Смоленск 1.6: установка и запуск службы RabbitMQ с ненулевой меткой безопасности

Данная статья применима к:

- ОС СН Смоленск 1.6
- ОС СН Смоленск 1.5 (с установленным обновлением Бюллетень № 20190329SE15)

RabbitMQ — программный брокер сообщений на основе стандарта AMQP — тиражируемое связующее программное обеспечение, ориентированное на обработку сообщений. Создан на основе системы Open Telecom Platform, написан на языке Erlang, в качестве движка базы данных для хранения сообщений использует Mnesia.

Состоит из сервера, библиотек поддержки протоколов HTTP, XMPP и STOMP, клиентских библиотек AMQP для Java и .NET Framework и различных плагинов (таких как плагины для мониторинга и управления через HTTP или веб-интерфейс или плагин «Shovel» для передачи сообщений между брокерами). Имеется реализация клиентов для доступа к RabbitMQ для целого ряда языков программирования, в том числе для Perl, Python, Ruby, PHP. Поддерживается горизо нтальное масштабирование для построения кластерных решений.
Источник информации.

Статья разработана на основе материалов, предоставленных коллегами из АО "РТИ"

Предисловие

В данной статье рассматривается запуск сервиса RabbitMQ с ненулевой меткой безопасности (для примера используется метка безопасности с уровнем конфиденциальности 3, категориями доступа 0 и уровнем целостности 0, т.е. 3:0:0).

При этом сервис работает на одном и только одном уровне конфиденциальности, работа одного экземпляра сервиса одновременно на нескольких уровнях конфиденциальности невозможна, так как это противоречит требованиям мандатного разграничения доступа.
При этом RabbitMQ использует для своей работы базу данных Mnesia, также не поддерживающую работу с метками безопасности.
При необходимости работать с данными, имеющими разные уровни мандатного доступа, необходимо запустить несколько экземпляров сервиса, каждый из которых будет работать на своём изолированном уровне.

В целом для запуска любого сервиса для работы с ненулевой меткой безопасности нужно выполнить следующие типовые операции:

1. Установить сервис и выполнить его базовые настроки;
2. Исправить системный юнит (файл запуска) сервиса, внеся в него параметр с необходимой меткой безопасности.
3. Установить на файловые объекты, в которые сервисом производится запись, необходимые мандатные уровни.

Далее рассматривается выполнение этих операций применительно к сервису RabbitMQ.

Установка сервиса

Пакет rabbitmq-server, устанавливающий службу RabbitMQ, не входит в состав стандартного дистрибутива ОС СН Atra Linux SE Смоленск 1.6, поэтому для установки службы нужно подключить репозиторий Debian.

После подключения репозитория пакет rabbitmq-server может быть установлен с помощью графического менеджера пакетов или из командной строки командами

```
apt update && apt install rabbitmq-server
```

При установке сервис будет запущен, и будет настроен автозапуск сервиса при запуске ОС.

Настройка сервиса

Базовая настройка

Настройка плагинов:

```
rabbitmq-plugins enable rabbitmq_management
```

Пример вывода команды:

```
The following plugins have been enabled:
  mochiweb
  webmachine
  rabbitmq_web_dispatch
 amqp_client
  rabbitmq_management_agent
  rabbitmq_management
```

Добавление пользователя для RabbitMQ, задание пароля, назначение прав

```
rabbitmqctl add_user user password && \
rabbitmqctl set_user_tags user administrator && \
rabbitmqctl set_permissions -p / user ".*" ".*" ".*"
```

Для выполнения дальнейших настроек остановить службу:

```
systemctl stop rabbitmq-server
```

Остановка службы занимает 90 секунд, это нормально.

Создать каталоги для работы с ненулевой меткой безопасности и назначить их владельцем автоматически созданного при установке пакета пользователя rabbitmq:

```
mkdir -p /opt/rabbitmq/{etc,log,run}  && chown -R rabbitmq:rabbitmq /opt
/rabbitmq/
```

Переместить файлы настроек в ранее созданный каталог:

```
mv /etc/rabbitmq/* /opt/rabbitmq/etc/
```

В реальности редактируемые далее файлы представляют собой ссылки на внутренние файлы RabbitMQ, поэтому для их редактирования рекомендуется использовать какой-нибудь простой текстовый редактор (например, nano).
Использование продвинутых редакторов (например, kate) может привести к тому, что ссылки будут заменены на копии файлов, после чего служба полностью потеряет работоспособность.

Отредактировать конфигурационный файл /opt/rabbitmq/etc/rabbitmq-env.conf, добавив или изменив следующие строки (в параметре NODE_IP_ADDRESS указать ip-адрес сервера):

NODENAME=example-rabbit
NODE_IP_ADDRESS=**<IP-address>**
NODE_PORT=5672
LOG_BASE=/opt/rabbitmq/log
HOME=/opt/rabbitmq
MNESIA_BASE=/var/lib/rabbitmq/mnesia

Настройка запуска с ненулевой меткой безопасности

Отредактировать юнит (файл запуска) службы в /etc/systemd/system/multi-user.target.wants/rabbitmq-server.service, добавив в него параметр с нужной меткой безопасности:

```
[Unit]
Description=RabbitMQ Messaging Server
After=network.target
[Service]
PDPLabel=3:0:0
Type=simple
User=rabbitmq
SyslogIdentifier=rabbitmq
LimitNOFILE=65536
ExecStart=/usr/sbin/rabbitmq-server
ExecStartPost=/usr/lib/rabbitmq/bin/rabbitmq-server-wait
ExecStop=/usr/sbin/rabbitmqctl stop
[Install]
WantedBy=multi-user.target
```

После выполнения редактирования юнита запуска службы обновить конфигурацию для загрузки внесённых изменений:

```
systemctl daemon-reload
```

Создание файловых объектов с нужной меткой безопасности

Отредактировать файл запуска службы в /etc/init.d/rabbitmq-server, исправив пути к файлам:

```
....
INIT_LOG_DIR=/opt/rabbitmq/log
PID_FILE=/opt/rabbitmq/run/pid
...
```

Отредактировать запускающий файл /usr/lib/rabbitmq/bin/rabbitmq-script-wrapper, исправив пути к файлам журналов:

```
if [ `id -u` = `id -u rabbitmq` -a "$SCRIPT" = "rabbitmq-server" ] ; then
 /usr/lib/rabbitmq/bin/rabbitmq-server "$@"  > "/opt/rabbitmq/log/startup_log" 2> "/opt/rabbitmq/log/startup_err"
```

Отредактировать файл переменных по умолчанию /usr/lib/rabbitmq/bin/rabbitmq-defaults. Изменить пути до файлов ENABLED_PLUGINS_FILE, CONF_ENV_FILE:

```
...
ENABLED_PLUGINS_FILE=${SYS_PREFIX}/opt/rabbitmq/etc/enabled_plugins
...
CONF_ENV_FILE=${SYS_PREFIX}/opt/rabbitmq/etc/rabbitmq-env.conf
...
```

Назначить уровень меток безопасности на директории и файлы

```
pdpl-file 3:0:0:ccnr /opt/
pdpl-file -R 3:0:0:ccnr /opt/rabbitmq
pdpl-file 3:0:0:ccnr /var/lib
pdpl-file R 3:0:0:ccnr /var/lib/rabbitmq
```

Запуск службы

Запустить службу:

```
systemctl start rabbitmq-server
```

Сценарий для ленивых

```
#!/bin/bash
set -eux
apt update && apt install -y rabbitmq-server
rabbitmq-plugins enable rabbitmq_management

( export U=user ; rabbitmqctl add_user $U password && rabbitmqctl set_user_tags $U administrator && rabbitmqctl set_permissions -p / $U ".*" ".*" ".*" )

time systemctl stop rabbitmq-server

( export R=/opt/rabbitmq ; mkdir -p $R/{etc,log,run} && mv /etc/rabbitmq/* $R/etc/ && chown -R rabbitmq:rabbitmq $R )

( export F=/opt/rabbitmq/etc/rabbitmq-env.conf
cat << EOF >>  $F
NODENAME=example-rabbit
NODE_IP_ADDRESS=$(ip a s eth0 2>/dev/null | grep "inet " | cut -d "/" -f 1 | cut -c 10-)
NODE_PORT=5672
LOG_BASE=/opt/rabbitmq/log
HOME=/opt/rabbitmq
MNESIA_BASE=/var/lib/rabbitmq/mnesia
EOF
)

( export F=/etc/systemd/system/multi-user.target.wants/rabbitmq-server.service
sed -i --follow-symlinks "s~^\[Service\].*$~\[Service\]\nPDPLabel=3:0:0~" $F
systemctl daemon-reload
)

( export F=/etc/init.d/rabbitmq-server
sed -i --follow-symlinks 's~^#!/bin/sh~#!/bin/sh -x~' $F
sed -i --follow-symlinks 's~^\([[:space:]]*INIT_LOG_DIR=.*\)~#\1\nINIT_LOG_DIR=/opt/rabbitmq/log~' $F
sed -i --follow-symlinks 's~^\([[:space:]]*PID_FILE=.*\)~#\1\nPID_FILE=/opt/rabbitmq/run/pid~' $F
)

( export F=/usr/lib/rabbitmq/bin/rabbitmq-script-wrapper
sed -i --follow-symlinks 's~^#!/bin/sh~#!/bin/sh -x~' $F
sed -i --follow-symlinks 's~\([[:space:]]*/usr/lib/rabbitmq/bin/rabbitmq-server.*\)~  /usr/lib/rabbitmq/bin/rabbitmq-server "$@" > "/opt/rabbitmq/log
/startup_log" 2> "/opt/rabbitmq/log/startup_err"\n#  \1"~' $F
)

( export F=/usr/lib/rabbitmq/bin/rabbitmq-defaults
sed -i --follow-symlinks 's~^\([[:space:]]*ENABLED_PLUGINS_FILE=.*\)~#\1\nENABLED_PLUGINS_FILE=${SYS_PREFIX}/opt/rabbitmq/etc
/enabled_plugins~' $F
sed -i --follow-symlinks 's~^\([[:space:]]*CONF_ENV_FILE=.*\)~#\1\nCONF_ENV_FILE=${SYS_PREFIX}/opt/rabbitmq/etc/rabbitmq-env.conf~' $F
)

pdpl-file 3:0:0:ccnr /opt/ && pdpl-file -R 3:0:0:ccnr /opt/rabbitmq
pdpl-file 3:0:0:ccnr /var/lib && pdpl-file -R 3:0:0:ccnr /var/lib/rabbitmq

systemctl start rabbitmq-server
```