lipetsk	280321	0	0	278579	502	978	262	280292	53.6 KiB	56.0 B	8.54 GiB	15.2 MiB
Moscow	274972	0	0	273224	479	1028	241	274935	15.6 KiB	55.0 B	8.38 GiB	14.7 MiB
Omsk	271726	0	0	270024	510	943	249	271688	0	0	8.29 GiB	14.0 MiB
Sevastopol	275881	0	0	274075	497	1047	262	275852	0	0	8.40 GiB	15.8 MiB
Ufa	279348	2	0	277546	516	1021	265	279306	132 KiB	157 B	8.52 GiB	14.1 MiB

Здесь в сводном виде отображается статистика мониторинга зон разделяемой памяти для контекста `location` в `http`, формируемая на основе раздела API */status/http/location_zones/*. Для каждой зоны представлены следующие данные:

Zone	Имя зоны

Подсказка

Щелкните стрелку рядом с пунктом *Zone*, чтобы отсортировать зоны по алфавиту или порядку в конфигурации.

Requests	Текущее и общее количество запросов, а также число запросов в секунду
Responses	Количество ответов с разбиением по кодам статуса, их общее количество, а также число ответов в секунду
Traffic	Скорость исходящего и входящего трафика, а также общие объемы исходящего и входящего трафика

Раздел *Limit Conn*

Limit Conn

Zone	Passed	Rejected	Exhausted	Skipped
limit-conn-http	1345660	172873	0	0

Здесь приведена статистика зон `limit_conn` в контексте `http`, формируемая на основе раздела API */status/http/limit_conns/*. Для каждой зоны представлены следующие данные:

Zone	Имя зоны

Подсказка

Щелкните значок рядом с пунктом *Zone*, чтобы открыть или закрыть график со следующими показателями.

Passed	Общее количество проксированных соединений
Rejected	Общее количество сброшенных соединений
Exhausted	Общее количество соединений, сброшенных из-за переполнения хранилища зоны
Skipped	Общее количество соединений, переданных с нулевым или превосходящим 255 байт ключом

Раздел *Limit Req*


Limit Req

	Zone	Passed	Delayed	Rejected	Exhausted	Skipped
	limit-req-http	36790	697690	46865	0	0

Здесь приведена статистика зон `limit_reqs` в контексте `http`, формируемая на основе раздела API */status/http/limit_reqs/*. Для каждой зоны представлены следующие данные:

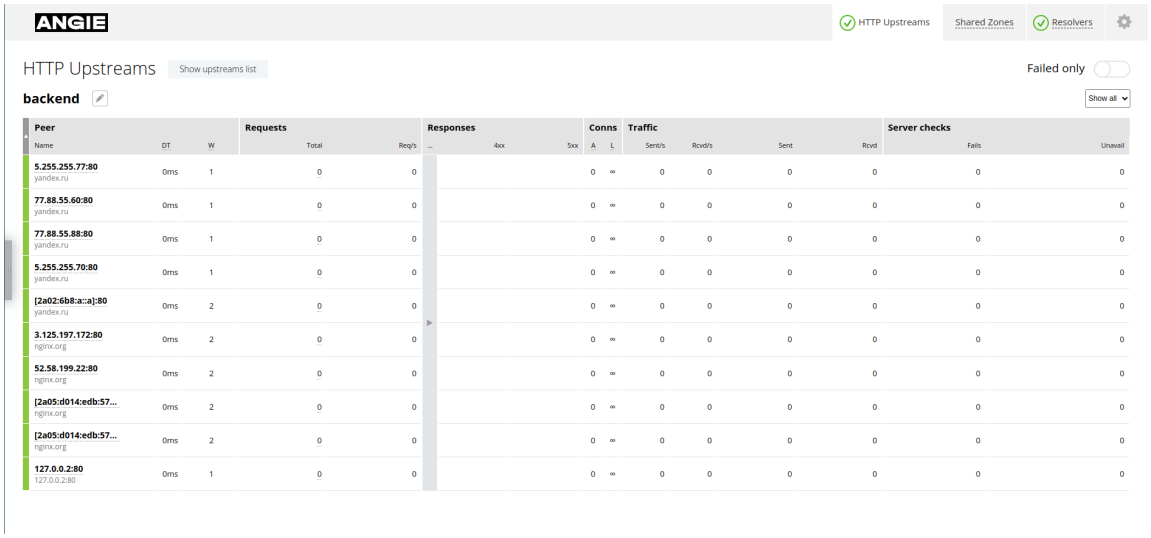
Zone	Имя зоны

Подсказка

Щелкните значок рядом с пунктом *Zone*, чтобы открыть или закрыть график со следующими показателями.

Passed	Общее количество проксированных соединений
Delayed	Общее количество задержанных соединений
Rejected	Общее количество сброшенных соединений
Exhausted	Общее количество соединений, сброшенных из-за переполнения хранилища зоны
Skipped	Общее количество соединений, переданных с нулевым или превосходящим 255 байт ключом

Вкладка *HTTP Upstreams*



Внимание

Требует задать директиву *upstream* в контексте `http`.

На этой вкладке в сводном виде отображается статистика мониторинга апстримов контекста `http`, формируемая на основе раздела API */status/http/upstreams/*.

- Кнопка *Show upstreams list* переключает краткий список апстримов с указанием числа проблемных апстримов и серверов.
- Переключатель *Failed only* переключает режим вывода статистики по проблемным апстримам.
- Кнопка редактирования (только в Angie PRO) переключает интерфейс *редактирования апстрима*.
- Раскрывающийся список с правой стороны таблицы каждого апстрима позволяет отфильтровать серверы в определенном состоянии (*Up*, *Failed*, *Checking*, *Down*).

Для каждого апстрима, помимо имени и коэффициента использования зоны разделяемой памяти, представлены следующие данные:

Server	Имена, время простоя и веса серверов апстрима

Подсказка

Щелкните стрелку рядом с пунктом *Server*, чтобы отсортировать серверы по их состоянию или порядку в конфигурации.

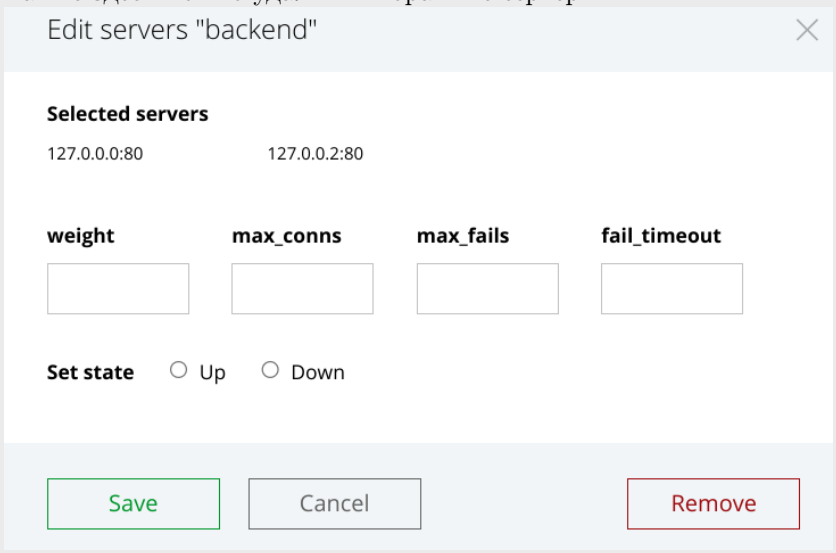
Requests	Общее количество и скорость обработки запросов
Responses	Количество ответов с разбиением по кодам статуса
Conns	Количество активных соединений и их максимальный предел, если он задан
Traffic	Скорость исходящего и входящего трафика, а также общие объемы исходящего и входящего трафика
Server checks	Количество неуспешных обращений к серверу и число раз, когда сервер считался недоступным (объект `health` в API)
Health monitors (только в Angie PRO)	Общее количество *проверок* сервера, количество неуспешных проверок, а также время последней проверки

Редактирование апстримов

В Angie PRO рядом с каждым апстримом есть кнопка редактирования; при нажатии она выводит еще две кнопки:

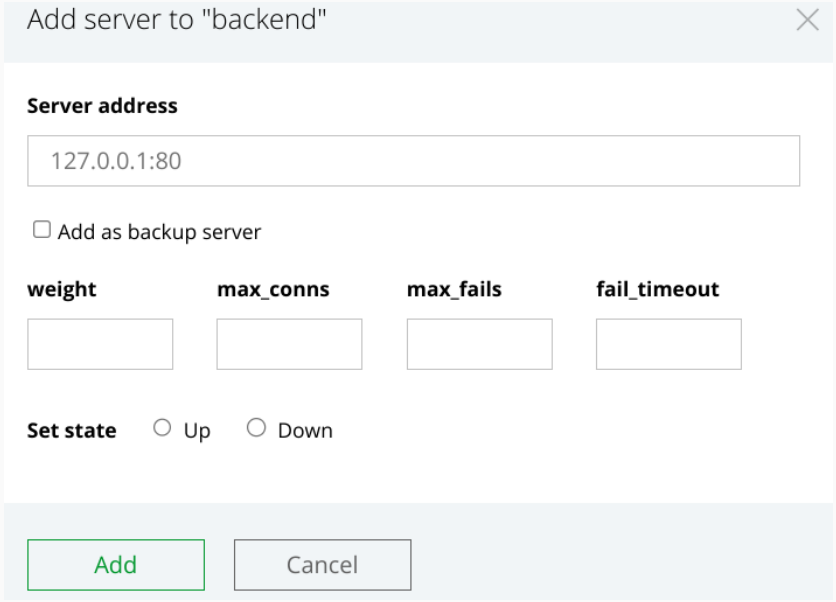
Edit selected

Редактирование выбранных серверов в составе апстрима. Позволяет одновременно задать для всех следующие параметры: *weight* (вес), *max_conns* (максимальный предел соединений), *max_fails* (максимальный предел сбоев, переводящий сервер в недоступные), *fail_timeout* (временное окно подсчета сбоев для *max_fails*), *state* (включен или отключен).
Также здесь можно удалить выбранные серверы.



Add server

Добавление сервера в апстрим. Позволяет задать следующие параметры: *address* (адрес), *backup* (запасной сервер или нет), *weight* (вес), *max_conns* (максимальный предел соединений), *max_fails* (максимальный предел сбоев, переводящий сервер в недоступные), *fail_timeout* (временное окно подсчета сбоев для *max_fails*), *state* (включен или отключен).



Вкладка *TCP/UDP Zones*

Внимание

Требует задать следующие директивы:

- `status_zone` в контексте *server* или *stream*;
- `limit_conn` в контексте *server* или *stream*;
- *limit_conn_zone* в контексте `stream`.

Пример:

```
stream {

    # ...
    limit_conn_zone $connection zone=limit-conn-stream:10m;

    server {

        # ...
        limit_conn limit-conn-stream 1;
        status_zone foo;
    }
}
```

Раздел *TCP/UDP Zones*

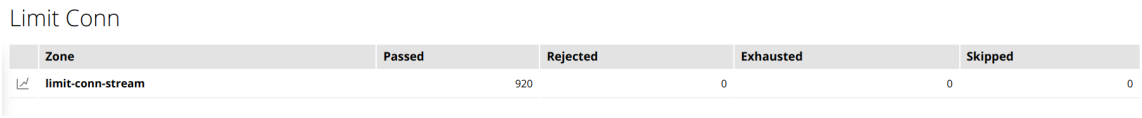
TCP/UDP Zones

Zone	Connections			Sessions				Traffic				SSL			
	Current	Total	Conn/s	2xx	4xx	5xx	Total	Sent/s	Rcvd/s	Sent	Rcvd	Handshakes	Handshakes Failed	Session Reuses	Verify Failures
sing_chorus	3	920	0	845	0	72	917	0	0	11.8 GiB	17.4 MiB	848	0	416	0

Здесь в сводном виде отображается статистика мониторинга зон разделяемой памяти контекста `server` в `stream`, формируемая на основе раздела API */status/stream/server_zones/*. Для каждой зоны представлены следующие данные:

Zone	Имя зоны
Connections	Текущее и общее количество соединений, а также число соединений в секунду
Sessions	Количество сессий с разбиением по кодам статуса, а также их общее число
Traffic	Скорость исходящего и входящего трафика, а также общие объемы исходящего и входящего трафика
SSL	Суммарные показатели количества: - успешных SSL-рукопожатий; - неуспешных SSL-рукопожатий; - повторных использований SSL-сессий; - SSL-рукопожатий с истекшим таймаутом.

Раздел *Limit Conn*



Здесь приведена статистика зон `limit_conn` в контексте `stream`, формируемая на основе раздела API */status/stream/limit_ conns/*. Для каждой зоны представлены следующие данные:

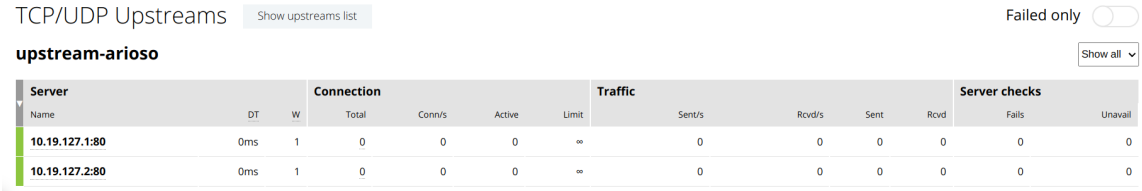
Zone	Имя зоны

Подсказка

Щелкните значок рядом с пунктом *Zone*, чтобы открыть или закрыть график со следующими показателями.

Passed	Общее количество проксированных соединений
Rejected	Общее количество сброшенных соединений
Exhausted	Общее количество соединений, сброшенных из-за переполнения хранилища зоны
Skipped	Общее количество соединений, переданных с нулевым или превосходящим 255 байт ключом

Вкладка *TCP/UDP Upstreams*



Внимание

Требует задать директиву *upstream* в контексте `stream`.

На этой вкладке в сводном виде отображается статистика мониторинга апстримов контекста `stream`, формируемая на основе раздела API */status/stream/upstreams/*.

- Кнопка *Show upstreams list* переключает отображение краткого списка апстримов с указанием числа проблемных апстримов и серверов.
- Переключатель *Failed only* включает и отключает режим вывода статистики по проблемным апстримам.
- Кнопка редактирования (только в Angie PRO) открывает виджет *редактирования апстрима*.
- Раскрывающийся список с правой стороны таблицы каждого апстрима позволяет отфильтровать серверы в определенном состоянии (*Up*, *Failed*, *Checking*, *Down*).

Для каждого апстрима представлены следующие данные:

Server	Имена, время простоя и веса серверов апстрима

Подсказка

Щелкните стрелку рядом с пунктом *Server*, чтобы отсортировать серверы по их состоянию или порядку в конфигурации.

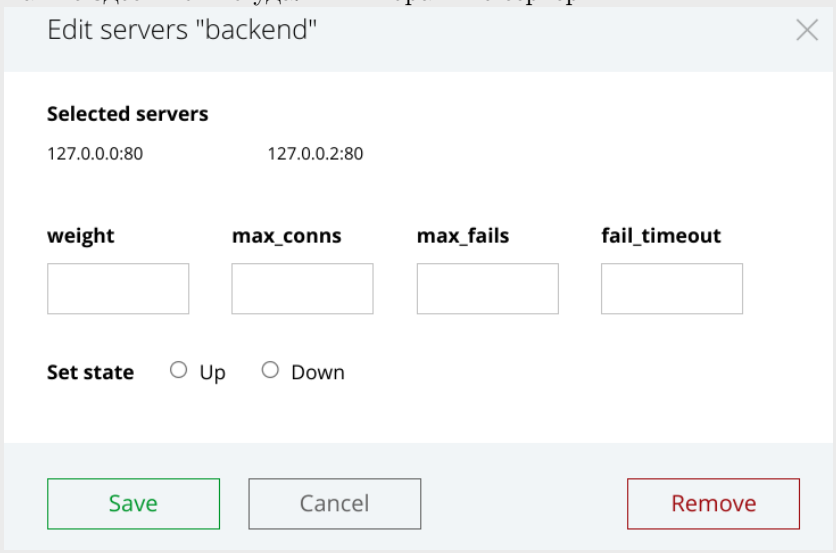
Requests	Общее количество и скорость обработки запросов
Responses	Количество ответов с разбиением по кодам статуса
Conns	Количество активных соединений и их максимальный предел, если он задан
Traffic	Скорость исходящего и входящего трафика, а также общие объемы исходящего и входящего трафика
Server checks	Количество неуспешных обращений к серверу и число раз, когда сервер считался недоступным (объект `health` в API)

Редактирование апстримов

В Angie PRO рядом с каждым апстримом есть кнопка редактирования; при нажатии она выводит еще две кнопки:

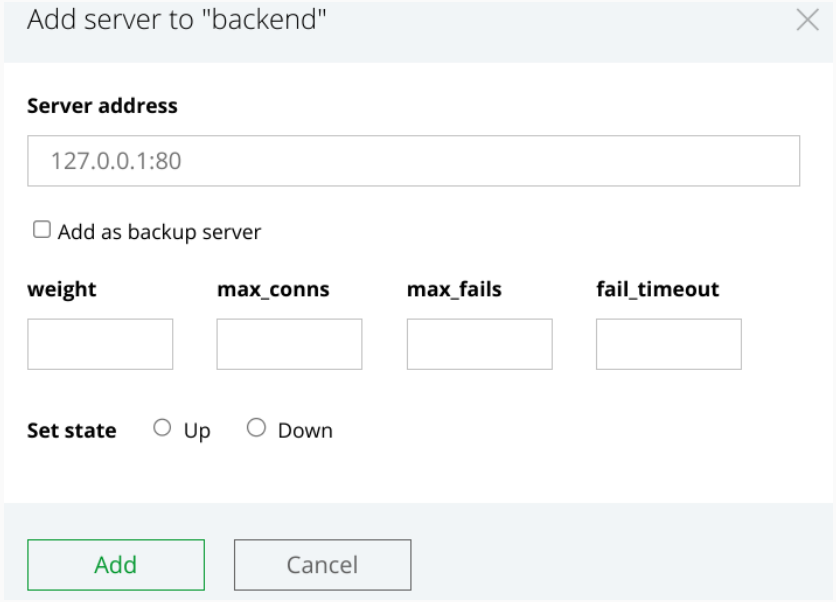
Edit selected

Редактирование выбранных серверов в составе апстрима. Позволяет одновременно задать для всех следующие параметры: *weight* (вес), *max_conns* (максимальный предел соединений), *max_fails* (максимальный предел сбоев, переводящий сервер в недоступные), *fail_timeout* (временное окно подсчета сбоев для *max_fails*), *state* (включен или отключен).
Также здесь можно удалить выбранные серверы.

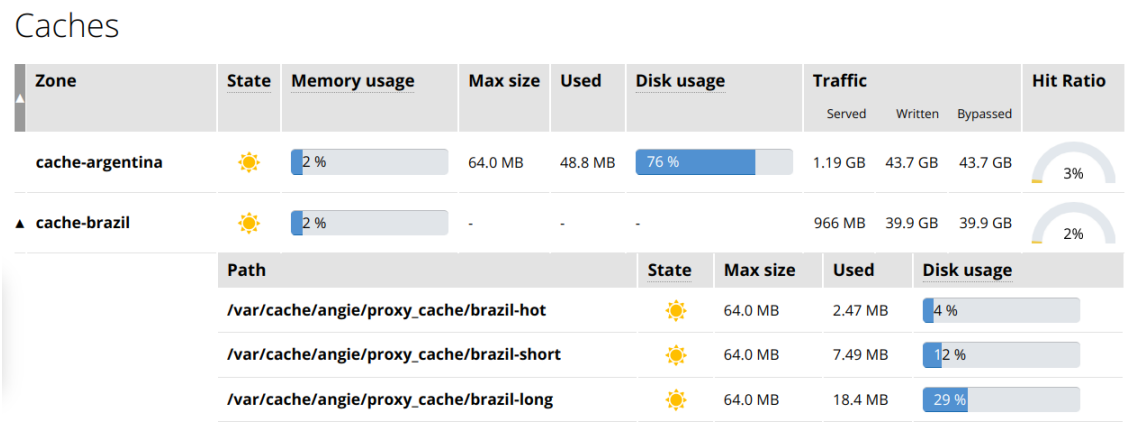


Add server

Добавление сервера в апстрим. Позволяет задать следующие параметры: *address* (адрес), *backup* (запасной сервер или нет), *weight* (вес), *max_conns* (максимальный предел соединений), *max_fails* (максимальный предел сбоев, переводящий сервер в недоступные), *fail_timeout* (временное окно подсчета сбоев для *max_fails*), *state* (включен или отключен).



Вкладка *Caches*



Внимание

Требует задать директиву *proxy_cache_path* в контексте `http`.

На этой вкладке в сводном виде отображается статистика мониторинга зон `proxy_cache` контекста `http`, формируемая на основе раздела API */status/http/caches/*. Для каждой зоны представлены следующие данные:

Zone	Имя зоны

Подсказка

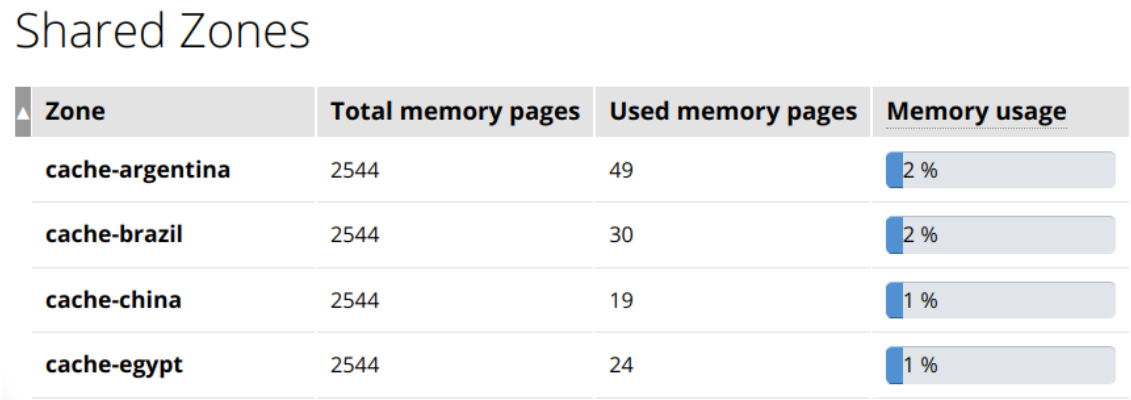
Щелкните значок рядом с пунктом *Zone*, чтобы открыть или закрыть списки *шардов* для всех зон, где они есть.

State	Состояние кэша: холодный (метаданные загружаются в память) или горячий (метаданные загружены)
Memory usage	Коэффициент использования памяти
Max size	Максимальный объем памяти
Used	Использованный объем памяти
Disk usage	Коэффициент использования дисковой памяти
Traffic	Переданный из кэша, записанный в кэш и возвращенный в обход кэша трафик
Hit ratio	Коэффициент попадания в кэш (отношение переданного из кэша трафика к общему объему) за временное окно, заданное в настройках

Если для зоны включен *шардинг*, то она обозначена как раскрывающийся список, в котором перечислены отдельные шарды:

Path	Путь шарда на диске
State	Состояние шарда: холодный (метаданные загружаются в память) или горячий (метаданные загружены)
Max size	Максимальный объем памяти
Used	Использованный объем памяти
Disk usage	Коэффициент использования дисковой памяти

Вкладка *Shared Zones*



На этой вкладке в сводном виде отображается статистика мониторинга **всех** зон разделяемой памяти для всех контекстов. Для каждой зоны представлены следующие данные:

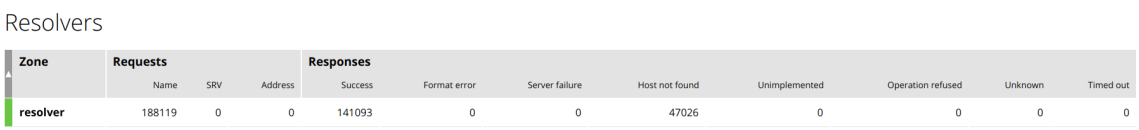
Zone	Имя зоны

Подсказка

Щелкните стрелку рядом с пунктом *Zone*, чтобы отсортировать зоны по размеру или порядку в конфигурации.

Total memory pages	Общее количество страниц памяти
Used memory pages	Количество используемых страниц памяти
Memory usage	Коэффициент использования памяти для зоны

Вкладка *Resolvers*



Внимание

Требует задать директиву *resolver* в контексте `http`.

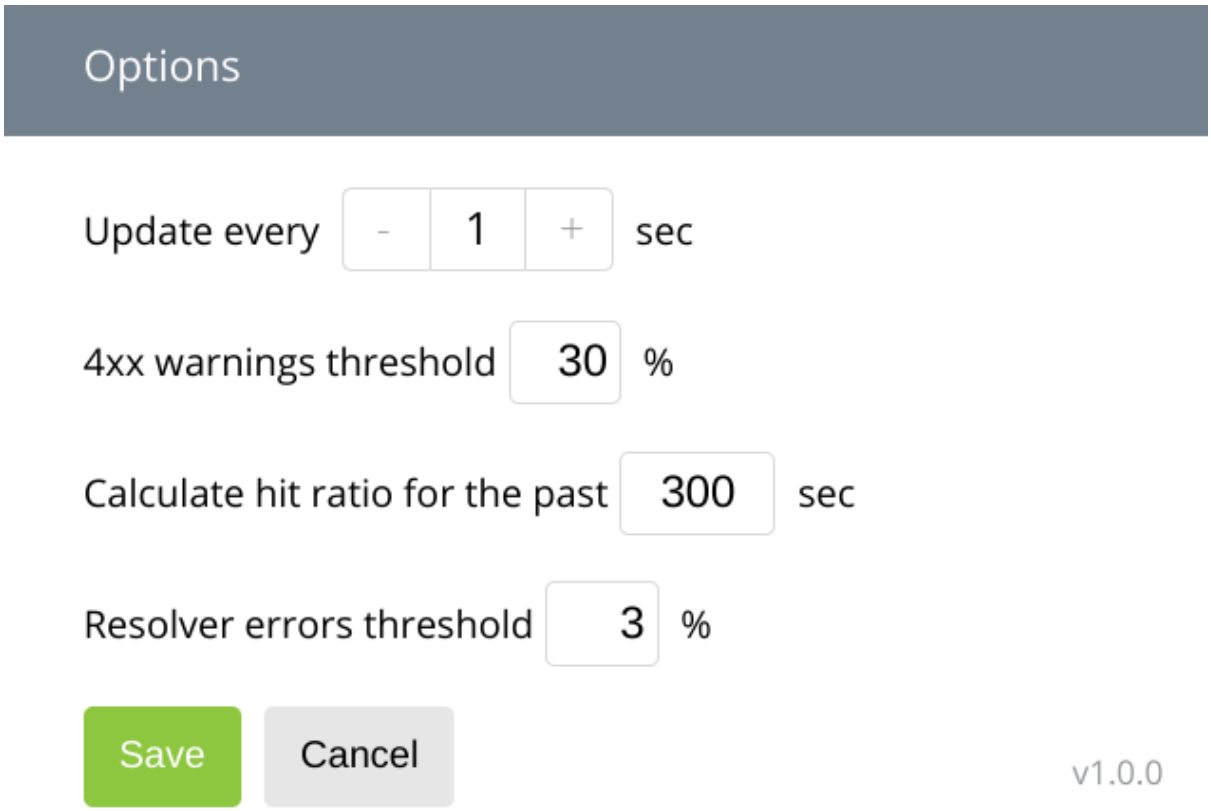
На этой вкладке в сводном виде отображается статистика запросов в зонах разделяемой памяти DNS, формируемая на основе раздела API */status/resolvers/*. Для каждой зоны представлены следующие данные:

Zone	Имя зоны

> **Подсказка**
>
> Щелкните стрелку рядом с пунктом *Zone*, чтобы отсортировать зоны по состоянию или порядку в конфигурации.

Requests	Количество запросов типа A и AAAA, SRV и PTR
Responses	Количество ответов с разделением по соответствующим кодам (*Format error*, *Server failure*, *Name Error*, *Not Implemented*, *Refused* и прочих)

Виджет *Настройки*



Позволяет настроить частоту обновления данных в консоли, пороговое соотношение статусов *4xx*, по достижении которого в соответствующих разделах, посвященных ответам сервера, появляются «желтые» предупреждения, а также временное окно для вычисления соотношения успешных попаданий в кэш (*Hit ratio*) и порог учета ошибок для резолвера, по достижении которого он станет «красным».

Панель управления консолью

На всех вкладках в середине левой части страницы есть выдвигающаяся панель с двумя кнопками; верхняя приостанавливает и вновь запускает обновление данных из API, а нижняя позволяет обновить данные вручную, когда обновление приостановлено.

3.3.5 Настройка панели Prometheus

Чтобы настроить панель Prometheus для Angie в Grafana, выполните следующие шаги:

1. Используя модуль *Prometheus*, добавьте следующую директиву *include* в блок `http` *файла конфигурации*:

   ```
   http {
       include prometheus_all.conf;

       # ...
   }
   ```

   Также добавьте соответствующую директиву *prometheus* внутри `location` в отдельном блоке `server` со специально отведенными для этой цели IP-адресом и портом, например:

   ```
   server {

       listen 192.168.1.100:80;

       location =/p8s {
           prometheus all;
       }

       # ...

   }
   ```

   Они включают экспорт метрик Angie в формате Prometheus в конечной точке, заданной в `location`.

2. Добавьте следующую конфигурацию в Prometheus, указав IP-адрес и порт, заданные ранее в `server`:

   ```
   scrape_configs:
     - job_name: "angie"
       scrape_interval: 15s
       metrics_path: "/p8s"
       static_configs:
         - targets: ["192.168.1.100:80"]
   ```

   Она будет собирать метрики каждые 15 секунд, используя настроенный на предыдущем шаге путь `/p8s`.

> **Примечание**
>
> Убедитесь, что значение глобального параметра `scrape_interval` не превышает указанное здесь значение.

3. Импортируйте панель Prometheus для Angie в Grafana.

ГЛАВА 4

Отладка

Если у вас возникла техническая проблема, но нужное решение не удалось найти в других разделах, задайте нам вопрос на форуме сообщества или в Telegram-канале.

Техническая поддержка для клиентов:

- https://support.angie.software
- support@angie.software

4.1 Отладочный лог

Отладочный лог следует включать перед самостоятельной диагностикой или по рекомендации технической поддержки.

Для этого запустите Angie PRO, используя исполняемый файл с поддержкой отладки:

Linux

В готовых пакетах для Linux файл `angie-debug` собран с включенным отладочным логом:

```
$ ls -l /usr/sbin/ | grep angie

   lrwxrwxrwx 1 root root      13 Sep 21 18:58 angie -> angie-nodebug
   -rwxr-xr-x 1 root root 1561224 Sep 21 18:58 angie-debug
   -rwxr-xr-x 1 root root 1426056 Sep 21 18:58 angie-nodebug
```

Настройте запуск `angie-debug`:

```
$ sudo ln -fs angie-debug /usr/sbin/angie
$ sudo angie -t && sudo service angie upgrade
```

Запустится *обновление исполняемого файла на лету*.

Чтобы вернуться к обычному исполняемому файлу после окончания отладки:

```
$ sudo ln -fs angie-nodebug /usr/sbin/angie
$ sudo angie -t && sudo service angie upgrade
```

FreeBSD

В готовых пакетах для FreeBSD файл `angie-debug` собран с включенным отладочным логом:

```
$ ls -l /usr/local/sbin/ | grep angie

  lrwxrwxrwx 1 root root      13 Sep 21 18:58 angie -> angie-nodebug
  -rwxr-xr-x 1 root root 1561224 Sep 21 18:58 angie-debug
  -rwxr-xr-x 1 root root 1426056 Sep 21 18:58 angie-nodebug
```

Настройте запуск `angie-debug`:

```
$ sudo ln -fs angie-debug /usr/local/sbin/angie
$ sudo angie -t && sudo service angie upgrade
```

Запустится *обновление исполняемого файла на лету*.

Чтобы вернуться к обычному исполняемому файлу после окончания отладки:

```
$ sudo ln -fs angie-nodebug /usr/local/sbin/angie
$ sudo angie -t && sudo service angie upgrade
```

Сборка из исходников

При самостоятельной сборке Angie PRO нужно включить отладку перед сборкой:

```
$ ./configure --with-debug ...
```

После установки команда `angie -V` позволяет убедиться, что отладочный лог включен:

```
$ angie -V

  ...
  configure arguments: --with-debug ...
```

Примечание

Использование исполняемого файла с поддержкой отладки может незначительно снизить производительность; включение же отладочного лога может заметно снизить ее, а также увеличить расход места на диске.

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

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

И перезагрузите конфигурацию:

```
$ sudo angie -t && sudo service angie reload
```

Примечание

Если переключиться на исполняемый файл без поддержки отладки, но оставить уровень `debug` в директиве *error_log*, Angie PRO будет добавлять записи в лог на уровне `info`.

Переопределение *error_log* в конфигурации без указания уровня `debug` отключит отладочный лог. Здесь переопределение лога на уровне *server* отключает отладочный лог для отдельного сервера:

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

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

Во избежание этого уберите строку, переопределяющую *error_log*, либо задайте в ней уровень debug:

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

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

4.1.1 Лог для отдельных адресов

Можно включить отладочный лог только для *указанных клиентских адресов*:

```
error_log /path/to/log;

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

4.1.2 Кольцевой буфер в памяти

Отладочный лог можно записывать в кольцевой буфер в памяти:

```
error_log memory:32m debug;
```

Запись в буфер в памяти на уровне debug не будет существенно влиять на производительность даже при высоких нагрузках. В этом случае лог можно извлечь при помощи GDB-скрипта, например:

```
set $log = ngx_cycle->log

while $log->writer != ngx_log_memory_writer
  set $log = $log->next
end

set $buf = (ngx_log_memory_buf_t *) $log->wdata
dump binary memory debug_log.txt $buf->start $buf->end
```

ГЛАВА 5

Права на интеллектуальную собственность

Документация на программный продукт Angie PRO является интеллектуальной собственностью ООО «Веб-Сервер», документация создана в результате изменения (переработки) документации на программный продукт Angie.

Алфавитный указатель

Символы

$1, 187, 265, 382, 413

A

absolute_redirect (*http*), 316
accept_mutex (*core*), 20
accept_mutex_delay (*core*), 20
access_log (*http*), 138
access_log (*stream*), 374
acme (*http*), 33
acme_client (*http*), 34
acme_client_path (*http*), 34
add_after_body (*http*), 36
add_before_body (*http*), 36
add_header (*http*), 119
add_trailer (*http*), 119
addition_types (*http*), 36
aio (*http*), 316
aio_write (*http*), 317
alias (*http*), 318
allow (*http*), 31
allow (*stream*), 359
ancient_browser (*http*), 73
ancient_browser_value (*http*), 73
api (*http*), 37
api_config_files (*http*), 38
auth_basic (*http*), 69
auth_basic_user_file (*http*), 69
auth_delay (*http*), 318
auth_http, 435
auth_http_header, 435
auth_http_pass_client_cert, 435
auth_http_timeout, 435
auth_request (*http*), 70
auth_request_set (*http*), 70
auto_redirect (*http*), 319
autoindex (*http*), 71
autoindex_exact_size (*http*), 71
autoindex_format (*http*), 71
autoindex_localtime (*http*), 72

B

bind_conn (*http*), 264
break (*http*), 212

C

charset (*http*), 75
charset_map (*http*), 75
charset_types (*http*), 76
chunked_transfer_encoding (*http*), 319
client_body_buffer_size (*http*), 319
client_body_in_file_only (*http*), 320
client_body_in_single_buffer (*http*), 320
client_body_temp_path (*http*), 320
client_body_timeout (*http*), 320
client_header_buffer_size (*http*), 321
client_header_timeout (*http*), 321
client_max_body_size (*http*), 321
connection_pool_size (*http*), 322
create_full_put_path (*http*), 78

D

daemon (*core*), 21
dav_access (*http*), 78
dav_methods (*http*), 78
debug_connection (*core*), 21
debug_points (*core*), 21
default_type (*http*), 322
deny (*http*), 31
deny (*stream*), 360
directio (*http*), 322
directio_alignment (*http*), 322
disable_symlinks (*http*), 323

E

empty_gif (*http*), 79
env (*core*), 22
error_log (*core*), 22
error_page (*http*), 324
etag (*http*), 324
events (*core*), 23
expires (*http*), 119

F

fastcgi_bind (*http*), 80
fastcgi_buffer_size (*http*), 80

fastcgi_buffering (*http*), 81
fastcgi_buffers (*http*), 81
fastcgi_busy_buffers_size (*http*), 81
fastcgi_cache (*http*), 82
fastcgi_cache_background_update (*http*), 82
fastcgi_cache_bypass (*http*), 82
fastcgi_cache_key (*http*), 82
fastcgi_cache_lock (*http*), 83
fastcgi_cache_lock_age (*http*), 83
fastcgi_cache_lock_timeout (*http*), 83
fastcgi_cache_max_range_offset (*http*), 83
fastcgi_cache_methods (*http*), 84
fastcgi_cache_min_uses (*http*), 84
fastcgi_cache_path (*http*), 84
fastcgi_cache_revalidate (*http*), 85
fastcgi_cache_use_stale (*http*), 86
fastcgi_cache_valid (*http*), 86
fastcgi_catch_stderr (*http*), 87
fastcgi_connect_timeout (*http*), 88
fastcgi_connection_drop (*http*), 88
fastcgi_force_ranges (*http*), 88
fastcgi_hide_header (*http*), 89
fastcgi_ignore_client_abort (*http*), 89
fastcgi_ignore_headers (*http*), 89
fastcgi_index (*http*), 90
fastcgi_intercept_errors (*http*), 90
fastcgi_keep_conn (*http*), 90
fastcgi_limit_rate (*http*), 90
fastcgi_max_temp_file_size (*http*), 91
fastcgi_next_upstream (*http*), 91
fastcgi_next_upstream_timeout (*http*), 92
fastcgi_next_upstream_tries (*http*), 92
fastcgi_no_cache (*http*), 93
fastcgi_param (*http*), 93
fastcgi_pass (*http*), 94
fastcgi_pass_header (*http*), 94
fastcgi_pass_request_body (*http*), 94
fastcgi_pass_request_headers (*http*), 95
fastcgi_read_timeout (*http*), 95
fastcgi_request_buffering (*http*), 95
fastcgi_send_lowat (*http*), 95
fastcgi_send_timeout (*http*), 96
fastcgi_socket_keepalive (*http*), 96
fastcgi_split_path_info (*http*), 96
fastcgi_store (*http*), 97
fastcgi_store_access (*http*), 98
fastcgi_temp_file_write_size (*http*), 98
fastcgi_temp_path (*http*), 98
flv (*http*), 100

G

geo (*http*), 101
geo (*stream*), 360
geoip_city (*http*), 103
geoip_city (*stream*), 362
geoip_country (*http*), 103
geoip_country (*stream*), 362
geoip_org (*http*), 103
geoip_org (*stream*), 363
geoip_proxy (*http*), 104
geoip_proxy_recursive (*http*), 104
google_perftools_profiles, 457
grpc_bind (*http*), 105
grpc_buffer_size (*http*), 105
grpc_connect_timeout (*http*), 105
grpc_connection_drop (*http*), 106
grpc_hide_header (*http*), 106
grpc_ignore_headers (*http*), 106
grpc_intercept_errors (*http*), 107
grpc_next_upstream (*http*), 107
grpc_next_upstream_timeout (*http*), 108
grpc_next_upstream_tries (*http*), 108
grpc_pass (*http*), 108
grpc_pass_header (*http*), 109
grpc_read_timeout (*http*), 109
grpc_send_timeout (*http*), 109
grpc_set_header (*http*), 110
grpc_socket_keepalive (*http*), 110
grpc_ssl_certificate (*http*), 110
grpc_ssl_certificate_key (*http*), 111
grpc_ssl_ciphers (*http*), 111
grpc_ssl_conf_command (*http*), 111
grpc_ssl_crl (*http*), 112
grpc_ssl_name (*http*), 112
grpc_ssl_password_file (*http*), 112
grpc_ssl_protocols (*http*), 112
grpc_ssl_server_name (*http*), 113
grpc_ssl_session_reuse (*http*), 113
grpc_ssl_trusted_certificate (*http*), 113
grpc_ssl_verify (*http*), 113
grpc_ssl_verify_depth (*http*), 114
gunzip (*http*), 114
gunzip_buffers (*http*), 114
gzip (*http*), 115
gzip_buffers (*http*), 115
gzip_comp_level (*http*), 116
gzip_disable (*http*), 116
gzip_http_version (*http*), 116
gzip_min_length (*http*), 116
gzip_proxied (*http*), 117
gzip_static (*http*), 118
gzip_types (*http*), 117
gzip_vary (*http*), 117

H

hash (*http*), 266
hash (*stream*), 414
http (*http*), 325
http2 (*http*), 308
http2_body_preread_size (*http*), 308
http2_chunk_size (*http*), 308
http2_max_concurrent_pushes (*http*), 308
http2_max_concurrent_streams (*http*), 308
http2_push (*http*), 309
http2_push_preload (*http*), 309
http2_recv_buffer_size (*http*), 309

http3 (*http*), 311
http3_hq (*http*), 311
http3_max_concurrent_streams (*http*), 311
http3_stream_buffer_size (*http*), 311

I

if (*http*), 213
if_modified_since (*http*), 325
ignore_invalid_headers (*http*), 325
image_filter (*http*), 121
image_filter_buffer (*http*), 122
image_filter_interlace (*http*), 122
image_filter_jpeg_quality (*http*), 122
image_filter_sharpen (*http*), 123
image_filter_transparency (*http*), 123
image_filter_webp_quality (*http*), 123
imap_auth, 438
imap_capabilities, 438
imap_client_buffer, 439
include (*core*), 23
index (*http*), 124
internal (*http*), 325
ip_hash (*http*), 267

J

js_access (*stream*), 365
js_body_filter (*http*), 126
js_content (*http*), 127
js_fetch_buffer_size (*http*), 127
js_fetch_buffer_size (*stream*), 365
js_fetch_ciphers (*http*), 127
js_fetch_ciphers (*stream*), 366
js_fetch_max_response_buffer_size (*http*), 128
js_fetch_max_response_buffer_size (*stream*), 366
js_fetch_protocols (*http*), 128
js_fetch_protocols (*stream*), 366
js_fetch_timeout (*http*), 128
js_fetch_timeout (*stream*), 366
js_fetch_trusted_certificate (*http*), 128
js_fetch_trusted_certificate (*stream*), 367
js_fetch_verify (*http*), 129
js_fetch_verify (*stream*), 367
js_fetch_verify_depth (*http*), 129
js_fetch_verify_depth (*stream*), 367
js_filter (*stream*), 367
js_header_filter (*http*), 129
js_import (*http*), 129
js_import (*stream*), 368
js_path (*http*), 130
js_path (*stream*), 368
js_preload_object (*http*), 130
js_preload_object (*stream*), 369
js_preread (*stream*), 369
js_set (*http*), 130
js_set (*stream*), 370
js_shared_dict_zone (*http*), 131
js_shared_dict_zone (*stream*), 370
js_var (*http*), 132
js_var (*stream*), 371

K

keepalive (*http*), 267
keepalive_disable (*http*), 326
keepalive_requests (*http*), 269, 326
keepalive_time (*http*), 269, 327
keepalive_timeout (*http*), 270, 327

L

large_client_header_buffers (*http*), 327
least_conn (*http*), 270
least_conn (*stream*), 415
least_time (*http*), 270
least_time (*stream*), 415
limit_conn (*http*), 133
limit_conn (*stream*), 372
limit_conn_dry_run (*http*), 134
limit_conn_dry_run (*stream*), 372
limit_conn_log_level (*http*), 134
limit_conn_log_level (*stream*), 372
limit_conn_status (*http*), 134
limit_conn_zone (*http*), 134
limit_conn_zone (*stream*), 373
limit_except (*http*), 328
limit_rate (*http*), 328
limit_rate_after (*http*), 329
limit_req (*http*), 135
limit_req_dry_run (*http*), 136
limit_req_log_level (*http*), 136
limit_req_status (*http*), 137
limit_req_zone (*http*), 137
lingering_close (*http*), 329
lingering_time (*http*), 330
lingering_timeout (*http*), 330
listen, 452
listen (*http*), 330
listen (*stream*), 424
load_module (*core*), 24
location (*http*), 334
lock_file (*core*), 24
log_format (*http*), 139
log_format (*stream*), 375
log_not_found (*http*), 336
log_subrequest (*http*), 336

M

mail, 454
map (*http*), 141
map (*stream*), 376
map_hash_bucket_size (*http*), 142
map_hash_bucket_size (*stream*), 378
map_hash_max_size (*http*), 143
map_hash_max_size (*stream*), 378
master_process (*core*), 24
max_commands, 454
max_errors, 454

max_ranges (*http*), 337
memcached_bind (*http*), 143
memcached_buffer_size (*http*), 144
memcached_connect_timeout (*http*), 144
memcached_gzip_flag (*http*), 144
memcached_next_upstream (*http*), 144
memcached_next_upstream_timeout (*http*), 145
memcached_next_upstream_tries (*http*), 145
memcached_pass (*http*), 146
memcached_read_timeout (*http*), 146
memcached_send_timeout (*http*), 146
memcached_socket_keepalive (*http*), 147
merge_slashes (*http*), 337
min_delete_depth (*http*), 78
mirror (*http*), 148
mirror_request_body (*http*), 148
modern_browser (*http*), 74
modern_browser_value (*http*), 74
mp4 (*http*), 150
mp4_buffer_size (*http*), 150
mp4_limit_rate (*http*), 150
mp4_limit_rate_after (*http*), 151
mp4_max_buffer_size (*http*), 150
mp4_start_key_frame (*http*), 151
mqtt_preread (*stream*), 379
msie_padding (*http*), 337
msie_refresh (*http*), 338
multi_accept (*core*), 25

O

open_file_cache (*http*), 338
open_file_cache_errors (*http*), 338
open_file_cache_min_uses (*http*), 339
open_file_cache_valid (*http*), 339
open_log_file_cache (*http*), 140
open_log_file_cache (*stream*), 375
output_buffers (*http*), 339
override_charset (*http*), 76

P

pass (*stream*), 380
pcre_jit (*core*), 25
perl (*http*), 153
perl_modules (*http*), 153
perl_require (*http*), 153
perl_set (*http*), 154
pid (*core*), 25
pop3_auth, 439
pop3_capabilities, 439
port_in_redirect (*http*), 339
postpone_output (*http*), 340
preread_buffer_size (*stream*), 427
preread_timeout (*stream*), 427
prometheus (*http*), 175
prometheus_template (*http*), 175
protocol, 455
proxy_bind (*http*), 178
proxy_bind (*stream*), 381
proxy_buffer, 440
proxy_buffer_size (*http*), 178
proxy_buffer_size (*stream*), 381
proxy_buffering (*http*), 178
proxy_buffers (*http*), 179
proxy_busy_buffers_size (*http*), 179
proxy_cache (*http*), 179
proxy_cache_background_update (*http*), 180
proxy_cache_bypass (*http*), 181
proxy_cache_convert_head (*http*), 181
proxy_cache_key (*http*), 181
proxy_cache_lock (*http*), 182
proxy_cache_lock_age (*http*), 182
proxy_cache_lock_timeout (*http*), 182
proxy_cache_max_range_offset (*http*), 182
proxy_cache_methods (*http*), 183
proxy_cache_min_uses (*http*), 183
proxy_cache_path (*http*), 183
proxy_cache_revalidate (*http*), 185
proxy_cache_use_stale (*http*), 185
proxy_cache_valid (*http*), 185
proxy_connect_timeout (*http*), 186
proxy_connect_timeout (*stream*), 381
proxy_cookie_domain (*http*), 187
proxy_cookie_flags (*http*), 188
proxy_cookie_path (*http*), 188
proxy_download_rate (*stream*), 382
proxy_force_ranges (*http*), 189
proxy_half_close (*stream*), 383
proxy_headers_hash_bucket_size (*http*), 189
proxy_headers_hash_max_size (*http*), 189
proxy_hide_header (*http*), 189
proxy_http3_hq (*http*), 190
proxy_http3_max_concurrent_streams (*http*), 190
proxy_http3_stream_buffer_size (*http*), 190
proxy_http_version (*http*), 190
proxy_ignore_client_abort (*http*), 191
proxy_ignore_headers (*http*), 191
proxy_intercept_errors (*http*), 191
proxy_limit_rate (*http*), 191
proxy_max_temp_file_size (*http*), 192
proxy_method (*http*), 192
proxy_next_upstream (*http*), 193
proxy_next_upstream (*stream*), 383
proxy_next_upstream_timeout (*http*), 194
proxy_next_upstream_timeout (*stream*), 383
proxy_next_upstream_tries (*http*), 194
proxy_next_upstream_tries (*stream*), 383
proxy_no_cache (*http*), 194
proxy_pass (*http*), 195
proxy_pass (*stream*), 384
proxy_pass_error_message, 440
proxy_pass_header (*http*), 196
proxy_pass_request_body (*http*), 196
proxy_pass_request_headers (*http*), 196
proxy_protocol, 440
proxy_protocol (*stream*), 384

proxy_protocol_timeout (*stream*), 427
proxy_quic_active_connection_id_limit (*http*), 197
proxy_quic_gso (*http*), 197
proxy_quic_host_key (*http*), 197
proxy_read_timeout (*http*), 197
proxy_redirect (*http*), 198
proxy_request_buffering (*http*), 199
proxy_requests (*stream*), 384
proxy_responses (*stream*), 384
proxy_send_lowat (*http*), 199
proxy_send_timeout (*http*), 200
proxy_set_body (*http*), 200
proxy_set_header (*http*), 200
proxy_smtp_auth, 440
proxy_socket_keepalive (*http*), 201
proxy_socket_keepalive (*stream*), 385
proxy_ssl (*stream*), 385
proxy_ssl_certificate (*http*), 201
proxy_ssl_certificate (*stream*), 385
proxy_ssl_certificate_key (*http*), 202
proxy_ssl_certificate_key (*stream*), 386
proxy_ssl_ciphers (*http*), 202
proxy_ssl_ciphers (*stream*), 386
proxy_ssl_conf_command (*http*), 202
proxy_ssl_conf_command (*stream*), 386
proxy_ssl_crl (*http*), 203
proxy_ssl_crl (*stream*), 387
proxy_ssl_name (*http*), 203
proxy_ssl_name (*stream*), 387
proxy_ssl_ntls (*http*), 203
proxy_ssl_ntls (*stream*), 387
proxy_ssl_password_file (*http*), 204
proxy_ssl_password_file (*stream*), 388
proxy_ssl_protocols (*http*), 204
proxy_ssl_protocols (*stream*), 388
proxy_ssl_server_name (*http*), 204
proxy_ssl_server_name (*stream*), 388
proxy_ssl_session_reuse (*http*), 205
proxy_ssl_session_reuse (*stream*), 389
proxy_ssl_trusted_certificate (*http*), 205
proxy_ssl_trusted_certificate (*stream*), 389
proxy_ssl_verify (*http*), 205
proxy_ssl_verify (*stream*), 389
proxy_ssl_verify_depth (*http*), 205
proxy_ssl_verify_depth (*stream*), 389
proxy_store (*http*), 206
proxy_store_access (*http*), 207
proxy_temp_file_write_size (*http*), 207
proxy_temp_path (*http*), 207
proxy_timeout, 441
proxy_timeout (*stream*), 390
proxy_upload_rate (*stream*), 390

Q

queue (*http*), 271
quic_active_connection_id_limit (*http*), 312
quic_bpf (*http*), 312
quic_gso (*http*), 312
quic_host_key (*http*), 312
quic_retry (*http*), 313

R

random (*http*), 271
random (*stream*), 416
random_index (*http*), 209
rdp_preread (*stream*), 392
read_ahead (*http*), 340
real_ip_header (*http*), 209
real_ip_recursive (*http*), 210
recursive_error_pages (*http*), 340
referer_hash_bucket_size (*http*), 211
referer_hash_max_size (*http*), 211
request_pool_size (*http*), 340
reset_timedout_connection (*http*), 341
resolver, 455
resolver (*http*), 341
resolver (*stream*), 427
resolver_timeout, 456
resolver_timeout (*http*), 342
resolver_timeout (*stream*), 428
response_time_factor (*http*), 272
response_time_factor (*stream*), 416
return (*http*), 214
return (*stream*), 393
rewrite (*http*), 214
rewrite_log (*http*), 215
root (*http*), 342

S

satisfy (*http*), 342
scgi_bind (*http*), 217
scgi_buffer_size (*http*), 217
scgi_buffering (*http*), 218
scgi_buffers (*http*), 218
scgi_busy_buffers_size (*http*), 218
scgi_cache (*http*), 219
scgi_cache_background_update (*http*), 219
scgi_cache_bypass (*http*), 219
scgi_cache_key (*http*), 220
scgi_cache_lock (*http*), 220
scgi_cache_lock_age (*http*), 220
scgi_cache_lock_timeout (*http*), 220
scgi_cache_max_range_offset (*http*), 221
scgi_cache_methods (*http*), 221
scgi_cache_min_uses (*http*), 221
scgi_cache_path (*http*), 221
scgi_cache_revalidate (*http*), 223
scgi_cache_use_stale (*http*), 223
scgi_cache_valid (*http*), 224
scgi_connect_timeout (*http*), 224
scgi_connection_drop (*http*), 225
scgi_force_ranges (*http*), 225
scgi_hide_header (*http*), 225
scgi_ignore_client_abort (*http*), 225
scgi_ignore_headers (*http*), 226

scgi_intercept_errors (*http*), 226
scgi_limit_rate (*http*), 226
scgi_max_temp_file_size (*http*), 227
scgi_next_upstream (*http*), 227
scgi_next_upstream_timeout (*http*), 228
scgi_next_upstream_tries (*http*), 228
scgi_no_cache (*http*), 229
scgi_param (*http*), 229
scgi_pass (*http*), 229
scgi_pass_header (*http*), 230
scgi_pass_request_body (*http*), 230
scgi_pass_request_headers (*http*), 230
scgi_read_timeout (*http*), 231
scgi_request_buffering (*http*), 231
scgi_send_timeout (*http*), 231
scgi_socket_keepalive (*http*), 231
scgi_store (*http*), 232
scgi_store_access (*http*), 233
scgi_temp_file_write_size (*http*), 233
scgi_temp_path (*http*), 233
secure_link (*http*), 234
secure_link_md5 (*http*), 234
secure_link_secret (*http*), 235
send_lowat (*http*), 343
send_timeout (*http*), 343
sendfile (*http*), 343
sendfile_max_chunk (*http*), 344
server, 456
server (*http*), 272, 344
server (*stream*), 410, 428
server_name, 456
server_name (*http*), 344
server_name (*stream*), 428
server_name_in_redirect (*http*), 346
server_names_hash_bucket_size (*http*), 347
server_names_hash_bucket_size (*stream*), 430
server_names_hash_max_size (*http*), 347
server_names_hash_max_size (*stream*), 430
server_tokens (*http*), 347
set (*http*), 215
set (*stream*), 394
set_real_ip_from, 442
set_real_ip_from (*http*), 209
set_real_ip_from (*stream*), 393
slice (*http*), 237
smtp_auth, 442
smtp_capabilities, 442
smtp_client_buffer, 443
smtp_greeting_delay, 443
source_charset (*http*), 76
split_clients (*http*), 238
split_clients (*stream*), 395
ssi (*http*), 239
ssi_last_modified (*http*), 239
ssi_min_file_chunk (*http*), 239
ssi_silent_errors (*http*), 239
ssi_types (*http*), 240
ssi_value_length (*http*), 240
ssl_alpn (*stream*), 396
ssl_buffer_size (*http*), 245
ssl_certificate, 444
ssl_certificate (*http*), 245
ssl_certificate (*stream*), 396
ssl_certificate_key, 445
ssl_certificate_key (*http*), 246
ssl_certificate_key (*stream*), 397
ssl_ciphers, 445
ssl_ciphers (*http*), 247
ssl_ciphers (*stream*), 398
ssl_client_certificate, 445
ssl_client_certificate (*http*), 247
ssl_client_certificate (*stream*), 398
ssl_conf_command, 446
ssl_conf_command (*http*), 248
ssl_conf_command (*stream*), 398
ssl_crl, 446
ssl_crl (*http*), 248
ssl_crl (*stream*), 399
ssl_dhparam, 446
ssl_dhparam (*http*), 248
ssl_dhparam (*stream*), 399
ssl_early_data (*http*), 249
ssl_ecdh_curve, 447
ssl_ecdh_curve (*http*), 249
ssl_ecdh_curve (*stream*), 399
ssl_engine (*core*), 26
ssl_handshake_timeout (*stream*), 400
ssl_ntls (*http*), 250
ssl_ntls (*stream*), 400
ssl_ocsp (*http*), 250
ssl_ocsp_cache (*http*), 251
ssl_ocsp_responder (*http*), 251
ssl_password_file, 447
ssl_password_file (*http*), 251
ssl_password_file (*stream*), 401
ssl_prefer_server_ciphers, 448
ssl_prefer_server_ciphers (*http*), 252
ssl_prefer_server_ciphers (*stream*), 401
ssl_preread (*stream*), 408
ssl_protocols, 448
ssl_protocols (*http*), 252
ssl_protocols (*stream*), 401
ssl_reject_handshake (*http*), 252
ssl_session_cache, 448
ssl_session_cache (*http*), 253
ssl_session_cache (*stream*), 402
ssl_session_ticket_key, 449
ssl_session_ticket_key (*http*), 253
ssl_session_ticket_key (*stream*), 402
ssl_session_tickets, 450
ssl_session_tickets (*http*), 254
ssl_session_tickets (*stream*), 403
ssl_session_timeout, 450
ssl_session_timeout (*http*), 254
ssl_session_timeout (*stream*), 403
ssl_stapling (*http*), 254

ssl_stapling_file (*http*), 255
ssl_stapling_responder (*http*), 255
ssl_stapling_verify (*http*), 255
ssl_trusted_certificate, 450
ssl_trusted_certificate (*http*), 256
ssl_trusted_certificate (*stream*), 403
ssl_verify_client, 450
ssl_verify_client (*http*), 256
ssl_verify_client (*stream*), 404
ssl_verify_depth, 451
ssl_verify_depth (*http*), 256
ssl_verify_depth (*stream*), 404
starttls, 451
state (*http*), 275
state (stream) ((stream upstream module), 412
status_zone (*http*), 347
status_zone (*stream*), 430
sticky (*http*), 275
sticky (*stream*), 417
sticky_secret (*http*), 277
sticky_secret (*stream*), 419
sticky_strict (*http*), 278
sticky_strict (*stream*), 419
stream (*stream*), 430
stub_status (*http*), 261
sub_filter (*http*), 262
sub_filter_last_modified (*http*), 263
sub_filter_once (*http*), 263
sub_filter_types (*http*), 263
subrequest_output_buffer_size (*http*), 348

T

tcp_nodelay (*http*), 348
tcp_nodelay (*stream*), 431
tcp_nopush (*http*), 348
thread_pool (*core*), 26
timeout, 457
timer_resolution (*core*), 26
try_files (*http*), 348
types (*http*), 350
types_hash_bucket_size (*http*), 351
types_hash_max_size (*http*), 351

U

underscores_in_headers (*http*), 351
uninitialized_variable_warn (*http*), 215
upstream (*http*), 278
upstream (*stream*), 409
upstream_probe (*http*), 282
upstream_probe (*stream*), 421
upstream_probe_timeout (*stream*), 390
use (*core*), 27
user (*core*), 27
userid (*http*), 285
userid_domain (*http*), 285
userid_expires (*http*), 285
userid_flags (*http*), 285
userid_mark (*http*), 285
userid_name (*http*), 286
userid_p3p (*http*), 286
userid_path (*http*), 286
userid_service (*http*), 286
uwsgi_bind (*http*), 287
uwsgi_buffer_size (*http*), 288
uwsgi_buffering (*http*), 288
uwsgi_buffers (*http*), 288
uwsgi_busy_buffers_size (*http*), 289
uwsgi_cache (*http*), 289
uwsgi_cache_background_update (*http*), 289
uwsgi_cache_bypass (*http*), 290
uwsgi_cache_key (*http*), 290
uwsgi_cache_lock (*http*), 290
uwsgi_cache_lock_age (*http*), 290
uwsgi_cache_lock_timeout (*http*), 291
uwsgi_cache_max_range_offset (*http*), 291
uwsgi_cache_methods (*http*), 291
uwsgi_cache_min_uses (*http*), 291
uwsgi_cache_path (*http*), 292
uwsgi_cache_revalidate (*http*), 293
uwsgi_cache_use_stale (*http*), 293
uwsgi_cache_valid (*http*), 294
uwsgi_connect_timeout (*http*), 295
uwsgi_connection_drop (*http*), 295
uwsgi_force_ranges (*http*), 295
uwsgi_hide_header (*http*), 295
uwsgi_ignore_client_abort (*http*), 296
uwsgi_ignore_headers (*http*), 296
uwsgi_intercept_errors (*http*), 296
uwsgi_limit_rate (*http*), 297
uwsgi_max_temp_file_size (*http*), 297
uwsgi_modifier1 (*http*), 297
uwsgi_modifier2 (*http*), 298
uwsgi_next_upstream (*http*), 298
uwsgi_next_upstream_timeout (*http*), 299
uwsgi_next_upstream_tries (*http*), 299
uwsgi_no_cache (*http*), 299
uwsgi_pass (*http*), 300
uwsgi_pass_header (*http*), 300
uwsgi_pass_request_body (*http*), 300
uwsgi_pass_request_headers (*http*), 300
uwsgi_read_timeout (*http*), 301
uwsgi_request_buffering (*http*), 301
uwsgi_send_timeout (*http*), 301
uwsgi_socket_keepalive (*http*), 301
uwsgi_ssl_certificate (*http*), 302
uwsgi_ssl_certificate_key (*http*), 302
uwsgi_ssl_ciphers (*http*), 302
uwsgi_ssl_conf_command (*http*), 302
uwsgi_ssl_crl (*http*), 303
uwsgi_ssl_name (*http*), 303
uwsgi_ssl_password_file (*http*), 303
uwsgi_ssl_protocols (*http*), 304
uwsgi_ssl_server_name (*http*), 304
uwsgi_ssl_session_reuse (*http*), 304
uwsgi_ssl_trusted_certificate (*http*), 304

uwsgi_ssl_verify (*http*), 305
uwsgi_ssl_verify_depth (*http*), 305
uwsgi_store (*http*), 305
uwsgi_store_access (*http*), 306
uwsgi_temp_file_write_size (*http*), 306
uwsgi_temp_path (*http*), 306

V

valid_referers (*http*), 211
variables_hash_bucket_size (*http*), 352
variables_hash_bucket_size (*stream*), 431
variables_hash_max_size (*http*), 352
variables_hash_max_size (*stream*), 431

W

worker_aio_requests (*core*), 27
worker_connections (*core*), 28
worker_cpu_affinity (*core*), 28
worker_priority (*core*), 29
worker_processes (*core*), 29
worker_rlimit_core (*core*), 29
worker_rlimit_nofile (*core*), 29
worker_shutdown_timeout (*core*), 30
working_directory (*core*), 30

X

xclient, 441
xml_entities (*http*), 314
xslt_last_modified (*http*), 314
xslt_param (*http*), 314
xslt_string_param (*http*), 315
xslt_stylesheet (*http*), 315
xslt_types (*http*), 316

Z

zone (*http*), 279
zone (*stream*), 413