

# **Руководство администратора**

для серверного ПО Manul

2023

## Содержание

Описание .....	3
Системные требования .....	3
Установка.....	4
Настройка и оптимизация операционной системы .....	5
Первичная настройка.....	6
Работа с потоками. ....	9
Проигрывание потоков. ....	10
Авторизация доступа при проигрывании потока .....	11

## Описание

Серверное программное обеспечение «MANUL» является программным обеспечением для провайдеров облачного видеонаблюдения, реализующим следующие функции:

- Прием видео-потокa с источника по протоколам RTSP, RTMP;
- Вещание принятых потоков по протоколам RTSP, RTMP, HLS, HTTP-TS;
- Перекодирование аудио из семейства форматов G711 в формат AAC для вещания в HLS;
- Запись принятых потоков в архив с настраиваемой глубиной хранения и вещание записей из архива по протоколу HLS;
- Скачивание фрагментов архива в формате MPEG-TS;
- Авторизация доступа к вещанию потоков с сервера по белому списку адресов и/или отправкой HTTP-запроса к авторизационному серверу;
- REST-API для управления потоками и получения статистики;

## Системные требования

- Сервер под управлением ОС Debian linux версии не ниже 10, или Ubuntu linux версии не ниже 16. Характеристики сервера зависят от планируемого количества обрабатываемых потоков, обслуживаемых клиентов и глубины хранимого архива. Ниже приведен пример характеристик серверов:
  - для работы со **100 потоками и глубиной хранимого архива 5 дней**:
    - Процессор: x86-64 с тактовой частотой 2 ГГц и количеством ядер 8.
    - Оперативная память: 16 GB DDR4
    - HDD для хранения архива: 5 \* 6TB / Raid 5
    - SSD для установки системы и хранения индексной БД архива: 256 GB

- Сетевой интерфейс: 1 gb/s.
- для работы с 550 потоками и глубиной хранения архива 5 дней:
  - Платформа Supermicro 6039P-E1CR16H
  - Процессор 2 \* Intel Xeon Silver 4210
  - Оперативная память 32 GB DDR4 ECC Registered
  - HDD для хранения архива: 16 \* 6TB / SW Raid 50
  - SSD для установки системы и хранения индексной БД архива: 2 \* 480 GB
  - HBA контроллер.
- для работы с 600 потоками и глубиной хранения архива 30 дней:
  - Платформа Supermicro 6049P-E1CR36H
  - Процессор 2 \* Intel Xeon Silver 4210
  - Оперативная память 64 GB DDR4 ECC Registered
  - HDD для хранения архива: 36 \* 12TB / HW Raid 60
  - SSD для установки системы и хранения индексной БД архива: 2 \* 480 GB
  - Аппаратный RAID контроллер с энергонезависимым кэшем.
- Доступ к сети интернет.

## Установка

Установка серверного ПО Manul производится с консоли. Для установки необходимы права суперпользователя.

1. **Установка с репозитория пакетов.** Для получения доступа к репозиторию пакетов необходимо сообщить публичный IP-адрес сервера, на который будет устанавливаться ПО.

1.1.Подключить репозиторий пакетов:

```
echo "deb http://repo.iptv.ufanet.ru/debian xenial main" > /etc/apt/sources.list.d/manul.list
```

1.2.Подключить репозиторий пакетов:

```
wget --quiet -O - https://repo.iptv.ufanet.ru/public.key | apt-key add -
```

1.3.Обновить список пакетов:

```
apt-get update
```

1.4.Установить пакет manul:

```
apt-get install manul
```

2. **Установка файла пакета локально.** Подходит для установки на серверах, не имеющих доступа к сети интернет. Установочный пакет предоставляется разработчиком.

2.1.Скопировать установочный пакет на сервер;

2.2.Установить пакет:

```
dpkg -i manul.deb
```

## Настройка и оптимизация операционной системы

Для хранения архивов рекомендуется использовать отдельный раздел, с файловой системой XFS. Рекомендации по настройке файловой системы:

- в случае использования программного RAID при создании массива рекомендуется использовать опции `--bitmap=internal --bitmap-chunk=131072`. Также в автозагрузку, например в `rc.local`, добавить команды:  

```
blockdev --setra 65536 /dev/md1
blockdev --setra 65536 /dev/md2
echo 32768 > /sys/block/md1/md/stripe_cache_size
echo 32768 > /sys/block/md2/md/stripe_cache_size
```
- при создании файловой системы рекомендуется использовать опции `-δ συ=512к -δ σω=12 -λ συ=4096` где `sw=12` общее количество дисков RAID массива за исключением избыточных дисков. Например для RAID60, состоящего из 2 массивов RAID6 по 8 дисков `sw` будет равняться 12.
- для монтирования раздела рекомендуется использовать опции `async,noatime,nodiratime,attr2,nobarrier,logbufs=8,logbsize=256k,allocsize=64M`
- В случае использования программного RAID рекомендуется ограничить скорость ребилда массива в `sysctl dev.raid.speed_limit_max=25000`
- рекомендации для настройки `sysctl`:  

```
kernel.pid_max = 419430
net.core.somaxconn = 65535
net.core.netdev_max_backlog = 10000
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 87380 33554432
net.ipv4.tcp_wmem = 4096 65536 33554432
net.core.wmem_default = 33554432
net.core.rmem_default = 33554432
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_tw_reuse = 1
net.ipv4.conf.default.rp_filter=0
net.ipv4.conf.all.rp_filter=0
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
kernel.panic=15
dev.raid.speed_limit_max=25000
vm.swappiness=10
vm.overcommit_memory=2
vm.overcommit_ratio=300
vm.min_free_kbytes=1048576
fs.file-max = 105257912
```

fs.nr\_open = 8388608

## Первичная настройка

После установки ПО оно запускается автоматически с конфигурацией по-умолчанию. Изменение конфигурации производится редактированием файла `/etc/manul/manul.conf.json`. Файл конфигурации имеет формат JSON, поэтому при его редактировании необходимо соблюдать требования синтаксиса JSON. Конфигурация применяется один раз при запуске ПО, поэтому после редактирования файла конфигурации ПО необходимо перезапустить командой `systemctl restart manul.service` ИЛИ `service manul restart`.

Описание полей файла конфигурации:

- **conf\_version:** версия конфигурации. Тип: строка. Может использоваться для контроля версий конфигураций;
- **server\_auth:** раздел для конфигурации доступа к REST-API. Включает в себя поля:
  - **login:** имя пользователя для доступа к REST-API. Тип: строка;
  - **password:** пароль пользователя для доступа к REST-API. Тип: строка;
  - **allowed\_ips:** список подсетей, которым разрешен доступ к REST-API. Тип: список строк. Элемент списка может представлять собой одиночный IP-адрес или CIDR-префикс.
- **auth\_backends:** раздел для конфигурации бэкендов аутентификации для проигрывания видеопотоков. Тип: список, элемент списка: раздел, представляющий настройки одного бэкенда, поля:
  - **name:** имя бэкенда. Тип: строка. Используется для указания имени бэкенда аутентификации при создании/редактировании потока;
  - **type:** тип бэкенда. Тип: строка. Используется для указания метода аутентификации. Возможные значения: `url`, `ip`;
  - **url:** урл бэкенда. Тип: строка. Используется при типе бэкенда `url`;
  - **allowed\_ips:** список IP-адресов, которым разрешено проигрывание потоков. Тип: список строк. Элемент списка может представлять собой одиночный IP-адрес или CIDR-префикс.
- **task\_workers:** количество одновременно выполняемых служебных задач. Тип: целое число. Определяет максимальное количество одновременно выполняемых фоновых задач, таких как очистка старых архивных записей.
- **rtmp:** раздел с настройками RTMP сервера. Включает в себя поля:

- **enable:** флаг включения сервера. Тип: булево значение. При выключенном состоянии прослушивание RTMP-подключений запускаться не будет.
- **addr:** локальный адрес для прослушивания RTMP подключений. Тип: строка. Значение должно содержать адрес локального сетевого интерфейса и порт разделенные двоеточием;
- **gop\_num:** объем кэша для быстрого запуска проигрывания. Тип: целое число;
- **default\_http:** раздел с настройками HTTP-сервера. Включает в себя поля:
  - **http\_domain:** домен, для которого будут обрабатываться запросы. Тип: строка. Если данное поле не заполнено HTTPS-сервер не будет запущен;
  - **http\_listen\_addr:** локальный адрес для прослушивания HTTP подключений. Тип: строка. Значение должно содержать адрес локального сетевого интерфейса и порт разделенные двоеточием;
  - **enable\_https:** флаг включения HTTPS. Тип: строка;
  - **https\_listen\_addr:** локальный адрес для прослушивания HTTPS подключений. Тип: строка. Значение должно содержать адрес локального сетевого интерфейса и порт разделенные двоеточием;
  - **https\_cert\_file, https\_key\_file:** пути к сертификату и закрытому ключу для HTTPS-сервера. Тип: строка. Если данные поля не заполнены, то сервер будет пытаться получить сертификат через сервис Letsencrypt;
- **httpflv:** раздел с настройками HTTP-FLV протокола . Включает в себя поля:
  - **enable:** флаг включения протокола . Тип: булево значение. При выключенном состоянии проигрывание потоков через HTTP-FLV будет невозможно;
  - **gop\_num:** объем кэша для быстрого запуска проигрывания. Тип: целое число;
- **hls:** раздел с настройками HLS-протокола. Включает в себя поля:
  - **enable:** флаг включения протокола. Тип: булево значение. При выключенном состоянии проигрывание потоков через HLS будет невозможно;
  - **use\_memory\_as\_disk\_flag:** флаг хранения сегментов в оперативной памяти. Тип: булево значение. При включенном значении HLS-фрагменты будут находиться в оперативной памяти. При выключенном - писаться в файловую систему в соответствии со значением поля **out\_path**;
  - **out\_path:** путь для сохранения HLS-сегментов. Тип: строка. Используется когда хранение сегментов в оперативной памяти отключено;
  - **fragment\_duration\_ms:** длительность одного HLS-фрагмента в миллисекундах. Тип - целое число;
  - **fragment\_num:** количество сегментов в плей-листе. Тип: целое число;
  - **delete\_threshold:** количество сегментов, которое необходимо хранить после их удаления из плей-листа. Тип: целое число;

- **https:** раздел с настройками HTTP-TS протокола . Включает в себя поля:
  - **enable:** флаг включения протокола. Тип: булевое значение. При выключенном состоянии проигрывание потоков через HTTP-TS будет невозможно;
  - **gop\_num:** объем кэша для быстрого запуска проигрывания. Тип: целое число;
- **fmp4 :** раздел с настройками HTTP-FMP4 протокола . Включает в себя поля:
  - **enable:** флаг включения протокола. Тип: булевое значение. При выключенном состоянии проигрывание потоков через HTTP-FMP4 будет невозможно;
  - **gop\_num:** объем кэша для быстрого запуска проигрывания. Тип: целое число;
- **rtsp:** раздел с настройками RTSP протокола . Включает в себя поля:
  - **enable:** флаг включения протокола. Тип: булевое значение. При выключенном состоянии проигрывание потоков через RTSP будет невозможно.
  - **addr:** локальный адрес для прослушивания RTSP подключений. Тип: строка. Значение должно содержать адрес локального сетевого интерфейса и порт разделенные двоеточием;
  - **out\_wait\_key\_frame\_flag:** флаг ожидания ключевого кадра для новых клиентских сессий. Тип: булевое значение. Если включено для каждой новой клиентской сессии RTP-пакеты будут начинать отдаваться только после поступления ключевого кадра. В противном случае - сразу;
- **dvr:** раздел с настройками DVR. Включает в себя поля:
  - **enable:** флаг включения DVR. Тип: булевое значение. Если отключено запись потоков вестись не будет;
  - **out\_path:** путь к базовой директории для хранения записей. Тип: строка;
  - **disk\_usage\_pct:** максимальный процент заполнения раздела файловой системы. Тип: целое число. При превышении значения глубина хранения архивов для каждого записываемого потока будет уменьшаться, до тех пор, пока порог не будет соблюден.
  - **idx\_path:** путь для хранения индексов архивных записей. Тип: строка. При пустом значении индексы будут сохраняться вместе с архивными записями;
- **replication:** раздел с настройками репликации потоков и архивов между серверами. Включает в себя поля:
  - **addr:** локальный адрес для для запуска службы репликации. Тип: строка. При пустом значении функции репликации будут недоступны;
  - **token:** токен кластера. Тип: строка. Используется для аутентификации между серверами, участвующими в репликации. Должен совпадать на всех серверах участвующих в репликации;
  - **concurrent\_tasks:** количество одновременных репликаций архивных записей. Тип - целое число;



- **log:** раздел с настройками логирования. Включает в себя поля:
  - **level:** уровень логирования. Тип: строка. Возможные значения: debug, info, warning, error;
  - **filename:** имя файла, в который будет писаться лог. Тип: строка;
  - **log\_format:** формат логирования. Тип: строка. Допустимые значения: console, json;
  - **is\_to\_stdout:** флаг дублирования сообщений в консоль. Тип: булевое значение;
  - **file\_max\_size:** максимальный размер файла в мегабайтах, по достижении которого будет запущена ротация. Тип: целое число;
  - **max\_backups:** количество файлов, сохраняемых после ротации. Тип: целое число;
  - **short\_file\_flag:** флаг вывода в лог дополнительной отладочной информации. Тип: булевое значение;
  - **timestamp\_flag:** флаг сохранения ротированного файла с временной меткой в имени файла. Тип: булевое значение;
  - **timestamp\_with\_ms\_flag:** флаг вывода времени в логе с точностью до миллисекунд. Тип: булевое значение.

## Работа с потоками.

Добавление и удаление потоков производится через REST-API. Документация к API в формате Blueprint находится в /usr/share/doc/manul. Ниже приведены примеры работы с потоками с помощью утилиты curl.

**Добавить поток test1 с RTSP-источником, перекодированием аудио в AAC, и глубиной хранения записи 24 часа:**

```
curl -X POST -d '{"stream_name": "test1", "dvr_depth_hour": 24, "url":
"rtsp://admin:admin12345@rtsp.host:554/ch01/0", "encode_audio": true}'
http://admin:admin@127.0.0.1:8080/api/ctrl/stream
```

**Изменить глубину хранения записи у потока с именем test1:**

```
curl -X PATCH -d '{"dvr_depth_hour": 12}'
http://admin:admin@127.0.0.1:8080/api/ctrl/stream/test1
```

**Приостановить обработку потока с именем test1:**

```
curl -X PATCH -d '{"state": inactive}'
http://admin:admin@127.0.0.1:8080/api/ctrl/stream/test1
```

### **Удалить поток с именем test1:**

```
curl -X DELETE  
http://admin:admin@127.0.0.1:8080/api/ctrl/stream/test1/delete
```

### **Получить список всех потоков на сервере:**

```
curl http://admin:admin@127.0.0.1:8080/api/ctrl/stream
```

## **Проигрывание потоков.**

После добавления потока на сервер он сразу становится доступен для проигрывания. В зависимости от настроенного бэкенда аутентификации проигрывание потоков доступно либо настроенному списку IP-адресов, либо при прохождении авторизации в соответствии логикой аутентификации по URL. Ниже приведены ссылки для проигрывания на примере потока с именем test1:

RTSP: <rtsp://server/test1>

RTMP: <rtmp://server/live/test1>

HLS: <http://server/test1/index.m3u8>

HTTP-TS: <http://server/test1/mpegts>

HTTP-FLV: <http://server/test1/flv>

Проигрывание DVR возможно только по протоколу HLS. Ссылка для проигрывание должна быть сформирована в формате

<http://server/test1/index-{timestamp}-{duration}.m3u8>

где:

- `timestamp` - отметка времени (unix timestamp) времени начала проигрывания;
- `duration` - длительность записи для проигрывания.

Приме ссылки: <http://server/test1/index-1707543492-1800.m3u8> - проиграть запись потока test1 с 2024-02-10 05:38:12 (UTC) длительностью 30 минут.

## Авторизация доступа при проигрывании потока

Для защиты доступа к проигрыванию потоков в ПО Manul может использоваться два механизма.

1. **Защита доступа по IP.** Доступ для проигрывания предоставляется только списку разрешенных IP-подсетей. Для использования механизма необходимо прописать в конфигурационном файле бэкенд с типом ip, перечислить список разрешенных подсетей, и передать имя этого бэкенда в поле auth\_backend\_name при создании или редактировании потока.
2. **Защита доступа по URL.** При запросе на проигрывание потока manul ожидает аргумент с именем token. После получения запроса manul формирует HTTP-запрос к бэкенду, передавая в запросе: токен из запроса на проигрывание, IP-адрес клиента, тип (live, архивная запись), протокол (HLS, MPEGTS, FLV, RTSP, RTMP). В случае ответа от бэкенда с кодом 200 проигрывание потока разрешается. В остальных случаях - запрещается.