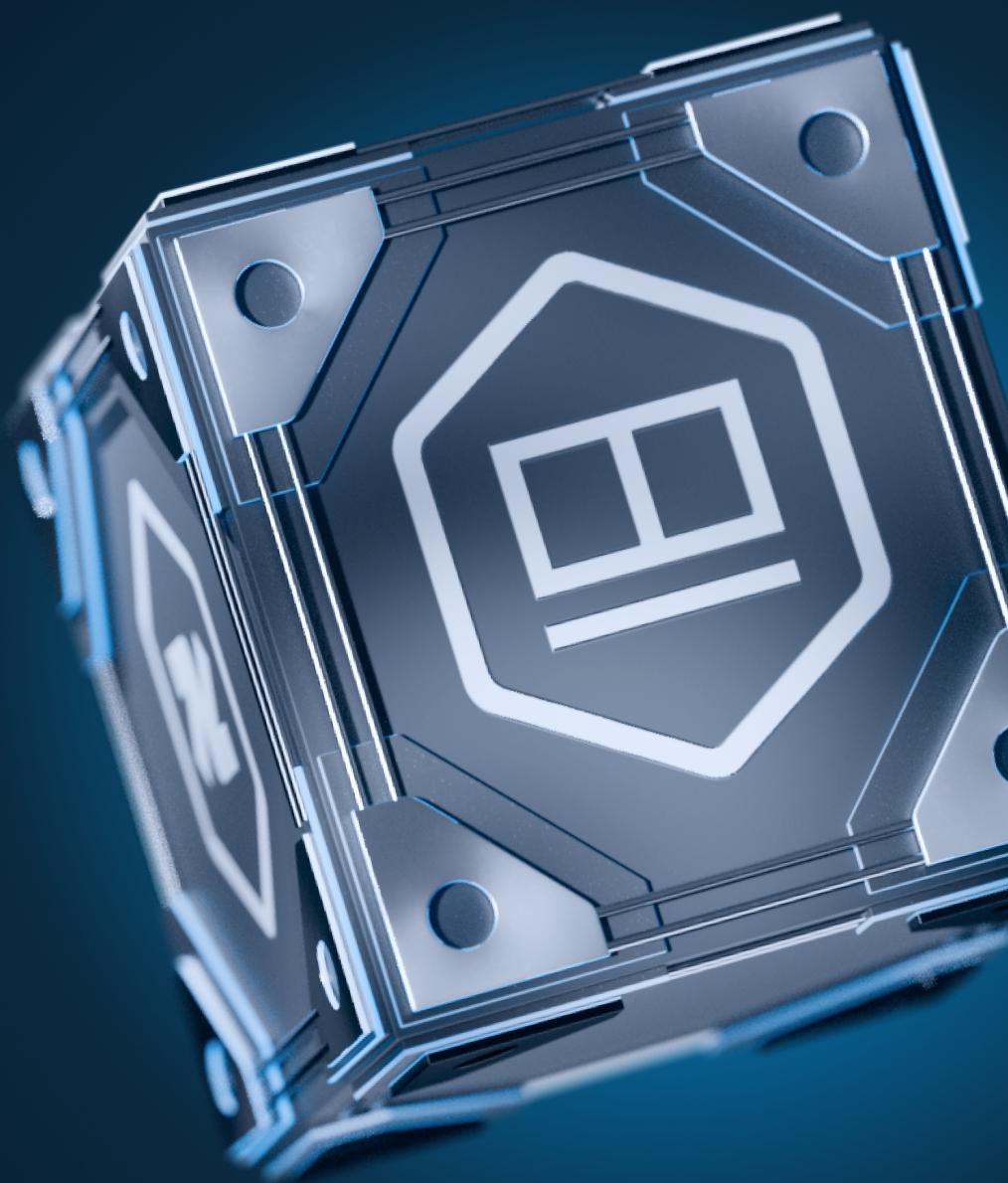




TERMIDESK



РУКОВОДСТВО АДМИНИСТРАТОРА

Настройка компонента «Ретранслятор»

СЛЕТ.10001-01 90 05

6.1. Выпуск от декабря 2025

ОГЛАВЛЕНИЕ

1 .	ОБЩИЕ СВЕДЕНИЯ.....	3
1.1 .	О документе.....	3
1.2 .	Назначение «Ретранслятора».....	3
1.3 .	Требования к аппаратному и программному обеспечению	3
1.4 .	Типографские соглашения	4
2 .	УСТАНОВКА И УДАЛЕНИЕ КОМПОНЕНТА.....	5
2.1 .	Получение пакетов установки в ОС Astra Linux Special Edition	5
2.2 .	Подготовка среды функционирования.....	7
2.3 .	Установка «Ретранслятора»	9
2.4 .	Удаление «Ретранслятора».....	9
2.5 .	Обновление «Ретранслятора».....	10
3 .	НАСТРОЙКА КОМПОНЕНТА	11
3.1 .	Параметры конфигурирования	11
3.1.1 .	Конфигурационный файл fluent-bit.conf	11
3.1.2 .	Конфигурационный файл parsers.conf.....	14
3.1.3 .	Конфигурационный файл plugins.conf	17
3.2 .	Журналирование	17
4 .	НЕШТАТНЫЕ СИТУАЦИИ.....	19
4.1 .	Нештатные ситуации и способы их устранения.....	19
5 .	ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	20
6 .	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	21

1. ОБЩИЕ СВЕДЕНИЯ

1.1. О документе

Настоящий документ является пятой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk). Документ предназначен для администраторов системы и сети.

В этом руководстве приведено назначение, установка и настройка компонента «Ретранслятор». Для того чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

1.2. Назначение «Ретранслятора»

Компонент «Ретранслятор» Termidesk (далее - «Ретранслятор») - это программное обеспечение (ПО), предназначенное для сбора и фильтрации записей журналов, поступающих от компонентов Termidesk, и их перенаправления в централизованное хранилище журналов или базу данных (БД).

Функции «Ретранслятора»:

- сбор данных (журналов событий) компонентов Termidesk;
- обработка и преобразование данных;
- отправка результатов в централизованное хранилище.

1.3. Требования к аппаратному и программному обеспечению

Для установки минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры x86-64 (AMD, Intel), не менее 4 шт.;
- оперативная память, не менее 4 ГБ;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

В среде функционирования должны быть предварительно установлены:

- операционная система (ОС) Astra Linux Special Edition версии 1.8 (минимальная версия - 1.8.1);
- система управления БД (СУБД) PostgreSQL версии 15 из состава репозитория ОС Astra Linux Special Edition версии 1.8. Из внешних по отношению к ОС Astra Linux Special Edition версии 1.8 СУБД поддерживается СУБД PostgreSQL версии 12 и выше.

ОС Astra Linux Special Edition версии 1.8 должна быть установлена из iso-образа, доступного в личном кабинете на портале Astra Linux: <https://lk-new.astralinux.ru/>. Работа на преднастроенных образах ОС не гарантируется.

1.4 . Типографские соглашения

Приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

2. УСТАНОВКА И УДАЛЕНИЕ КОМПОНЕНТА

2.1. Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в deb-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате iso-образа.

Получить iso-образ можно двумя способами:

- заполнив запрос через сайт Termidesk: <https://termidesk.ru/support/#request-support>;
- через личный кабинет: <https://lk.astra.ru/>.

Для подключения локального репозитория Termidesk на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить Интернет-репозиторий Termidesk в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор sh:

- либо указав `$(cat /etc/astra_version)`, если используется не последняя версия ОС:

```
1 sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat /etc/astra_version) non-free" > /etc/apt/sources.list.d/termidesk_local.list'
```

- либо указав `$(lsb_release -cs)`, если используется актуальная версия ОС:

```
1 sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs) non-free" > /etc/apt/sources.list.d/termidesk_local.list'
```

где:

`-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

`echo` - команда вывода текста, совместно с символом «» используется для перенаправления строки в файл;

`deb https://repos.termidesk.ru/astra <...>` - добавляемый репозиторий с вложенной командой получения версии ОС;

- выполнить поиск ключа репозитория Termidesk GPG-KEY-PUBLIC и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o /etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

⚠ В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ GPG-KEY-PUBLIC существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где 4E1632CC - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

Данную команду (`sudo apt update`) необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

2.2 . Подготовка среды функционирования

Перед установкой «Ретранслятора» должна быть предварительно подготовлена среда функционирования узла, а именно установлена и настроена система управления базами данных (СУБД) PostgreSQL.

⚠ Рекомендуется использовать отдельную инсталляцию СУБД для «Ретранслятора». «Ретранслятор» может использовать ту же СУБД, что и ферма Termidesk, но имя БД должно быть отличным от уже существующего (`termidesk`).

Установка СУБД PostgreSQL осуществляется аналогично подразделу **Установка и настройка СУБД PostgreSQL** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Для настройки БД следует перейти в интерфейс командной строки и выполнить:

- переключиться на пользователя `postgres`:

```
sudo su postgres
```

- запустить терминальный клиент СУБД PostgreSQL:

```
psql
```

● Если после выполнения команды отображается ошибка «`could not change directory to "/home/": Отказано в доступе`» и не появляется приглашение командной строки `postgres=#`, необходимо вместо `su postgres` использовать конструкцию `su - postgres`. Если приглашение `postgres=#` появилось, то сообщение об ошибке можно проигнорировать. Если приглашение `postgres=#` не появляется, то вероятнее всего ОС Astra Linux Special Edition используется в более защищенном режиме, например, «Смоленск». В таком случае нужно для пользователя `postgres` назначить высокий уровень целостности:

```
sudo pdpl-user -i 63 postgres
```

- используя интерактивный интерфейс терминального клиента СУБД PostgreSQL, создать БД `termidesk` (символ ; в конце строки при работе с интерактивным интерфейсом обязательен):

```
postgres=# CREATE DATABASE fluentbit LC_COLLATE 'ru_RU.utf8' LC_CTYPE 'ru_RU.utf8'  
TEMPLATE template0;
```

где:

LC_COLLATE - порядок сортировки для использования в БД, влияет на порядок сортировки, применяемый к строкам. Значение ru_RU.utf8 указывает на использование русской локализации;

LC_CTYPE - классификация символов для использования в БД, влияет на категоризацию символов;

TEMPLATE - имя шаблона, из которого создается БД. Шаблон template0 используется для системной БД самой СУБД PostgreSQL.

- создать пользователя fluentbit с паролем Password! для дальнейшего подключения к БД:

```
postgres=# CREATE USER fluentbit WITH PASSWORD 'Password!';
```

 В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы \$!@%^&#_-=+~`;:,?.(){}[]\`.

- назначить права по использованию БД fluentbit созданному пользователю fluentbit:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE fluentbit TO fluentbit;
```

- в случае, если используется СУБД PostgreSQL из состава ОС Astra Linux Special Edition 1.8, то сделать пользователя fluentbit владельцем БД fluentbit, тем самым предоставив ему все возможные права:

```
postgres=# ALTER DATABASE fluentbit OWNER TO fluentbit;
```

- выйти из интерактивного интерфейса терминального клиента СУБД PostgreSQL:

```
postgres=# \q
```

- выйти из сеанса пользователя postgres:

```
exit
```

- отредактировать файл /etc/parsec/mswitch.conf, установив параметр zero_if_notfound в значение yes, точно соблюдая отступы и пробелы:

```
1 # Return zero data instead of ENOENT/ENODATA in the absence of record
```

```
2 zero_if_notfound: yes
```

- ✖ В случае последующего обновления СУБД PostgreSQL может понадобиться пересоздать БД. В этом случае следует предусмотреть экспорт БД перед обновлением СУБД PostgreSQL.

2.3 . Установка «Ретранслятора»

Для установки «Ретранслятора» нужно:

- подключить репозиторий Termidesk;
- выполнить:

```
sudo apt install termidesk-repeater
```

- ℹ При установке пакета `termidesk-repeater` возможно активировать режим отладки инсталлятора через переменную окружения `TDSK_DEBUG` (например, `TDSK_DEBUG=1`).

После установки нужно:

- задать актуальные параметры подключения к БД в конфигурационном файле (см. подраздел **Конфигурационный файл `fluent-bit.conf`**);
- выполнить перезапуск службы:

```
sudo systemctl restart termidesk-repeater
```

- убедиться, что служба активна:

```
sudo systemctl status termidesk-repeater
```

2.4 . Удаление «Ретранслятора»

Для удаления нужно выполнить:

```
sudo apt purge termidesk-repeater
```

Для удаления БД следует выполнить следующие действия, строго соблюдая их последовательность:

- переключиться на пользователя `postgres` (через пользователя `root`):

```
sudo su postgres
```

- запустить терминальный клиент СУБД:

```
psql
```

- используя интерактивный интерфейс терминального клиента СУБД, удалить БД:

```
postgres=# DROP DATABASE fluentbit;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя postgres:

```
exit
```

2.5 . Обновление «Ретранслятора»

Обновление выполняется установкой новой версии поверх предыдущей.

Перед любым обновлением рекомендуется выполнить резервное копирование БД «Ретранслятора»:

```
1 pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W > <имя_файла_для_сохранения_БД.sql>
```

где:

-d <наименование БД> - имя БД. Например, repeater;
-h <IP-адрес_хоста> - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать localhost;
-p <порт> - порт для подключения к БД. При стандартных настройках используется 5432;
-U <пользователь> - имя пользователя для подключения. При стандартных настройках используется имя termidesk;
-W - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать ksedimret;
<имя_файла_для_сохранения_БД.sql> - имя и формат файла (sql) для сохранения БД.

Для обновления «Ретранслятора» нужно:

- подключить репозиторий Termidesk;
- выполнить:

```
sudo apt install termidesk-repeater
```

3. НАСТРОЙКА КОМПОНЕНТА

3.1. Параметры конфигурирования

3.1.1. Конфигурационный файл fluent-bit.conf

Для настройки «Ретранслятора» используется основной конфигурационный файл /etc/opt/termidesk-repeater/fluent-bit.conf.

Конфигурационный файл структурирован по секциям, каждая из которых описывает определенный компонент конвейера данных:

- [SERVICE] - описываются глобальные настройки termidesk-repeater;
- [INPUT] - описываются настройки для получения входящих событий;
- [OUTPUT] - описываются настройки для сохранения обработанных событий.

Описание секций и параметров приведено в таблице (см. Таблица 1).

⚠ При изменении файла fluent-bit.conf потребуется перезапуск службы termidesk-repeater:

```
sudo systemctl restart termidesk-repeater
```

Пример конфигурационного файла:

```
1 [SERVICE]
2   flush      1
3   daemon     off
4   log_level  info
5   parsers_file parsers.conf
6   plugins_file plugins.conf
7   http_server off
8   http_listen 0.0.0.0
9   http_port   2020
10  storage.metrics on
11
12 [INPUT]
13  Name        forward
14  Listen      0.0.0.0
15  Port        24224
16  Buffer_Chunk_Size 1M
17  Buffer_Max_Size  6M
18
19 [OUTPUT]
20  Name        pgsql
21  Match       *
22  Host        127.0.0.1
23  Port        5432
24  User        fluentbit
25  Password    Password!
26  Database    fluentbit
27  Table       logs
```

```

28      Time_Key          timestamp
29      Time_Format        %Y-%m-%d %H:%M:%S.%LZ
30      min_pool_size     1
31      max_pool_size     20

```

Таблица 1 – Параметры файла fluent-bit.conf

Параметр	Значение по умолчанию	Описание
Секция [SERVICE]		
flush	1	Частота отправки данных (в секундах) из внутреннего буфера в выходные плагины
daemon	Off	Управление режимом работы в фоновом режиме
log_level	info	Уровень детализации журнала событий. Может быть: <ul style="list-style-type: none">■ error;■ warning;■ info;■ debug
parsers_file	parsers.conf	Путь к конфигурационному файлу настройки обработчиков данных (парсеров). Можно задать несколько путей
plugins_file	plugins.conf	Путь к конфигурационному файлу настройки внешних расширений (плагинов)
http_server	Off	Управление режимом работы встроенного HTTP-сервера, предоставляющего API для мониторинга и управления. Возможные значения: <ul style="list-style-type: none">■ on - встроенный HTTP-сервер включен;■ off - встроенный HTTP-сервер выключен
http_listen	0.0.0.0	IP-адрес прослушивания встроенного HTTP-сервера
http_port	2020	Порт встроенного HTTP-сервера
storage.metrics	on	Управление режимом сохранения в постоянное хранилище. Возможные значения: <ul style="list-style-type: none">■ on - «Ретранслятор» сохраняет внутренние метрики производительности в то же постоянное хранилище, что и обычные данные событий. Метрики буду экспортироваться только при включенном параметре http_server;■ off - «Ретранслятор» не сохраняет внутренние метрики в постоянное хранилище
storage.path	/tmp/storage	<p>i По умолчанию параметр закомментирован.</p> <p>Абсолютный путь для хранения буферов данных файловой системы (chunk)</p>
storage.sync	normal	<p>i По умолчанию параметр закомментирован.</p> <p>Управление режимом синхронизации, используемого для хранения данных в файловой системе. Возможные значения:<ul style="list-style-type: none">■ normal;■ full</p>

Параметр	Значение по умолчанию	Описание
storage.checksum	off	<p>i По умолчанию параметр закомментирован.</p> <p>Управление режимом проверки целостности данных при записи и чтении данных из файловой системы, используется алгоритм CRC32</p>
storage.backLog.mem_limit	5M	<p>i По умолчанию параметр закомментирован.</p> <p>Максимальное значение памяти, используемое при обработке резервных данных. Резервные данные - это данные, которые не были отправлены и находятся на уровне хранилища. Такие данные проверяются, если задан и используется параметр <code>storage.path</code></p>
Секция [INPUT]		
Name	forward	Тип входного плагина. Значение <code>forward</code> используется для получения событий от других узлов «Ретранслятора»
Listen	0.0.0.0	IP-адрес прослушивания входящих событий. Значение 0.0.0.0 позволяет принимать соединения на всех интерфейсах
Port	24224	Порт прослушивания входящих событий
Buffer_Chunk_Size	1M	Размер буфера для хранения временных меток (chunk). Значение 1M зарезервировало 1 МБ для хранения данных
Buffer_Max_Size	6M	Максимальный размер буфера в случае очереди данных
Секция [OUTPUT]		
Name	pgsql	Определение типа выходного плагина. Значение <code>pgsql</code> указывает на отправку данных в СУБД PostgreSQL
Match	*	Указывает на тег и суффикс записи, обрабатываемой выходным плагином. Параметр используется для вывода событий с определенным тегом и суффиксом в другие системы. Формат: <тег>.<суффикс>. Значение * соответствует всем записям
Host	127.0.0.1	Адрес сервера СУБД PostgreSQL
Port	5432	Порт, на котором работает СУБД PostgreSQL
User	fluentbit	Имя пользователя для подключения к БД
Password	Password!	Пароль пользователя для подключения к БД
Database	fluentbit	Имя БД, в которую будут отправлены события
Table	logs	Название таблицы БД, в которую будут записываться события
Time_Key	timestamp	Ключ, под которым будет храниться временная метка

Параметр	Значение по умолчанию	Описание
Time_Format	%Y-%m-%d %H:%M:%S.%LZ	Формат временной метки
min_pool_size	1	Минимальный размер пула соединений
max_pool_size	20	Максимальный размер пула соединений

3.1.2 . Конфигурационный файл parsers.conf

Конфигурационный файл /etc/opt/termidesk-repeater/parsers.conf предназначен для определения и управления обработчиками (парсерами) журналов. Обработчики необходимы для преобразования неструктурированных записей журнала в структурированный формат, что упрощает их обработку, фильтрацию и анализ.

Пример файла:

```

1 [PARSER]
2   Name apache
3   Format regex
4   Regex ^(?<host>[^ ]*) [^ ]* (?<user>[^ ]*) \[(?<time>[^ ]*)\] "(?
<method>\S+)(?: +(?<path>[^"]*?) (?: +\S*)?)" (?<code>[^ ]*) (?<size>[^ ]*) (?: "
<referer>[^"]*") "(?<agent>[^"]*"))?$
5     Time_Key time
6     Time_Format %d/%b/%Y:%H:%M:%S %z
7
8 [PARSER]
9   Name apache2
10  Format regex
11  Regex ^(?<host>[^ ]*) [^ ]* (?<user>[^ ]*) \[(?<time>[^ ]*)\] "(?
<method>\S+)(?: +(?<path>[^ ]*) +\S*)?" (?<code>[^ ]*) (?<size>[^ ]*) (?: " (?
<referer>[^"]*") "(?<agent>.*"))?$
12    Time_Key time
13    Time_Format %d/%b/%Y:%H:%M:%S %z
14
15 [PARSER]
16   Name apache_error
17   Format regex
18   Regex ^\[[^ ]* (?<time>[^ ]*)\] \[(?<level>[^ ]*)\](?: \[pid (?
<pid>[^ ]*)\])?( \[client (?<client>[^ ]*)\])? (?<message>.*)$
19
20 [PARSER]
21   Name nginx
22   Format regex
23   Regex ^(?<remote>[^ ]*) (?<host>[^ ]*) (?<user>[^ ]*) \[(?<time>[^ ]*)\] "
<method>\S+)(?: +(?<path>[^"]*?) (?: +\S*)?)" (?<code>[^ ]*) (?<size>[^ ]*) (?: "
<referer>[^"]*") "(?<agent>[^"]*")"
24     Time_Key time
25     Time_Format %d/%b/%Y:%H:%M:%S %z
26

```

```
27 [PARSER]
28     # https://rubular.com/r/IhIbCAIs7Im0kc
29     Name      k8s-nginx-ingress
30     Format    regex
31     Regex     ^(?:<host>[^ ]*) - (?:<user>[^ ]*) \[(?:<time>[^ ]*)\] "(?
<method>[^ ]+)(?: +<path>[^ ]*) (?: +<code>[^ ]*) (?:<size>[^ ]*) " (?
<referer>[^ ]*)" "(?:<agent>[^ ]*)" (?:<request_length>[^ ]*) (?
<request_time>[^ ]*) \[(?:<proxy_upstream_name>[^ ]*)\] (\[(?:<proxy_alternative_upstream_name>[^ ]*)\]) (?:<upstream_addr>[^ ]*) (?
<upstream_response_length>[^ ]*) (?:<upstream_response_time>[^ ]*) (?
<upstream_status>[^ ]*) (?:<reg_id>[^ ]*) .*$
32     Time_Key  time
33     Time_Format %d/%b/%Y:%H:%M:%S %z
34
35 [PARSER]
36     Name      json
37     Format    json
38     Time_Key  time
39     Time_Format %d/%b/%Y:%H:%M:%S %z
40
41 [PARSER]
42     Name      logfmt
43     Format    logfmt
44
45 [PARSER]
46     Name      docker
47     Format    json
48     Time_Key  time
49     Time_Format %Y-%m-%dT%H:%M:%S.%L
50     Time_Keep  On
51     # --
52     # Since Fluent Bit v1.2, if you are parsing Docker logs and using
53     # the Kubernetes filter, it's not longer required to decode the
54     # 'log' key.
55     #
56     # Command      | Decoder | Field | Optional Action
57     # ======|=====|=====|=====
58     #Decode_Field_As  json      log
59
60 [PARSER]
61     Name      docker-daemon
62     Format    regex
63     Regex    time="(?:<time>[^ ]*)" level="(?:<level>[^ ]*)" msg="(?:<msg>[^ ].*)"
64     Time_Key  time
65     Time_Format %Y-%m-%dT%H:%M:%S.%L
66     Time_Keep  On
67
68 [PARSER]
69     Name      syslog-rfc5424
70     Format    regex
71     Regex     ^\<(?<pri>[0-9]{1,5})\>1 (?:<time>[^ ]+) (?:<host>[^ ]+) (?
<ident>[^ ]+) (?:<pid>[-0-9]+) (?:<msgid>[^ ]+) (?:<extradata>(\[(.*?)\]|-)) (?
<message>.+)$
72     Time_Key  time
73     Time_Format %Y-%m-%dT%H:%M:%S.%L%z
```

```
74     Time_Keep  On
75
76 [PARSER]
77     Name      syslog-rfc3164-local
78     Format    regex
79     Regex     ^\<(?<pri>[0-9]+)\>(?<time>[^ ]* {1,2}[^ ]* [^ ]*) (?<ident>[a-zA-Z0-9_/\.\-]*)?(?:\[?(?<pid>[0-9]+)\])?(?:[^:]*)? *(?<message>.*)$
80     Time_Key  time
81     Time_Format %b %d %H:%M:%S
82     Time_Keep  On
83
84 [PARSER]
85     Name      syslog-rfc3164
86     Format    regex
87     Regex     /^\<(?<pri>[0-9]+)\>(?<time>[^ ]* {1,2}[^ ]* [^ ]*) (?<host>[^ ]*) (?<ident>[a-zA-Z0-9_/\.\-]*)?(?:\[?(?<pid>[0-9]+)\])?(?:[^:]*)? *(?<message>.*)$/
88     Time_Key  time
89     Time_Format %b %d %H:%M:%S
90     Time_Keep  On
91
92 [PARSER]
93     Name      mongodb
94     Format    regex
95     Regex     ^(?<time>[^ ]*)\s+(?<severity>\w)\s+(?<component>[^ ]+)\s+\[(?<context>[^ ]*)]\s+(?<message>.*?) *(?<ms>(\d+))?(?:ms)?$
96     Time_Format %Y-%m-%dT%H:%M:%S.%L
97     Time_Keep  On
98     Time_Key  time
99
100 [PARSER]
101   # https://rubular.com/r/0VZmcYcLwMGAp1
102   Name      envoy
103   Format    regex
104   Regex     ^\[(?<start_time>[^ ]*)\] " (?<method>\S+)(?: +(?<path>[^"]*?)(?: +\S*)?)? (?<protocol>\S+)" (?<code>[^ ]*) (?<response_flags>[^ ]*) (?<bytes_received>[^ ]*) (?<bytes_sent>[^ ]*) (?<duration>[^ ]*) (?<x_envoy_upstream_service_time>[^ ]*) "(?<x_forwarded_for>[^ ]*)" "(?<user_agent>[^"]*)" "(?<request_id>[^"]*)" "(?<authority>[^ ]*)" "(?<upstream_host>[^ ]*)"
105   Time_Format %Y-%m-%dT%H:%M:%S.%L%z
106   Time_Keep  On
107   Time_Key  start_time
108
109 [PARSER]
110   # https://rubular.com/r/hbsTlxFFMozLmh
111   Name      istio-envoy-proxy
112   Format    regex
113   Regex     ^\[(?<start_time>[^ ]*)\] " (?<method>\S+)(?: +(?<path>[^"]*?)(?: +\S*)?)? (?<protocol>\S+)" (?<response_code>[^ ]*) (?<response_flags>[^ ]*) (?<response_code_details>[^ ]*) (?<connection_termination_details>[^ ]*) "(?<upstream_transport_failure_reason>[^ ]*)" (?<bytes_received>[^ ]*) (?<bytes_sent>[^ ]*) (?<duration>[^ ]*) (?<x_envoy_upstream_service_time>[^ ]*) "(?<x_forwarded_for>[^ ]*)" "(?<user_agent>[^"]*)" "(?<x_request_id>[^"]*)" "(?<authority>[^ ]*)" "(?<upstream_host>[^ ]*)" (?<upstream_cluster>[^ ]*) (?
```

```

<upstream_local_address>[^ ]*) (?<downstream_local_address>[^ ]*) (?<downstream_remote_address>[^ ]*) (?<requested_server_name>[^ ]*) (?<route_name>[^ ]*)$  

114     Time_Format %Y-%m-%dT%H:%M:%S.%L%z  

115     Time_Keep  On  

116     Time_Key start_time  

117  

118 [PARSER]  

119     # http://rubular.com/r/tjUt3Awgg4  

120     Name cri  

121     Format regex  

122     Regex ^(?<time>[^ ]+) (?<stream>stdout|stderr) (?<logtag>[^ ]*) (?<message>.*$)  

123     Time_Key    time  

124     Time_Format %Y-%m-%dT%H:%M:%S.%L%z  

125     Time_Keep  On  

126  

127 [PARSER]  

128     Name      kube-custom  

129     Format    regex  

130     Regex    (?<tag>[^.]+)?\.\.(?<pod_name>[a-z0-9](?:[-a-z0-9]*[a-z0-9])?(?:\.[a-z0-9](?:[-a-z0-9]*[a-z0-9])?)*)_(?<namespace_name>[^_]+)_(?<container_name>.+)-(?<docker_id>[a-z0-9]{64})\.\log$  

131  

132 [PARSER]  

133     # Examples: TCP: https://rubular.com/r/Q8YY6fHqlqwGI0 UDP: https://rubular.com/r/B0ID69H9FvN0tp  

134     Name      kmssg-netfilter-log  

135     Format    regex  

136     Regex    ^\<(?<pri>[0-9]{1,5})\>1 (?<time>[^ ]+) (?<host>[^ ]+) kernel ---\[[0-9\.]*\] (?<logprefix>[^ ]*)\s?IN=(?<in>[^ ]*) OUT=(?<out>[^ ]*) MAC=(?<macsrc>[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:(?<macdst>[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}):(?<ethertype>[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}):SRC=(?<saddr>[^ ]*) DST=(?<daddr>[^ ]*) LEN=(?<len>[^ ]*) TOS=(?<tos>[^ ]*) PREC=(?<prec>[^ ]*) TTL=(?<ttl>[^ ]*) ID=(?<id>[^ ]*) (D*F*)\s*PROTO=(?<proto>[^ ]*)\s?((SPT=)?(?<sport>[0-9]*))\s?((DPT=)?(?<dport>[0-9]*))\s?((LEN=)?(?<protolen>[0-9]*))\s?((WINDOW=)?(?<window>[0-9]*))\s?((RES=)?(?<res>0?x?[0-9]*))\s?((URGP=)?(?<urgp>[0-9]*))  

137     Time_Key    time  

138     Time_Format %Y-%m-%dT%H:%M:%S.%L%z

```

3.1.3 . Конфигурационный файл `plugins.conf`

Конфигурационный файл `/etc/opt/termidesk-repeater/plugins.conf` предназначен для определения и загрузки внешних или пользовательских плагинов. По умолчанию после установки никакие внешние плагины не подключены.

3.2 . Журналирование

Для просмотра журнала «Ретранслятора» можно выполнить:

```
sudo journalctl -f -u termidesk-repeater.service
```

или:

```
sudo less /var/log/syslog
```

4. НЕШТАТНЫЕ СИТУАЦИИ

4.1. Нештатные ситуации и способы их устранения

Возможные неисправности при работе с «Ретранслятором» и способы их устранения приведены в таблице (см. Таблица 2).

Таблица 2 – Перечень возможных нештатных ситуаций и способов их устранения

Индикация	Описание	Возможное решение						
Статус службы <code>termidesk-repeater</code> отображается как <code>failed</code>	<p>«Ретранслятор» не запускается:</p> <ul style="list-style-type: none">■ статус службы <code>termidesk-repeater</code> отображается как <code>failed</code>;■ в журнале отображаются сообщения: <table border="1"><tr><td>1</td><td><code>termidesk-repeater.service: Failed with result 'exit-code'.</code></td></tr><tr><td>2</td><td><code>Failed to start termidesk-repeater.service - Termidesk Repeater.</code></td></tr></table>	1	<code>termidesk-repeater.service: Failed with result 'exit-code'.</code>	2	<code>Failed to start termidesk-repeater.service - Termidesk Repeater.</code>	<p>Для работы «Ретранслятор» требуется указать актуальные параметры подключения к БД в конфигурационном файле (см. подраздел Конфигурационный файл fluent-bit.conf).</p> <p>Для исправления ситуации:</p> <ul style="list-style-type: none">■ задать актуальные параметры подключения к БД в конфигурационном файле <code>fluent-bit.conf</code>;■ выполнить перезапуск службы: <table border="1"><tr><td><code>sudo systemctl restart termidesk-repeater</code></td></tr></table> <ul style="list-style-type: none">■ убедиться, что служба активна: <table border="1"><tr><td><code>sudo systemctl status termidesk-repeater</code></td></tr></table>	<code>sudo systemctl restart termidesk-repeater</code>	<code>sudo systemctl status termidesk-repeater</code>
1	<code>termidesk-repeater.service: Failed with result 'exit-code'.</code>							
2	<code>Failed to start termidesk-repeater.service - Termidesk Repeater.</code>							
<code>sudo systemctl restart termidesk-repeater</code>								
<code>sudo systemctl status termidesk-repeater</code>								

5 . ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Ферма Termidesk	Ферма, объединяющая установку основных узлов Termidesk, взаимодействующих с одной БД

6 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
БД	База данных
ПО	Программное обеспечение
ОС	Операционная система
СУБД	Система управления базами данных
IP	Internet Protocol (межсетевой протокол)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
API	Application Programming Interface (интерфейс прикладного программирования)



© ООО «Увеон»

Телефон: +7 495 975 19 75
8 800 222 07 00

Электронная почта для связи: info@uveon.ru

Отдел продаж: info@astralinux.ru
Техподдержка: termidesk@astralinux.ru

Сайт: <https://termidesk.ru/>

Главный офис 119571, г. Москва,
Ленинский проспект, д. 119А