

Выполнение ansible-playbook

```
sergey@ubuntu1:~/otus/ldap$ ansible-playbook network.yml --tags vms

PLAY [vms] *****

TASK [deploy servers] *****
changed: [localhost] => (item={'name': 'ipa.skudrin.ru', 'memory_mb': 2048, 'hostname': 'ipa.skudrin.ru', 'ip': '10.100.11.147'})
changed: [localhost] => (item={'name': 'client1.skudrin.ru', 'memory_mb': 2048, 'hostname': 'client1.skudrin.ru', 'ip': '10.100.11.148'})
changed: [localhost] => (item={'name': 'client2.skudrin.ru', 'memory_mb': 2048, 'hostname': 'client2.skudrin.ru', 'ip': '10.100.11.149'})

PLAY [Base set up] *****

TASK [Gathering Facts] *****
ok: [client2.skudrin.ru]
ok: [ipa.skudrin.ru]
ok: [client1.skudrin.ru]

PLAY RECAP *****
client1.skudrin.ru      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
client2.skudrin.ru      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
ipa.skudrin.ru          : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
localhost               : ok=1    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

sergey@ubuntu1:~/otus/ldap$ ansible-playbook network.yml --tags ipa

PLAY [create vms] *****

PLAY [set ipa] *****

TASK [Gathering Facts] *****
ok: [ipa.skudrin.ru]

TASK [disable SELinux] *****
[WARNING]: SELinux state temporarily changed from 'enforcing' to 'permissive'. State change will take effect next reboot.
changed: [ipa.skudrin.ru]

TASK [disable SELinux now] *****
changed: [ipa.skudrin.ru]

TASK [enable chrony] *****
changed: [ipa.skudrin.ru]

TASK [change /etc/hosts] *****
changed: [ipa.skudrin.ru]

TASK [configure firewall] *****
changed: [ipa.skudrin.ru] => (item=firewall-cmd --permanent --add-port=53/{tcp,udp} --add-port={80,443}/tcp --add-port={88,464}/{tcp,udp} --add-port=123/udp --add-port={389,636}/tcp)
changed: [ipa.skudrin.ru] => (item=firewall-cmd --reload)
changed: [ipa.skudrin.ru] => (item=yum install -y @idm:DL1)
changed: [ipa.skudrin.ru] => (item=yum install -y ipa-server)

PLAY [set client] *****

PLAY RECAP *****
ipa.skudrin.ru          : ok=6    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

sergey@ubuntu1:~/otus/ldap$
```

Дополнительно на DNS сервере прописываем А записи

Диспетчер DNS

Файл Действие Вид Справка

DNS

DC

Зоны прямого просмотра

msdcs.ad.skudrin.ru

ad.skudrin.ru

skudrin.ru

Зоны обратного просмотра

Точки доверия

Серверы условной пер...

Название	Тип	Значение	Отметка времени
ad	(как папка верхнего уровня)		
(как папка верхнего уровня)	Начальная запись зон...	[3], dc.ad.skudrin.ru., host...	статический
(как папка верхнего уровня)	Сервер имен (NS)	dc.ad.skudrin.ru.	статический
dc	Узел (A)	10.100.11.200	статический
pc	Узел (A)	192.168.88.2	статический
ipa	Узел (A)	10.100.11.147	
client1	Узел (A)	10.100.11.148	
client2	Узел (A)	10.100.11.149	

[root@ipa ~]#ipa-server-install выполняем команду, вводим параметры

```
NetBIOS domain name [SKUDRIN]:

Do you want to configure chrony with NTP server or pool address? [no]:

The IPA Master Server will be configured with:
Hostname:      ipa.skudrin.ru
IP address(es): 10.100.11.147
Domain name:   skudrin.ru
Realm name:    SKUDRIN.RU

The CA will be configured with:
Subject DN:    CN=Certificate Authority, O=SKUDRIN.RU
Subject base:  O=SKUDRIN.RU
Chaining:      self-signed

Continue to configure the system with these values? [no]: yes

The following operations may take some minutes to complete.
Please wait until the prompt is returned.

Disabled p11-kit-proxy
Synchronizing time
No SRV records of NTP servers found and no NTP server or pool address was provided.
Using default chrony configuration.
Attempting to sync time with chronyc.
Time synchronization was successful.
Configuring directory server (dirsrv). Estimated time: 30 seconds
[1/43]: creating directory server instance
Validate installation settings ...
```

```
...

Client hostname: ipa.skudrin.ru
Realm: SKUDRIN.RU
DNS Domain: skudrin.ru
IPA Server: ipa.skudrin.ru
BaseDN: dc=skudrin,dc=ru

Configured /etc/sss/sss.conf
Systemwide CA database updated.
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring skudrin.ru as NIS domain.
Client configuration complete.
The ipa-client-install command was successful

Please add records in this file to your DNS system: /tmp/ipa.system.records.efkhq4xg.db
=====
Setup complete

Next steps:
  1. You must make sure these network ports are open:
      TCP Ports:
        * 80, 443: HTTP/HTTPS
        * 389, 636: LDAP/LDAPS
        * 88, 464: kerberos
      UDP Ports:
        * 88, 464: kerberos
        * 123: ntp

  2. You can now obtain a kerberos ticket using the command: 'kinit admin'
      This ticket will allow you to use the IPA tools (e.g., ipa user-add)
      and the web user interface.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password
The ipa-server-install command was successful
[root@ipa ~]#
```

После успешной установки FreeIPA, проверим, что сервер Kerberos может выдать нам билет:

```
[root@ipa ~]# kinit admin
Password for admin@SKUDRIN.RU:
[root@ipa ~]# klist
Ticket cache: KCM:0
Default principal: admin@SKUDRIN.RU

Valid starting    Expires    Service principal
06/01/2024 13:16:12  06/02/2024 12:45:59  krbtgt/SKUDRIN.RU@SKUDRIN.RU
[root@ipa ~]#
```

Заходим в Web-интерфейс нашего FreeIPA-сервера:

The screenshot shows the FreeIPA web interface in a browser. The address bar shows 'ipa.skudrin.ru'. The page title is 'Identity Management'. The main navigation bar includes 'Идентификация', 'Политика', 'Аутентификация', 'Сетевые службы', and 'IPA-сервер'. The 'Идентификация' section is active, showing 'Пользователи', 'Узлы', 'Службы', 'Группы', 'Представления ID', 'Автоучастник', and 'Subordinate IDs'. The 'Пользователи' section is further divided into 'Активные пользователи', 'Неподтвержденные пользователи', and 'Хранимые пользователи'. The 'Активные пользователи' section is selected, showing a table of active users. The table has columns: 'Имя учётной записи пользователя', 'Имя', 'Фамилия', 'Состояние', 'UID', 'Адрес электронной почты', 'Номер телефона', and 'Должность'. One user is listed: 'admin' with the role 'Administrator' and status 'Включено'. The table also shows a search bar, buttons for 'Обновить', 'Удалить', 'Добавить', 'Отключить', 'Включить', and 'Действия'. The footer of the table indicates 'Показано записей: с 1 по 1 из 1'.

Настраиваем клиентов:

```
sergey@ubuntu1:~/otus/ldap$ ansible-playbook network.yml --tags client

PLAY [create vms] *****

PLAY [set ipa] *****

PLAY [set client] *****

TASK [Gathering Facts] *****
ok: [client2.skudrin.ru]
ok: [client1.skudrin.ru]

TASK [disable SELinux] *****
[WARNING]: SELinux state temporarily changed from 'enforcing' to 'permissive'. State change will take effect next
reboot.
changed: [client2.skudrin.ru]
changed: [client1.skudrin.ru]

TASK [disable SELinux now] *****
changed: [client1.skudrin.ru]
changed: [client2.skudrin.ru]

TASK [enable chrony] *****
changed: [client1.skudrin.ru]
changed: [client2.skudrin.ru]

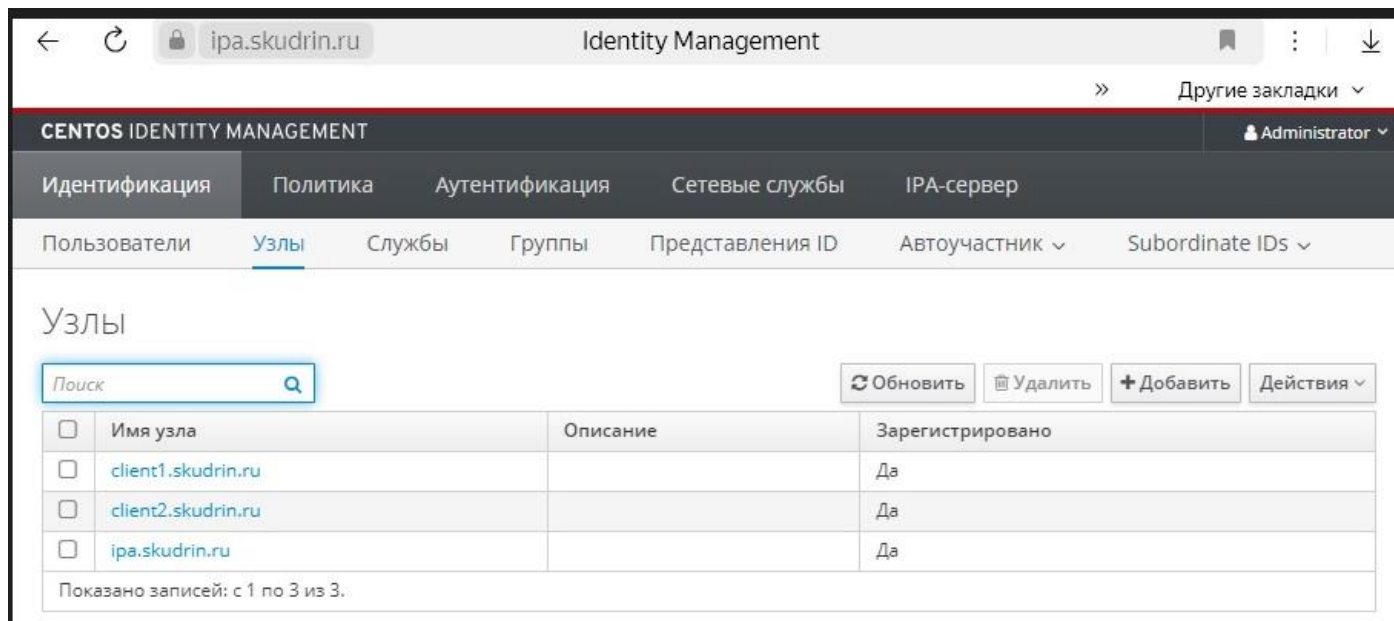
TASK [change /etc/hosts] *****
changed: [client2.skudrin.ru]
changed: [client1.skudrin.ru]

TASK [install module ipa-client] *****
changed: [client2.skudrin.ru]
changed: [client1.skudrin.ru]

TASK [add host to ipa-server] *****
changed: [client2.skudrin.ru]
changed: [client1.skudrin.ru]

PLAY RECAP *****
client1.skudrin.ru      : ok=7    changed=6    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
client2.skudrin.ru      : ok=7    changed=6    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```


Появились 2 новых узла:

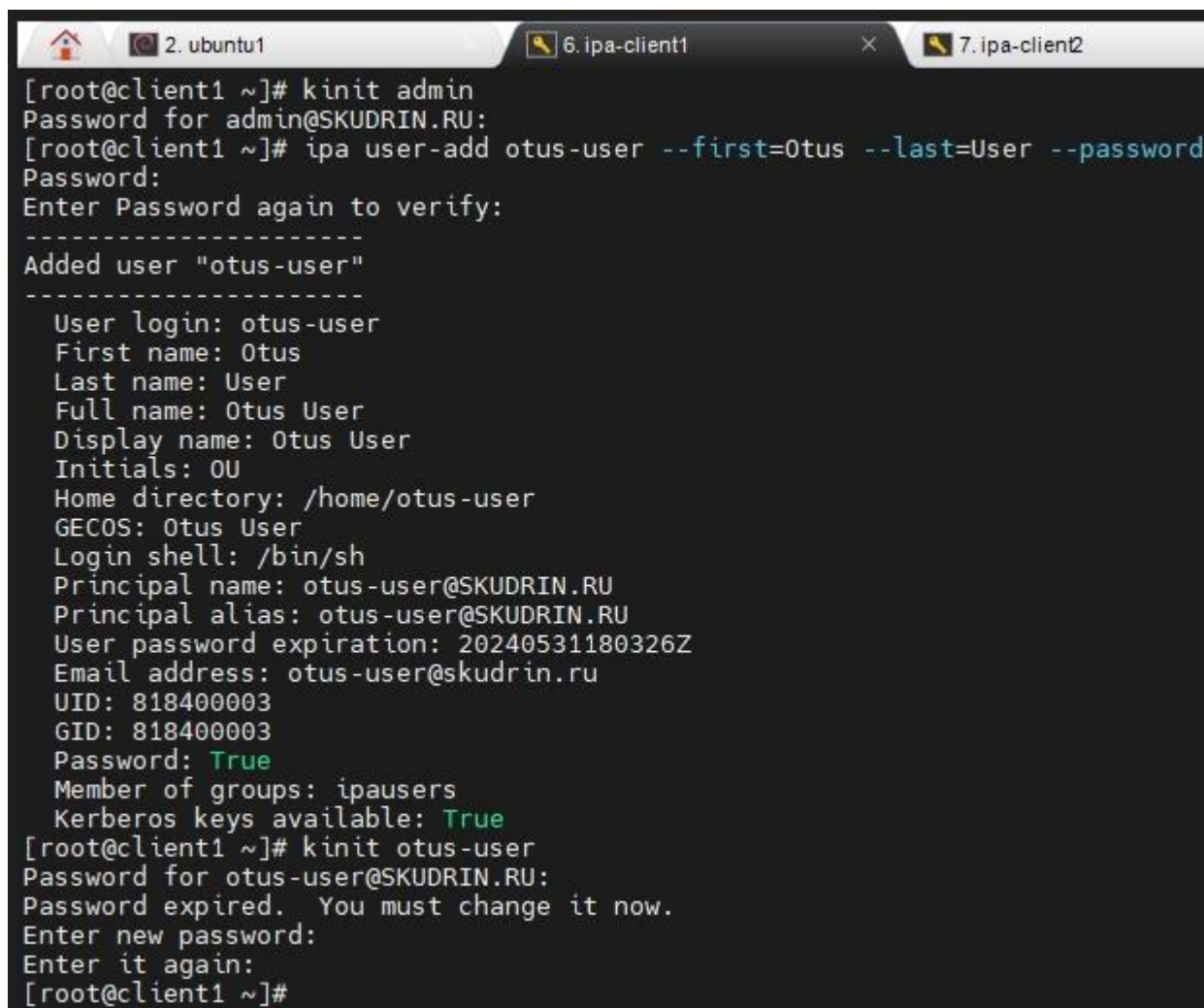


The screenshot shows the Identity Management web interface for ipa.skudrin.ru. The top navigation bar includes tabs for Идентификация, Политика, Аутентификация, Сетевые службы, and IPA-сервер. Below this, there are sub-tabs for Пользователи, Узлы (selected), Службы, Группы, Представления ID, Автоучастник, and Subordinate IDs. The main content area is titled 'Узлы' and contains a search bar, buttons for Обновить, Удалить, and + Добавить, and a Действия dropdown. A table lists three nodes:

<input type="checkbox"/>	Имя узла	Описание	Зарегистрировано
<input type="checkbox"/>	client1.skudrin.ru		Да
<input type="checkbox"/>	client2.skudrin.ru		Да
<input type="checkbox"/>	ipa.skudrin.ru		Да

Below the table, it says 'Показано записей: с 1 по 3 из 3.'

Проверим работу LDAP, для этого на сервере FreeIPA создадим пользователя и залогинимся:



```
[root@client1 ~]# kinit admin
Password for admin@SKUDRIN.RU:
[root@client1 ~]# ipa user-add otus-user --first=Otus --last=User --password
Password:
Enter Password again to verify:
-----
Added user "otus-user"
-----
User login: otus-user
First name: Otus
Last name: User
Full name: Otus User
Display name: Otus User
Initials: OU
Home directory: /home/otus-user
GECOS: Otus User
Login shell: /bin/sh
Principal name: otus-user@SKUDRIN.RU
Principal alias: otus-user@SKUDRIN.RU
User password expiration: 20240531180326Z
Email address: otus-user@skudrin.ru
UID: 818400003
GID: 818400003
Password: True
Member of groups: ipausers
Kerberos keys available: True
[root@client1 ~]# kinit otus-user
Password for otus-user@SKUDRIN.RU:
Password expired. You must change it now.
Enter new password:
Enter it again:
[root@client1 ~]#
```

Успешно