Содержание

Резервирование BRAS Active-Standby 3
Описание алгоритма переключения для BRAS L2 (DHCP, Static IP) 3
Скрипт мониторинга состояния работы Master сервера 3
Скрипт синхронизации профилей услуг 4
Установка и управление 5

Резервирование BRAS Active-Standby

Описание алгоритма переключения для BRAS L2 (DHCP, Static IP)

- Резервирование BRAS L2 для IPoE (DHCP и Static IP) рекомендуется по схеме Active-Standby, что предполагает включение двух CKAT BRAS в один широковещательный L2 домен: Один в режиме Master, другой в режиме Backup (горячий резерв).
- Master является активным сервером и обрабатывает трафик во время нормальной работы сети. Backup находится в состоянии ожидания и не пропускает трафик через себя, интерфейсы DPDK в сторону абонентов (IN порты) административно выключены (down).
- Backup сервер осуществляет мониторинг работы Master сервера с помощью скрипта, при сбое в работе Backup в автоматическом режиме активирует (up) DPDK интерфейсы в сторону абонентов (IN порты) и начинает обрабатывать трафик.
- Реализовано одиночное переключение трафика на Backup сервер и остановка Master сервера с целью избежать дальнейшие аварии на сети. Переключение трафика на Master осуществляется сетевым администратором в ручкном режиме.
- Для корректной работы необходимо, чтобы все профили услуг были идентично сконфигурированы на Master и Backup сервере, рекомендуем использовать скрипт синхронизации профилей.
- Необходимо обратить внимание, что CKAT BRAS поддерживает динамическую (OSPF, BGP) и статическую маршрутизацию. В случае динамической маршрутизации для Static IP абонентов с публичными IP адресами анонс изменится автоматически при переключении на Backup сервер, для абонентов с приватными адресами будет применен профиль NAT, под тем же именем, но из другого публичного пула адресов, который заведен на Backup сервере.

Скрипт мониторинга состояния работы Master сервера

Скрипт должен быть установлен на Backup сервере, где он работает в непрерывном цикле, мониторя состояние Master сервера через SSH.
Используется **4 проверки** для подтверждения нормальной работы Master сервера:

1. Сервер доступен по сети (pingcheck)
2. Процесс fastDPI присутствует
3. PID процесса fastDPI не изменился (нет неконтролируемого перезапуска процесса)
4. Состояние ссылки на основном fastDPI не изменилось (необязательная проверка). Эта проверка отключена по умолчанию, так как может быть не нужна в некоторых топологиях

Процесс установки скрипта:

1. Скачать все файлы из архива на целевой резервный сервер
2. Настроить IP-адрес Master сервера в скрипте `SRS.sh`
3. Создать пару SSH-ключей на Backup сервере с помощью команды

```
ssh-keygen -t ed25519
```

4. Создать нового пользователя с правами sudo на Master сервере
5. Скопировать приватные SSH-ключи с Backup сервера в файл `authorized_keys` нового аккаунта на Master сервере
6. Добавить права на выполнение установочного скрипта с помощью команды

```
chmod +x install.sh
```

7. Запустить

```
install.sh
```

Управление сервисом:

1. Запуск сервиса:

```
systemctl start fastsrs
```

2. Проверка статуса сервиса:

```
systemctl status fastsrs
```

3. Остановка сервиса:

```
systemctl stop fastsrs
```

4. Проверка логов сервиса:

```
journalctl -u fastsrs
```

Скрипт синхронизации профилей услуг

Скрипт синхронизирует профили услуг 4 (фильтрация по черному списку), 5 (белый список и Captive Portal), 18 (полисинг по сессии и переопределение классов трафика) и полисинга между Master и Backup серверами.
Скрипт запускается на Master сервере, профили услуг на Backup сервере будут приведены к виду профилей на Master сервере. Перенос профилей осуществляется с помощью команд `fdpi_ctrl` и удаленного доступа по ssh.

Требования к системе:

- SSH
- Bash
- Jq
- установленный CKAT
- Rsync

Логика работы скрипта:
Скрипт получает текущий профиль услуги от Master сервера и затем отправляет его на

указанный Backup сервер. Затем скрипт подключается к Backup серверу и получает данные для профилей, присутствующих на Master сервере, получает данные профиля на Backup сервере, сопоставляет их и удаляет профили, отсутствующие на Master сервере.

Установка и управление

1. Настроить авторизацию через сертификат: создать сертификат на Master сервере с помощью `ssh-keygen -t ed25519`, проще всего использовать для авторизации учетную запись root.
2. Загрузить скрипт на Master сервер и поместить его в каталог `/usr/local/bin/`
3. Добавить разрешения для скрипта с помощью команды

```
chmod +x /usr/local/bin/profile_sync.sh
```

4. Настроить пользователя и IP Backup сервера внутри скрипта. Пользователь должен иметь возможность записи в каталог `/etc/dpi`, самый простой вариант — использовать пользователя root. Также можно настроить другого пользователя с соответствующими правами.
5. Настроить cron для выполнения скрипта с желаемыми интервалами **(опционально)**:

```
crontab -u root -e
0 * * * * * /bin/bash /usr/local/bin/profile_sync.sh
```

6. Добавить псевдоним bash для запуска скрипта по желанию:

```
echo "alias dpi_sync='/bin/bash /usr/local/bin/profile_sync.sh'">>
~/.bashrc
```

7. Создать каталог `/etc/dpi/service18` и сохранить в нем все файлы service 18.

Работа скрипта:
Скрипт запускается crontab с указанными интервалами или вручную с помощью команды `dpi_sync`.

Обратите внимание, что если профиль сервиса применен к абоненту, он не будет удален. Также обратите внимание, что любые файлы, не сохраненные в папке `service18`, не будут перенесены на Backup сервер, и, таким образом, синхронизированный профиль услуги 18 не будет работать. При отсутствии alias `dpi_sync` скрипт следует запускать через `sudo bash /usr/local/bin/profile_sync.sh`.