## Краткое описание сервиса

**Цель сервиса:**

Создание SMTP-шлюза с гибкими правилами обработки почты и удобным администрированием, позволяющем автоматизировать выполнение ежедневных операций администратора.

**Основные задачи сервиса:**

* Фильтрация почтовых сообщений
* Предоставление полной информации о почтовых потоках
* Использование хорошо автоматизируемых способов функционирования решений.

**Основная функциональность сервиса:**

* Наличие балльной системы как на уровне самой почтовой системы, так и на уровне дополнительных обработчиков (Amavis/SA/etc)
* Предоставление возможности пропустить/отклонить/добавить баллов в сообщение на каждом этапе прохождения проверок (в т.ч. до его полного получения)
* Типизированная и отвязанная от конкретного вендора аутентификация (SQL-based)
* Хорошо автоматизируемый механизм aliases
* Удобная для конечного администратора система логгирования, доступная как в виде текстовых файлов на сервере, так и в веб-представлении.
* JSON-формат хранения данных конфигурации.

**Используемые технологии:**

* Exim 4.8x — SMTP-сервер
* Spamassassin spamd — сервер проверки писем с использованием Байес-классификатора
* Amavis — сервер проверки вложений
* Rsyslog 7.x — syslog-сервер
* SQLite — SQL-like формат хранения данных

**Текущие ограничения:**

* при файловом логгировании лог о доставке сообщений на алиасы пишется только в лог пользователю и не пишется в лог алиаса

## **Техническое описание сервиса**

Технически, сервис можно разделить на три части:

* Доступ по протоколу SMTP → Exim, TCP port 25
* Дополнительные обработчики почты → SpamAssassin, Amavis, linux pipes
* Сервер парсинга и генерации лог-сообщений → Rsyslog, linux pipe

**1. Exim**

Основной функциональной частью почтовой системы является разделение сущностей обработки на четыре типа:

1. Lookup
2. ACL
3. Transport
4. Router

* Lookup

Этот тип позволяет искать объекты в механизмах хранения, например:

SENDER\_CHECK = \

${lookup sqlite {DB\_FILE\_MAIL SELECT domain FROM domains WHERE \

domain = '${quote\_sqlite:$sender\_helo\_name}'}{yes}{no}}

* ACL

Этот тип регламентирует всю процедуру почтовых проверок, которая состоит из секций «acl\_check\_connect», «acl\_check\_mail», «acl\_check\_rcpt», «acl\_check\_predata», «acl\_check\_data». Каждая секция содержит правила вида «accept», «deny», «warn». Так же, она может содержать указание на логгирование.

Например,

# From = To => SA = +20

warn condition = ${if eq{$sender\_address}{$local\_part@$domain}{yes}{no}}

set acl\_c\_spamscore = ${eval:$acl\_c\_spamscore+20}

set acl\_c\_spamlog = $acl\_c\_spamlog Sender == recipient;

logwrite =no-eximid => $local\_part@$domain ACT: AddScore, RULE: acl\_check\_rcpt, DATA: "From" is equal to "To"

* Router

Этот тип позволяет создавать правила того, какой вид транспорта использовать при доставке сообщений. Так же, он может выполнять подставновку значений и резолв адресов.

Например,

virtual\_aliases:

driver = redirect

allow\_fail

allow\_defer

domains = +accepted\_domains

data = CHECK\_ALIASES

user = mailnull

group = mail

* Transport

Этот тип является конечным выражением того, куда и с помощью каких протоколов необходимо доставлять письма.

Например,

lmtp\_over\_smtp:

driver = smtp

authenticated\_sender = $local\_part

protocol = lmtp

hosts = {$address\_data}

port = 24

allow\_localhost = true

return\_path\_add

Весь поток, помеченный как «exim», «exim-main», «exim-panic», а, так же, поток из фалов /var/log/exim/main.log, /var/log/exim/panic.log идёт на обработку в rsyslog.

**Мониторинг**

Должны отслеживаться параметры:

* количество инициированных SMTP-подключений
* количество писем, прошедших доставку
* количество сообщений со статусом «Reject»
* количество сообщений со статусом «Greylist»
* ….

**Сохранность данных**

Критичными данными являются:

* /etc/exim
* /etc/mail/spamassassin
* /var/log/exim
* /var/spool/exim/

**Безопасность**

* Использование SMTPS является обязательным, рекомендуемое решение — HAProxy;
* SMTP-авторизация производится с использованием sqlite-базы, находящейся в /etc/exim/sqlite/mail.sqlite, доступные механизмы — PLAIN/LOGIN;
* Неавторизированный релей запрещен всём, кроме списка ip-адресов таблицы relay\_from;

**Полезные комманды**

exim -bt [test@domain.ee](mailto:test@domain.ee) — трассировка сообщения

exim -bt -d+all [test@domain.ee](mailto:test@domain.ee) — аналогично, с максимальной детализацией

## **Управление сервисом**

**Интерфейс редактирования конфигураций**

…

**Интерфейс просмотра лог-сообщений**

...