

Балансировка нагрузки Indeed PAM Gateway

Схема размещения компонентов

При большом количестве одновременно открытых сессий целесообразно добавить дополнительные серверы доступа.

Пусть их имена будут gw2 gw3 gw4 и т.д., настройка производится аналогично.

IP адреса HAProxy и дополнительных серверов доступа необходимо перечислить в настройках Indeed PAM Core в файле

C:\inetpub\wwwroot\pam\core\appsettings.json в секции **Auth**:

```
"PamGatewayIpAddresses": "192.168.10.140, 192.168.10.145, 192.168.10.146, 192.168.10.147, 192.168.10.148",
```

В Management Console в разделе Системные настройки в секциях **Настройки подключения к Gateway** и **Настройки SSH Proxy** необходимо ввести адрес балансировщика.

Настройки HAProxy в случае с четырьмя серверами представлены в примере:

```
global
log /dev/haproxy/log local0 # см https://en.wikipedia.org/wiki/Syslog#Facility
log /dev/haproxy/log local1 notice # notice - уровень ошибки. весь список: emerg, alert, crit,
err, warning, notice, info, debug
chroot /var/lib/haproxy # изменяем директорию выполнения для защиты от атак,
папка пуста и нет прав
maxconn 256 # максимальное количество одновременных
подключений.
stats socket /run/haproxy/admin.sock mode 660 level admin # связывает сокет с admin.sock
stats timeout 3s
user haproxy
group haproxy
daemon # Запустить процесс в фоновом режиме

defaults
log global # параметры лога берутся из секции global
mode tcp # режим работы экземпляра HAProxy
option dontlognull # отключить логи для фиктивных подключений
timeout connect 5000
timeout client 1h
timeout server 1h
retries 3 # кол-во попыток до того, как понизить статус сервера
balance roundrobin # выбор сервера перебором по порядку

# Статистика
frontend stats
mode http
bind *:8888 ssl crt /etc/haproxy/haproxy.pem
stats enable # включение вывода статистики
```

```

    timeout client 5m
    timeout server 5m
stats hide-version                # сккрытие версии HAProxy на странице статистики
stats realm    HAProxy\ Statistics # установка authentication realm
stats uri      /haproxy           # установка ссылки на страницу статистики
stats auth     stat:stat          # логин и пароль от страницы статистики

frontend frontend_gw
    mode      tcp
    bind      192.168.10.140:3389 # Адрес и порт на HAProxy для подключения клиентов
    timeout client 1h
    log       global
    option    tcplog # настройка логов TCP подключений с состояниями и таймерами
    tcp-request inspect-delay 2s # установка максимального времени анализа входящего
соединения
    tcp-request content accept if RDP_COOKIE # сессия открывается при наличии RDP протокола
    default_backend backend_gw # название backend, обрабатывающего запросы

frontend frontend_sshp
    mode      tcp
    bind      192.168.10.140:22
    timeout client 30m
    option tcplog
    default_backend backend_sshp

backend backend_sshp
    mode      tcp
    timeout server 30m
    timeout connect 5s
    balance leastconn
    option    tcp-check
    server gw4 192.168.10.148:22 weight 10 check port 22 inter 5000
    server gw3 192.168.10.147:22 weight 10 check port 22 inter 5000
    server gw2 192.168.10.146:22 weight 10 check port 22 inter 5000
    server gw1 192.168.10.145:22 weight 10 check port 22 inter 5000

backend backend_gw
    mode tcp
    balance leastconn # выбор сервера с наименьшим числом активных соединений
    timeout server 1h
    timeout connect 4s
    log global
    option tcp-check          # Выполнить проверку доступности по TCP,
    tcp-check    connect port 3389 ssl    # открывая зашифрованное соединение на порт
3389.
    stick-table type ip size 1m expire 12h # настраиваем таблицу привязки по ip размером 1 млн
записей и временем жизни записи 12 часов
    stick on src              # использовать ip-адрес клиента для привязки
    default-server inter 3s rise 2 fall 3 # Установить интервал проверки у серверов backend 3
сек. Сервер будет считаться активным после 2 успешных проверок и недоступным после 3
неудачных проверок.
    server gw4 192.168.10.148:3389 weight 10 check verify required #####
    server gw3 192.168.10.147:3389 weight 10 check verify required #Сервера РАМ Gateway
    server gw2 192.168.10.146:3389 weight 10 check verify required #веса серверов равны

```

относительно друг друга

server gw1 192.168.10.145:3389 weight 10 check verify required #проверка доступности
включена, сертификат не проверяется