Установка FreeIPA в Fedora 42

- Отключить репозиторий ciscobinary.openh264.org

```
sudo sed -i 's/enabled=1/enabled=0/g' /etc/yum.repos.d/fedora-cisco-openh264.repo
sudo yum update
```

- Установить пакеты freeipa-server

```
sudo dnf install freeipa-server freeipa-server-dns -y
```

- Открыть на Firewall порты

```
ipa-acme-manage enable
#sudo yum install firewall-cmd -y
#sudo systemctl enable firewalld --now
sudo firewall-cmd --add-service={freeipa-ldap,freeipa-ldaps,dns,kerberos,http,https,ntp} --permanent
sudo firewall-cmd --reload
```

- Выполнить установку Контроллера домена

```
set +o history
ipa-server-install --allow-zone-overlap \
  --ca-subject="CN=SDKSystems CA, O=SDKSystems Ltd, C=RU, L=Moscow" \
  --ca-signing-algorithm=SHA512withRSA \
  --hostname=dc01.sdksystems.ru \
  --realm=SDKSYSTEMS.RU \
  --domain=sdksystems.ru \
  --auto-reverse \
  --forwarder=10.10.0.1 \
  --no-dnssec-validation \
  --ntp-server=10.10.0.1 \
  --ntp-pool=0.ru.pool.ntp.ru \
  --mkhomedir \
  --no-hbac-allow \
  --no-host-dns \
  --setup-dns
set -o history
```

```
ipa-acme-manage enable
ipa-acme-manage pruning --enable --cron "0 0 1 * *"
```

```
Do you want to configure integrated DNS (BIND)? [no]: yes
Server host name [dc01.sdksystems.ru]:
Please confirm the domain name [sdksystems.ru]:
Please provide a realm name [SDKSYSTEMS.RU]:
Directory Manager password:
Password (confirm):
```

```
IPA admin password:
Password (confirm):

NetBIOS domain name [SDKSYSTEMS]:
Do you want to configure chrony with NTP server or pool address? [no]: yes
```

```
vi /etc/named/ipa-ext.conf
```

download

```
acl "trusted_network" {
  localnets;
  localhost;
  10.0.0.0/8;
  172.16.0.0/12;
  192.168.0.0/16;
};
```

```
vi /etc/named/ipa-options-ext.conf
```

download

```
allow-recursion { trusted_network; };
allow-query-cache { trusted_network; };
```

ipactl restart

Добавление реплики

На реплике:

```
yum install freeipa-server freeipa-server-dns -y
firewall-cmd --add-service={freeipa-ldap,freeipa-
ldaps,dns,kerberos,http,https,ntp} --permanent
firewall-cmd --reload
ipa-client-install --domain=sdksystems.ru --server=dc01.sdksystems.ru
kinit admin
ipa-replica-install
ipa-ca-install
ipa-dns-install --forwarder=10.10.0.1 \
--no-dnssec-validation \
--allow-zone-overlap
```