ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Руководство по установке программного комплекса «Центр управления пользователями (ЦУП) версия 2.0»

1. Назначение системы

Центр управления пользователями (ЦУП) версия 2.0 предназначен для хранения цифровых аутентификационных данных (секретов) технических учетных записей, передачи этих секретов приложениям и обновления (ротации) этих секретов. Система предназначена для повышения уровня защищенности инфраструктуры, путем автоматизации и унификации процессов управления секретами.

Из пользовательского интерфейса вы можете легко создавать, обновлять, считывать и удалять секреты, аутентифицировать, распечатывать и многое другое.

2. Цели и задачи системы

Основной целью системы является повышение уровня защищенности инфраструктуры, путем автоматизации и унификации процессов управления секретами.

Задачи:

- Безопасное хранение секретов.
- Безопасная доставка секретов на информационные ресурсы
- Безопасное создание секретов.
- Безопасная передача секретов по запросам.
- Отзыв (удаление) и ротация секретов.

3. Подготовка к работе

3.1.Состав дистрибутивного набора данных

Дистрибутив ЦУП модуль управления секретами доступен по ссылке: http://itsm.at-consulting.ru/ucp. Доступ для загрузки дистрибутива может быть получен по предварительному запросу на почту: atcitsmproduct@at-consulting.ru.

Далее представлены требования к запуску ЦУП модуля управления секретами:

- Операционная система CentOS версии не ниже 7, Ubuntu не ниже 18 версии;
- Среда выполнения программ GO версии не ниже 1.15.3;
- Исходные коды ЦУП модуля управления секретами;

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

- Сетевой балансировщик HAProxy;
- СУБД PostgreSQL версия не ниже 9.6.
- Etcd
- Patroni

3.2. Подготовка инфраструктуры для развертывания ЦУП модуль управления секретами

Для развертывания ЦУП модуль управления секретами требуется выделить виртуальные или физические серверы. В таблице 2 приведена минимальная конфигурация серверов:

Роль сервера	Кол-во	CPU, кол-во ядер	Память, Gb	Диск, Gb
Компонент кластера управления секретами	3	4	8	50
Сервер баз данных	3	4	8	50

На каждом сервере производится установка операционной системы согласно требованиям к запуску. Установка производится в соответствии документацией производителя дистрибутива.

Требования к параметрам установки операционной системы:

- Сетевая связанность серверов на втором уровне модели OSI;
- Должен быть отключен межсетевой экран внутри ОС;
- Обязательно должны быть соответствующе настроены либо отключены правила SELinux.
- Если Ваша установка проходит на ос Ubuntu, то нужно выполнить: sudo apt-get install acl

На серверах, где будет установлен postgresql нужно выполнить следующие шаги под пользователем root:

Установка Etcd:

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

- # URL для загрузки диструбутива
  - ETCD_VER=v3.5.5
  - GOOGLE_URL=https://storage.googleapis.com/etcd
  - GITHUB_URL=https://github.com/etcd-io/etcd/releases/download
  - DOWNLOAD_URL=${GITHUB_URL}

  # Скачиваем и распаковываем файлы приложения, удаляем временные файлы
  - curl -L ${DOWNLOAD_URL}/${ETCD_VER}/etcd-${ETCD_VER}-linux-amd64.tar.gz -o /tmp/etcd-${ETCD_VER}-linux-amd64.tar.gz
  - mkdir /tmp/etcd-download-test
  - tar xzvf /tmp/etcd-${ETCD_VER}-linux-amd64.tar.gz -C /tmp/etcd-download-test --strip-components=1
  - rm -f /tmp/etcd-${ETCD_VER}-linux-amd64.tar.gz

  # Проверяем корректность установки
  - mv /tmp/etcd-download-test/etcd* /usr/local/bin/
  - /usr/local/bin/etcd --version
  - /usr/local/bin/etcdctl version

Создаем пользователя для работы со службой:
- sudo groupadd --system etcd
- sudo useradd -s /sbin/nologin --system -g etcd etcd

Создаем и предоставляем права на каталог /var/lib/etcd пользователю etcd.
- sudo mkdir -p /var/lib/etcd/
- sudo mkdir /etc/etcd
- sudo chown -R etcd:etcd /var/lib/etcd/
- sudo chmod -R 700 /var/lib/etcd/

Создаем файл службы для сервиса ETCD /etc/systemd/system/etcd.service :

[Unit]
Description=etcd service
Documentation=https://github.com/coreos/etcd

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
[Service]
User=etcd
Type=notify
ExecStart=/usr/local/bin/etcd \
 --name cup-postgres1 \
 --enable-v2=true \
 --data-dir /var/lib/etcd \
 --initial-advertise-peer-urls http://172.24.160.224:2380 \
 --listen-peer-urls http://0.0.0.0:2380 \
 --listen-client-urls http://0.0.0.0:2379 \
 --advertise-client-urls http://172.24.160.224:2379 \
 --initial-cluster cup-postgres1=http://172.24.160.224:2380,cup-
postgres2=http://172.24.160.226:2380,cup-
target2=http://172.24.160.228:2380 \
 --initial-cluster-state new \
 --heartbeat-interval 1000 \
 --election-timeout 5000
Restart=on-failure
RestartSec=5
[Install]
WantedBy=multi-user.target
```

* --initial-cluster-state new использовать только на ноде, где планируется leader-нода; 172.24.160.224 – текущая нода, 172.24.160.226, 172.24.160.228 – другие ноды кластера.

В случае использования межсетевого экрана разрешить подключения по портам 2379,2380 по протоколу tcp.

- firewall-cmd --permanent --add-port=2380/tcp
- firewall-cmd --add-port=2380/tcp
- firewall-cmd --permanent --add-port=2379/tcp
- firewall-cmd --add-port=2379/tcp
- firewall-cmd --reload

После создания службы на всех серверах, включаем её, первый сервер будет выполнять роль сервера начальной загрузки, после успешного запуска службы на всех серверах, будет выбран лидер.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

- systemctl daemon-reload
- systemctl enable etcd
- systemctl start etcd.service

Проверяем состояние кластера после запуска:

- /usr/local/bin/etcdctl member list
- /usr/local/bin/etcdctl endpoint status --write-out=table --endpoints=http://172.24.160.226:2380,http://172.24.160.224:2380,http://172.24.160.228:2380
- systemctl status etcd.service

Установка Postgresql:

- dnf/apt install postgresql-server – устанавливаем postgresql на машину (для ubuntu нет такого пакета)
- Активируем Postgresql для автоматического запуска службы при запуске системы: sudo systemctl enable postgresql
- Запускаем команды:
  - firewall-cmd --permanent --add-port=8008/tcp
  - firewall-cmd --add-port=8008/tcp
  - firewall-cmd --permanent --add-port=5432/tcp
  - firewall-cmd --add-port=5432/tcp
  - firewall-cmd –reload

Далее нужно установить patroni на наши сервера, где развернут postgresql, для этого необходимо установить дополнительные пакеты:

- sudo dnf/apt -y install python3 python3-pip
- sudo -H pip install --upgrade testresources
- sudo -H pip install --upgrade setuptools
- sudo -H pip install psycopg2-binary
- sudo -H pip install patroni
- sudo -H pip install python-etcd

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Создаем файл конфигурации для кластера Patroni /etc/patroni/patroni.yml. Конфигурационный файл необходимо создать на всех ВМ с PostgreSQL.

```
name: cup-postgres1
scope: patroni_cluster

etcd:
  hosts: 172.24.160.224:2379,172.24.160.226:2379, 172.24.160.228:2379

restapi:
  listen: 0.0.0.0:8008
  connect_address: "172.24.160.224:8008"

bootstrap:
  users:
    replication:
      username: replicator
      password: password
  dcs:
    ttl: 30
    loop_wait: 10
    maximum_lag_on_failover: 1048576
    postgresql:
      use_pg_rewind: true
use_slots: true

parameters:
        archive_mode: "on"
        wal_level: hot_standby
        max_wal_senders: 10
        wal_keep_segments: 8
        archive_timeout: 1800s
        max_replication_slots: 5
        hot_standby: "on"
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
      wal_log_hints: "on"

  initdb:
    - encoding: UTF8
    - data-checksums

  postgresql:
    pgpass: /var/lib/pgsql/.pgpass
    listen: 0.0.0.0:5432
    connect_address: "172.24.160.224:5432"
    data_dir: /var/lib/pgsql/data/
    bin_dir: /usr/bin/
    pg_rewind:
      username: postgres
      password: password
    pg_hba:
      - local all postgres trust
      - host all postgres 127.0.0.1/32 trust
      - host replication replicator 172.24.160.224/32 trust
      - host replication replicator 127.0.0.1/32 trust
      - host replication replicator 172.24.160.226/32 trust
      - host all all 0.0.0.0/0 md5
    replication:
      username: replicator
      password: password
    superuser:
      username: postgres
      password: password
```

* особое внимание стоит уделить данным, которые отмечены желтым.
** данные конфигурационные файлы на разных серверах будут немного различаться.

- **name** — имя узла, на котором настраивается данный конфиг.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

- **scope** — имя кластера. Его мы будем использовать при обращении к ресурсу
- **restapi - connect_address** — адрес на настраиваемом сервере, на который будут приходить подключения к patroni.
- **pg_hba** — блок конфигурации pg_hba для разрешения подключения к СУБД и ее базам.
- **postgresql - pgpass** — путь до файла, который создаст patroni. В нем будет храниться пароль для подключения к postgresql. Он будет зависеть от версии СУБД.
- **postgresql - connect_address** — адрес и порт, которые будут использоваться для подключения к СУБД.
- **postgresql - data_dir** — путь до файлов с данными базы.
- **postgresql - bin_dir** — путь до бинарных файлов postgresql.
- **pg_replication, superuser** — логины и пароли, которые будут созданы для базы.

  На втором сервере будет такой же конфигурационный файл, за исключением следующих опций:

- name: postgresql2
  ...

  connect_address: "172.24.160.226:8008"
  ...

  connect_address: "172.24.160.226:5432"
  ...

Создаем systemd-service для работы Patroni:

- sudo nano /etc/systemd/system/patroni.service

  Содержание.
  [Unit]
  Description=High availability PostgreSQL Cluster
  After=syslog.target network.target

  [Service]
  Type=simple
  User=postgres

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
Group=postgres
ExecStart=/usr/local/bin/patroni /etc/patroni/patroni.yml
KillMode=process
TimeoutSec=30
Restart=no

[Install]
WantedBy=multi-user.target
```

Выполянем команду:

```
sudo systemctl daemon-reload
```

Разрешаем автозапуск и стартуем сервис patroni:

- systemctl enable patroni
- systemctl start patroni

Проверяем статусы сервиса на обоих серверах:

```
systemctl status patroni
```

Посмотреть список нод:

```
patronictl -c /etc/patroni/patroni.yml list
```

Мы должны увидеть что-то на подобие:я

```
+ Cluster: patroni_cluster (7126124696482454785) -+---------+----+-----------+
+------------+-------------+---------+---------+----+-----------+
| Member     | Host        | Role    | State   | TL | Lag in MB |
| postgresql1 | 172.24.160.224 | Leader  | running |  1 |           |
| postgresql2 | 172.24.160.226 | Replica | running |  1 |         0 |
+------------+-------------+---------+---------+----+-----------+
```

- Далее в файле /var/lib/pgsql/data/postgresql.base.conf:
  Испрвляем строчку listen_addresses = 'localhost' на listen_addresses = '*'

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Раскомментировать строку - port = 5432

- Создать пользователя, который указан в /inventories/example/dev/hosts.yaml, командой – CREATE ROLE vault WITH LOGIN PASSWORD ‘пароль’;
- Создать базы данных, которые указаны в /inventories/example/dev/hosts.yaml в поле db_name, командой – CREATE DATABASE название базы данной OWNER vault;
- Создать схему – CREATE SCHEMA VAULT;
- Создать таблицы в созданных бд - create table vault.vault_kv_store (parent_path TEXT COLLATE "C" NOT NULL, path TEXT COLLATE "C", key TEXT COLLATE "C", value BYTEA, constraint pkey PRIMARY KEY (path, key));

  - create table vault.vault_ha_locks (ha_key TEXT COLLATE "C" NOT NULL, ha_identity TEXT COLLATE "C" NOT NULL, ha_value TEXT COLLATE "C", valid_until TIMESTAMP WITH TIME ZONE NOT NULL, CONSTRAINT ha_key PRIMARY KEY (ha_key));

- В файле /etc/patroni/patroni.yml в самом конце нужно добавить созданные базы данных:
- host база данных пользователь адрес сервера target/32 md5
- host база данных пользователь адрес сервера transit/32 md5

Установка Pgbouncer:

Выполняем команду по установке:

dnf/yum/apt install pgbouncer

Далее редактируем конфигурационный файл /etc/pgbouncer/pgbouncer.ini:

[databases]
* = host=127.0.0.1 port=5432
[users]

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
[pgbouncer]
logfile = /var/log/pgbouncer/pgbouncer.log
pidfile = /var/run/pgbouncer/pgbouncer.pid
listen_addr = *
listen_port = 6432
auth_type = md5
auth_file = /etc/pgbouncer/userlist.txt
admin_users = postgres

stats_users = stats, postgres
```

Заходим в psql и выполняем запрос:

```
SELECT * FROM pg_authid WHERE rolname='pgbouncer';
```

Находим столбец rolpassword и копируем содержимое. Пароль необходимо вставить в /etc/pgboucer/userlist.txt для пользователя postgres. Аналогично выполнить для пользователя vault.

Запускаем Pgboucer:

```
sudo systemctl restart pgboucer
```

Проверяем статус:

```
sudo ssytemctl status pgbouncer
```

Установка Haproxy:

Выполняем команду по установке:

```
sudo dnf/apt install haproxy
```

Переходим в /etc/haproxy и редактируем haproxy.cfg:

```
Global

maxconn 100

 default
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
log global
    mode tcp
    retries 2
    timeout client 30m
    timeout connect 4s
    timeout server 30m
    timeout check 5s
listen stats
    mode http
    bind *:7000
    stats enable
    stats uri /
listen postgres
    bind *:5000
    option httpchk
    http-check expect status 200
    default-server inter 3s fall 3 rise 2 on-marked-down shutdown-sessions
    server patroni1 172.24.160.224:5432 maxconn 100 check port 8008
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

server patroni2 172.24.160.226:5432 maxconn 100 check port 8008

*Адреса 2 нод, на которых установлен patroni

Запускаем службу. Проверяем состояние.

- sudo systemctl restart haproxy
- sudo systemctl status haproxy

В дальнейшем применяем следующую идентификацию развернутых серверов:

Имя сервера	**IP адрес**	**Роль сервера**
vault1.local	IP1	Компонент кластера управления секретами
vault2.local	IP2	Компонент кластера управления секретами
vault3.local	IP3	Компонент кластера управления секретами
node01.local	IP4	Сервер баз данных
node02.local	IP5	Сервер баз данных
node03.local	IP6	Сервер баз данных

4. Подготовка дистрибутива

4.1. Сборка из исходных кодов

При наличии исходных кодов необходимо произвести компиляцию:
make prod

Данная команда произведет установку в директории bin и $GOPATH/bin

Чтобы скомпилировать версию с пользовательским интерфейсом необходимо выполнить:
make static-dist prod-ui

Данная команда произведет установку в директории bin и $GOPATH/bin

4.2. Установка дистрибутива

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая
Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Архив с дистрибутивом необходимо распаковать, получив директорию dist, в которой располагается бинарный файл и необходимые конфигурационные файлы.

В корневой директории архива располагаются файлы скриптов системы автоматической конфигурации Ansible.

Необходимо отредактировать файл inventory, задав названия серверов, на которых будет произведена установка и настройка дистрибутива.

Дополнительно необходимо указать путь до SSH-ключа шифрования, который предварительно должен быть помещен на все серверы.

Также необходимо указать путь до сертификатов, которые будут использованы в работе системы.

Для установки и настройки дистрибутива на серверы достаточно выполнить команду:

ansible-playbook first_deploy.yml

Для выполнения установки на сервере, где будет производиться установка требуются root-права.

При выполнении команды будут выведены 5 ключей, необходимые для распечатывания хранилища.

В дальнейшем для распечатывания хранилища требуется ввести команду на сервере transit:

vault operator unseal

Далее нужно ввести 3 ключа, которые были выведены на экран при первой установке.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая
Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

5. Запуск дистрибутива

5.1. В составе дистрибутива поставляется юнит-файл для системы инициализации Systemd — vault.service.

При выполнении шага установки дистрибутива данный файл должен быть установлен на все серверы с помощью Ansible. Для запуска дистрибутива достаточно выполнить команду:

```
systemctl start vault
```

Проверить статус службы можно командой:

```
systemctl status vault
```

За журналами системы и журналами аудита можно наблюдать в следующих файлах:

```
journalctl –eu vault
```

5.2. При первом запуске производится автоматическая инициализация сервера target.

В результате будет выдан список из 5 ключей, необходимых для распечатывания хранилища, а также токен авторизации с максимальными правами, их надо обязательно сохранить.

Проверить текущий статус хранилища можно с помощью команды vault status

```
Initialized     true
Sealed          false
```

Строка Initialized говорит о состоянии инициализации хранилища, должно быть значение true.

Строка Sealed сообщает о статусе "распечатывания" хранилища. Должно быть значение false.