Резервирование и балансировка Indeed PAM Core, IdP, MC и UC.

Настройка IDP

Выпуск сертификата для IdP

Можно воспользоваться сертификатом сервера балансировщика, либо выпустить самоподписанный.

Выпуск самоподписанного сертификата:

- Запустите PowerShell от имени администратора на любом из серверов PAM и выполните команду:

```
New-SelfSignedCertificate -DnsName idp.domain.local -CertStoreLocation cert:
\LocalMachine\My
```

Экспорт сертификата для IdP

1. Запустите оснастку MMC на сервере где был выпущен сертификат и выберите **сертификаты компьютера**.
2. Перейдите в раздел **Личные** (Personal), откройте контекстное меню сертификата и выберите пункт **Все задачи** (All Tasks) - **Экспорт** (Export). Экспорт необходимо выполнить два раза, с закрытым ключом и без закрытого ключа.

Импорт сертификата для IdP

1. Перенесите экспортированные сертификаты на второй сервер управления.
2. Откройте контекстное меню файла .pfx и выберите **Установить PFX** (Install PFX), установите сертификат в личные компьютера.
3. Откройте контекстное меню файла .crt и выберите **Установить сертификат** (Install Certificate), установите сертификат в доверенные корневые центры сертификации (этот пункт необходимо выполнить и для первого сервера. *Если сертификат не самоподписанный, то не надо*).

Настройка сертификата для IdP

Настройка выполняется на всех серверах.

1. Запустите оснастку MMC, откройте контекстное меню сертификата **балансировщика** и выберите пункт **Все задачи** (All Tasks) - **Управление закрытыми ключами** (Manage Private Keys).
2. Нажмите **Добавить** (Add) в разделе **Безопасность** (Security).
3. Нажмите **Размещение** (Locations) и выберите локальный компьютер.
4. Введите название пула **IIS AppPool\Indeed.idp** и нажмите **Проверить имена** (Check Names).
5. Сохраните изменения.

Настройка Indeed PAM IdP

Настройка выполняется на всех серверах.

1. Запустите оснастку MMC, откройте сертификат **балансировщика** и перейдите на вкладку **Состав** (Details).
2. Найдите пункт **Отпечаток** (Thumbprint) и скопируйте его значение

   В Windows Server до 2019 при копировании в начало строки всегда добавляется непечатаемый символ, его необходимо удалить. В Win Server 2019 копируется нормально.

3. Откройте файл **C:\inetpub\wwwroot\idp\appsettings.json** и укажите скопированный Отпечаток в качестве значения для параметра **SigningCertificate**
4. Перезагрузите IIS.

Настройка компонентов PAM для работы с балансировщиком

В файлах конфигурации Indeed PAM Core, IDP, MC, UC, ProxyAPP, SSHProxy необходимо изменить все URL компонентов на адрес балансировщика, кроме тех, что предназначены для работы с ILS

Например:

C:\inetpub\wwwroot\pam\core\appsettings.json

```
...
"Auth": {
  "IdpUrl": "https://haproxy.domain.local/idp",
...
"LogServer": {
  "AppId": "pam",
  "Component": "server",
  "EventCache": {
    "Directory": "C:\\ILS\\Core",
     "SendingIntervalSec": 10
  },
  "Server": {
    "Url": "https://srv1.domain.local/ils/api",
      "Certificate": {
        "Thumbprint": "",
        "FilePath": "",
        "FilePassword": ""
      }
    }
...
```

C:\inetpub\wwwroot\pam\idp\appsettings.json

```
"IdentitySettings": {
...
  "IdpUrl": "https://haproxy.domain.local/pam/idp",
...
"PamSettings": {
  "ManagementConsoleUrls": ["https://haproxy.domain.local/pam/mc"],
  "UserConsoleUrls": ["https://haproxy.domain.local/pam/uc"],
  "CoreUrls": ["https://haproxy.domain.local/pam/core"],
...
```

C:\inetpub\wwwroot\pam\uc\assets\config\config.prod.json

```
{
  "env": {
    "name": "PROD",
    "lang": "ru",
    "url": "https://haproxy.domain.local/pam/uc",
...
"core": {
  "url": "https://haproxy.domain.local/pam/core"
},
"idp": {
  "url": "https://haproxy.domain.local/pam/idp",
  "requireHttps": true
},
...
```

Пример файла **/etc/haproxy/haproxy.cfg**:

```
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 30s

# Неизменяемые настройки HAPROXY
    user haproxy
    group haproxy
    daemon                              # Запустить процесс в фоновом режиме

defaults
    log         global
    mode        http
    option      httplog
    option      dontlognull

# Таймауты
    timeout connect 5000
    timeout client 50000
    timeout server 50000
    retries 3                       # кол-во попыток до того, как понизить статус сервера

# Статистика
    stats enable
    stats hide-version
    stats realm Haproxy\ Statistics
```

```
    stats uri /haproxy              #здесь указываем ссылку на страницу статистики
    stats auth stat:stat
    option httpchk HEAD / HTTP/1.0

# Настройки доступа
    option redispatch               # Позволит пользователям пройти к другому серверу если сервер, на
который ссылаются их куки, не работает
    balance source # алгоритм выбора сервера (наименее загруженный по порядку)

frontend frontend_pam
    bind *:443 ssl crt /etc/ssl/certs/haproxy.domain.local.pem # настройка интерфейса фронтенда с
указанием пути к сертификату этого сервера
    option forwardfor                       # передать оригинальный ip адрес клиента серверу
    acl url_core path_beg /pam/core
    use_backend backend_api if url_core
    acl url_idp path_beg /pam/idp
    use_backend backend_idp if url_idp
    acl url_mc path_beg /pam/mc
    use_backend backend_mc if url_mc
    acl url_uc path_beg /pam/uc
    use_backend backend_uc if url_uc

backend backend_api
    option prefer-last-server         # попытка повторно использовать тоже соединение к серверу
    option httpchk GET /pam/core/health       # проверка доступности приложения PAM Core
    server PAM1 192.168.1.1:443 ssl verify required check inter 5000 fall 3
    server PAM2 192.168.1.2:443 ssl verify required check inter 5000 fall 3

backend backend_idp
    option prefer-last-server         # попытка повторно использовать тоже соединение к серверу
    option httpchk GET /pam/idp/          # проверка доступности приложения PAM Core
    server PAM1 192.168.1.1:443 ssl verify required check inter 5000 fall 3
    server PAM2 192.168.1.2:443 ssl verify required check inter 5000 fall 3

backend backend_mc
    option prefer-last-server         # попытка повторно использовать тоже соединение к серверу
    option httpchk GET /pam/mc/          # проверка доступности приложения PAM Core
    server PAM1 192.168.1.1:443 ssl verify required check inter 5000
    server PAM2 192.168.1.2:443 ssl verify required check inter 5000

backend backend_uc
    option prefer-last-server         # попытка повторно использовать тоже соединение к серверу
    option httpchk GET /pam/uc/          # проверка доступности приложения PAM Core
    server PAM1 192.168.1.1:443 ssl verify required check inter 5000
    server PAM2 192.168.1.2:443 ssl verify required check inter 5000
```