FreeIPA

1.6.3209 WNAM adctool FreeIPA :

- RADIUS- PAP EAP_PEAP (NT Hash).
- RADIUS- PAP, EAP_PEAP EAP_TLS (Identity) ( ).
- TACACS+ / .
- - WNAM.

FreeIPA 4.8.10, Astra Linux 1.7.3 "". Microsoft Active Directory, / , FreeIPA .

:

- (): astradom.wnam.ru;
- (): wnam16-astra.astradom.wnam.ru;
- , adctool: wnam-15.astradom.wnam.ru;

1.

- root (sudo).

```
###

apt install freeipa-server-trust-ad

ipa-adtrust-install --add-sids

###

ipa permission-add 'ipaNTHash service read' --attrs=ipaNTHash --type=user --
right=read
ipa privilege-add 'Radius services' --desc='Privileges needed to allow radiusd
servers to operate'
ipa privilege-add-permission 'Radius services' --permissions='ipaNTHash service
read'

###    RADIUS-,

ipa role-add 'Radius server' --desc="Radius server role"
ipa role-add-privilege --privileges="Radius services" 'Radius server'

###    ,

ipa service-add 'wnam/wnam16-astra.astradom.wnam.ru'
```

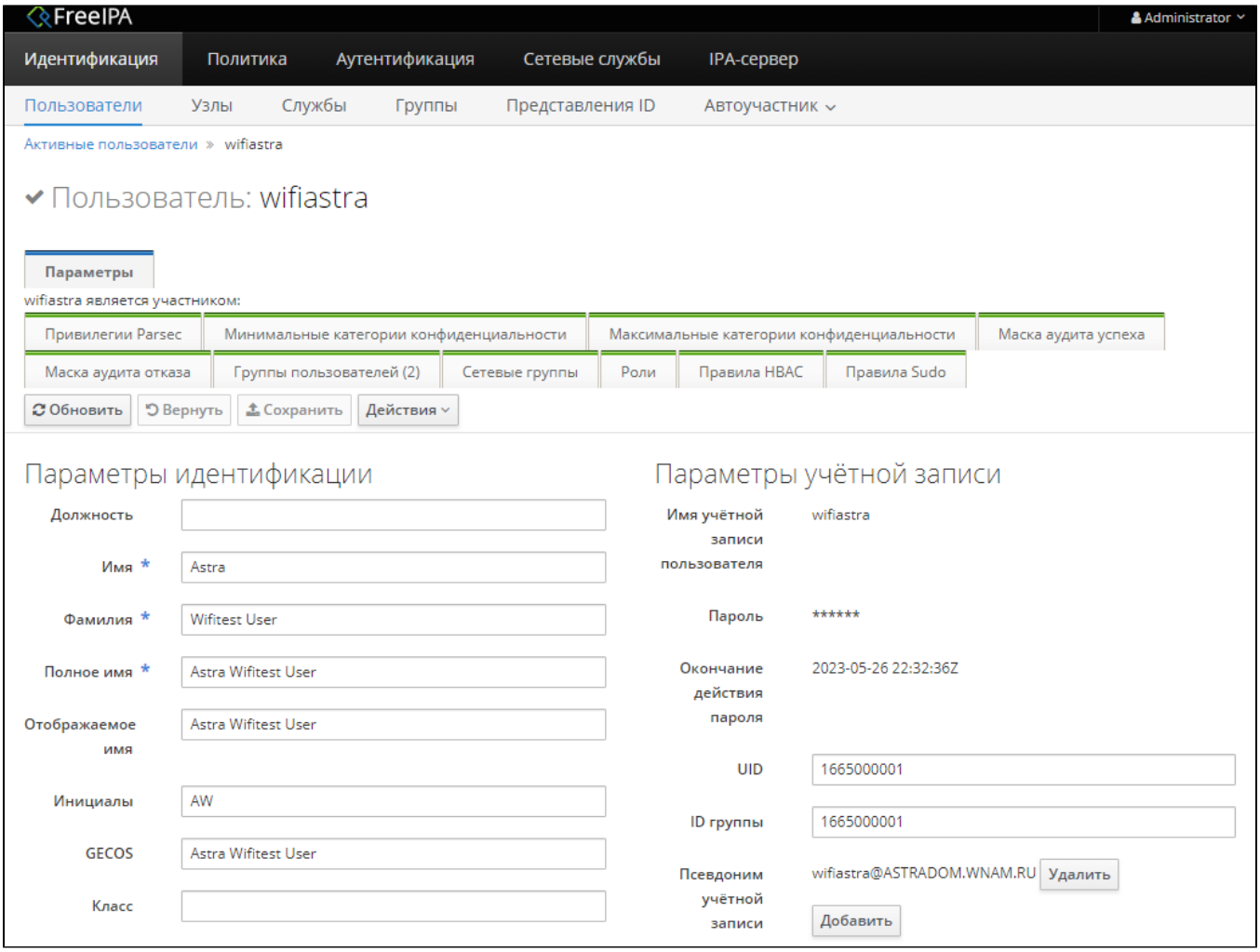
ldif.txt , (- Qwerty123):

```
dn: krbprincipalname=wnam/wnam16-astra.astradom.wnam.ru@ASTRADOM.WNAM.RU,
cn=services,cn=accounts,dc=astradom,dc=wnam,dc=ru
changetype: modify
add: objectClass
objectClass: simpleSecurityObject
-
add: userPassword
userPassword: Qwerty123
```

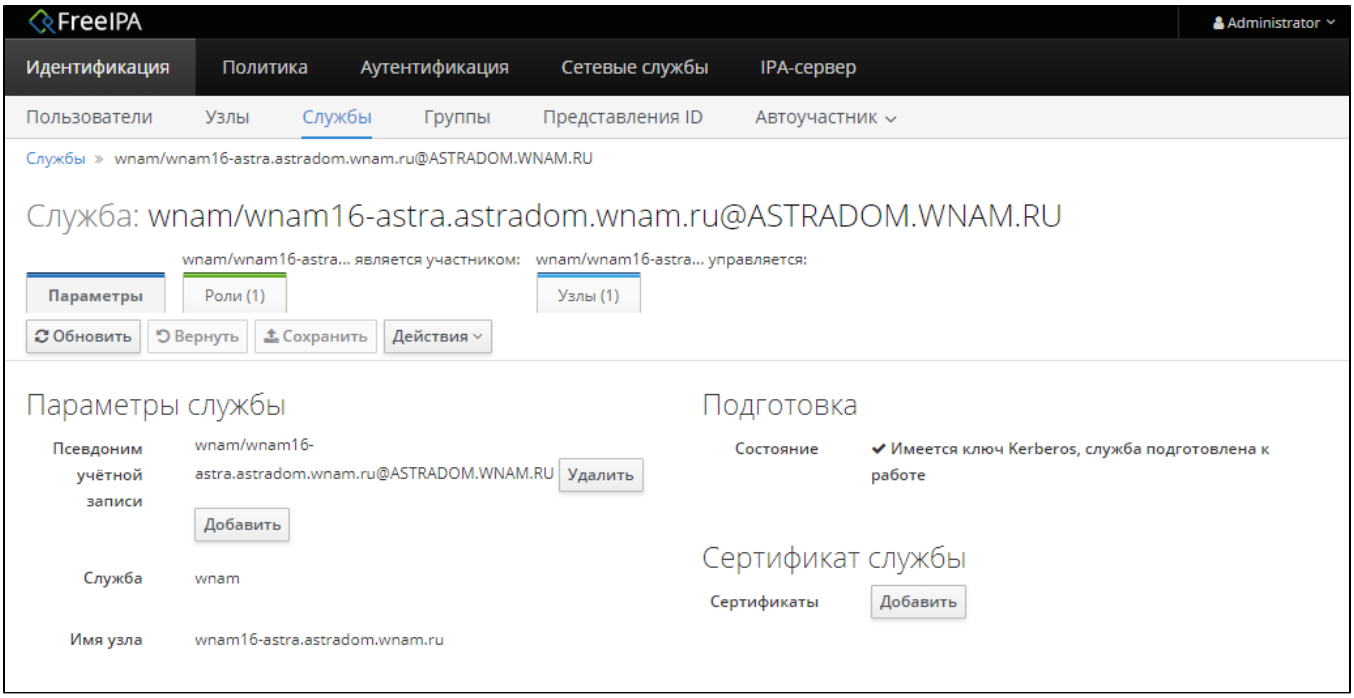
:

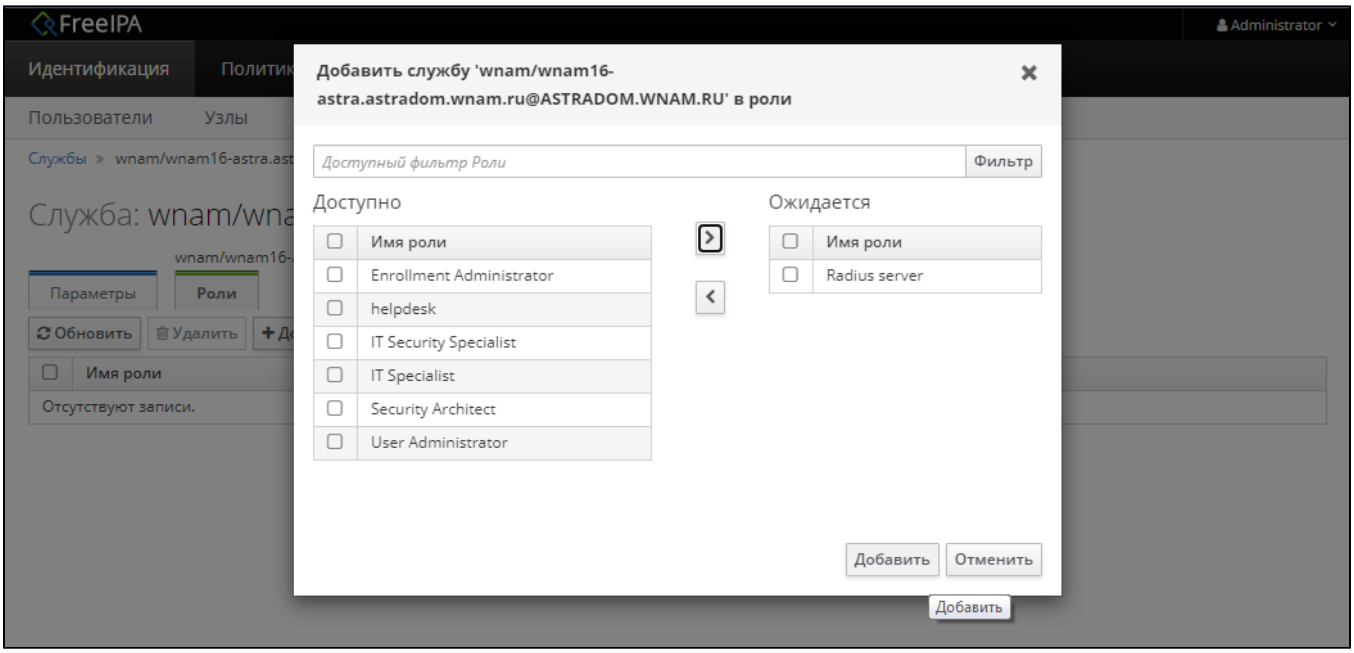
```
ldapmodify -f ldif.txt -D 'cn=Directory Manager' -W -H ldap://wnam16-astra.
astradom.wnam.ru -Z
```

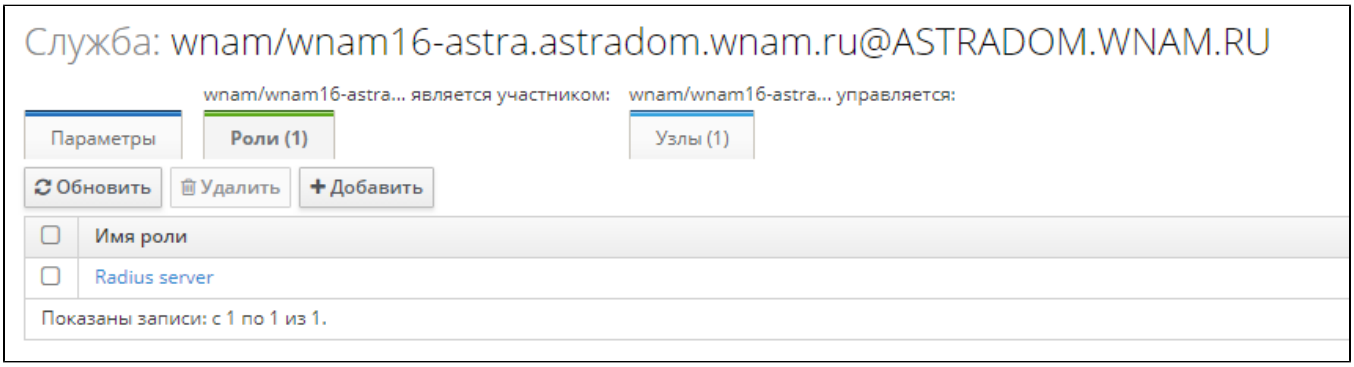
wifiastra (ipa-adtrust-install,):

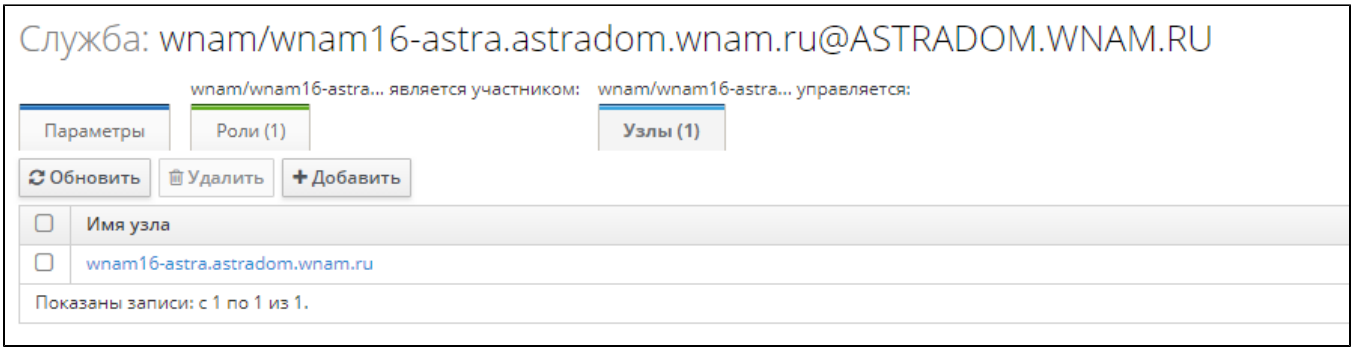


- FreeIPA "Radius server" wnam/wnam16-astra.astradom.wnam.ru :



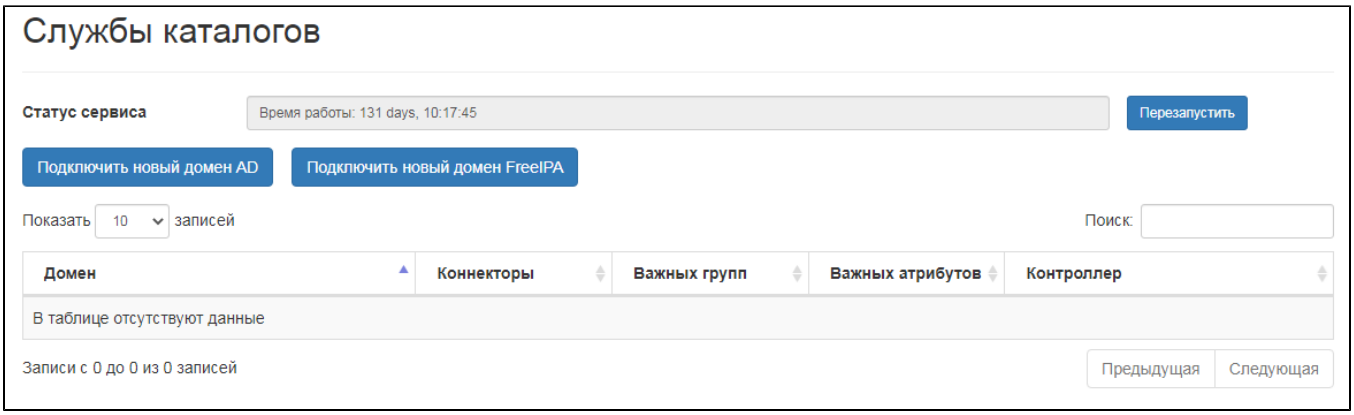






2. WNAM

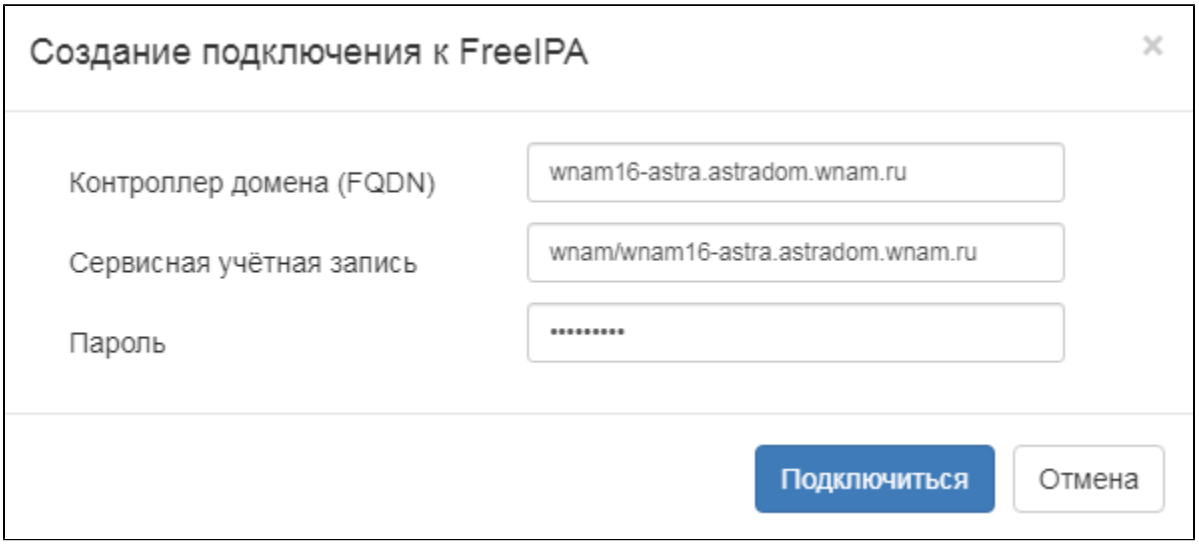
WNAM "" " " " FreeIPA":



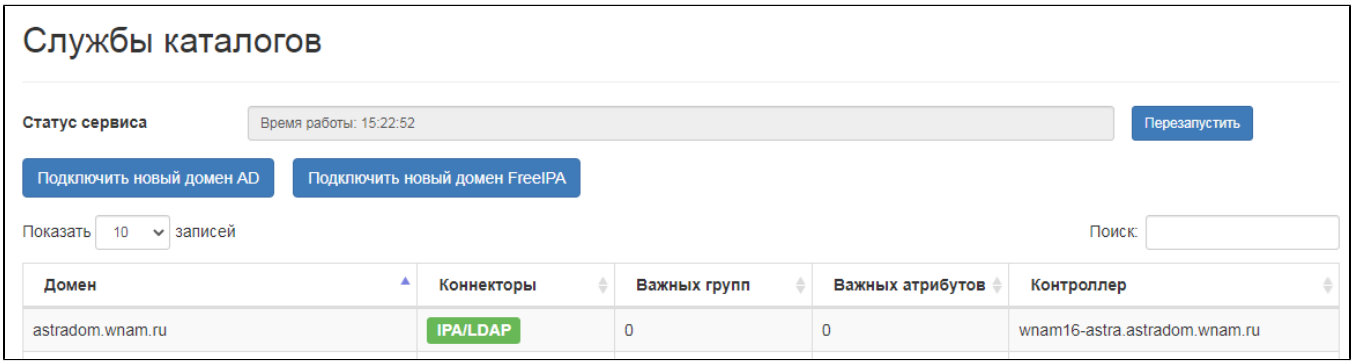
:

- ;
- ;
- .

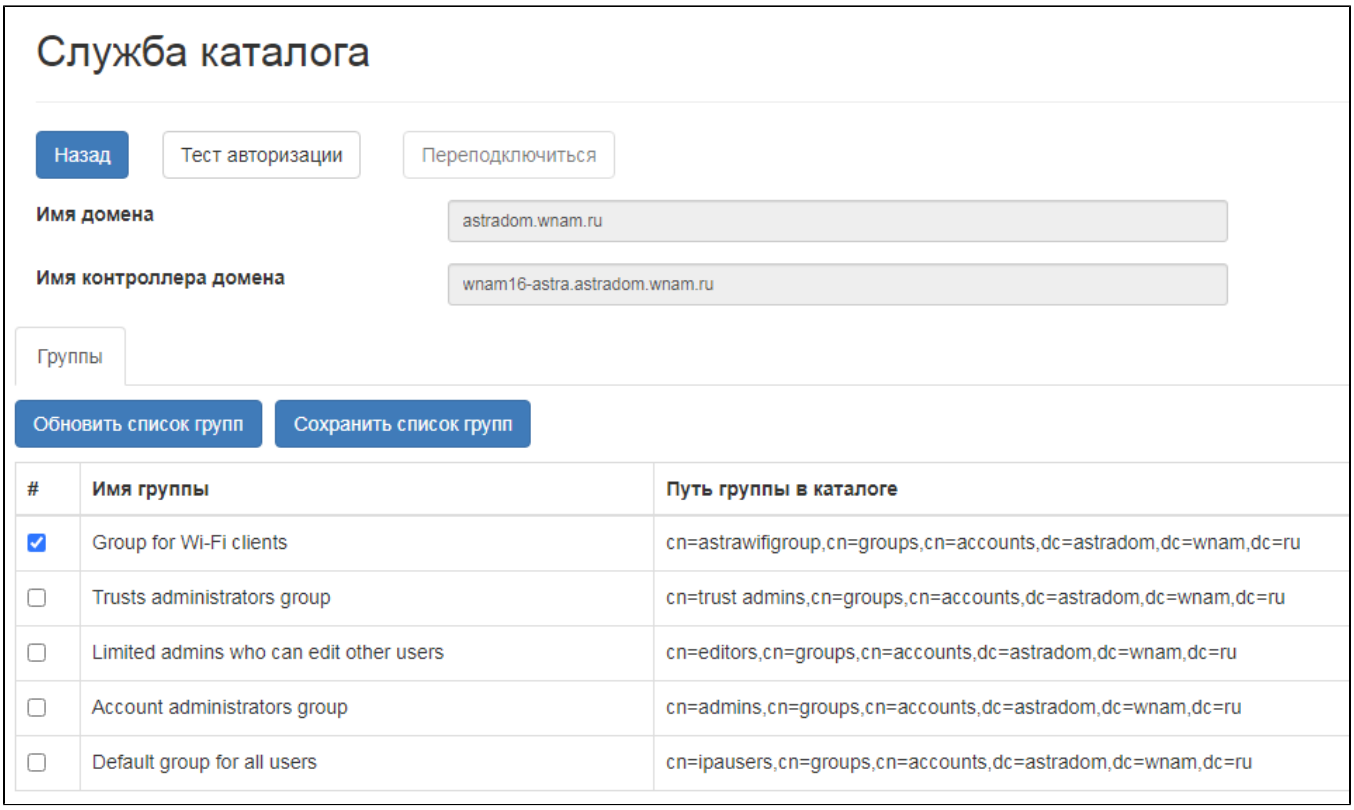
/home/wnam/adctool/config.json. .



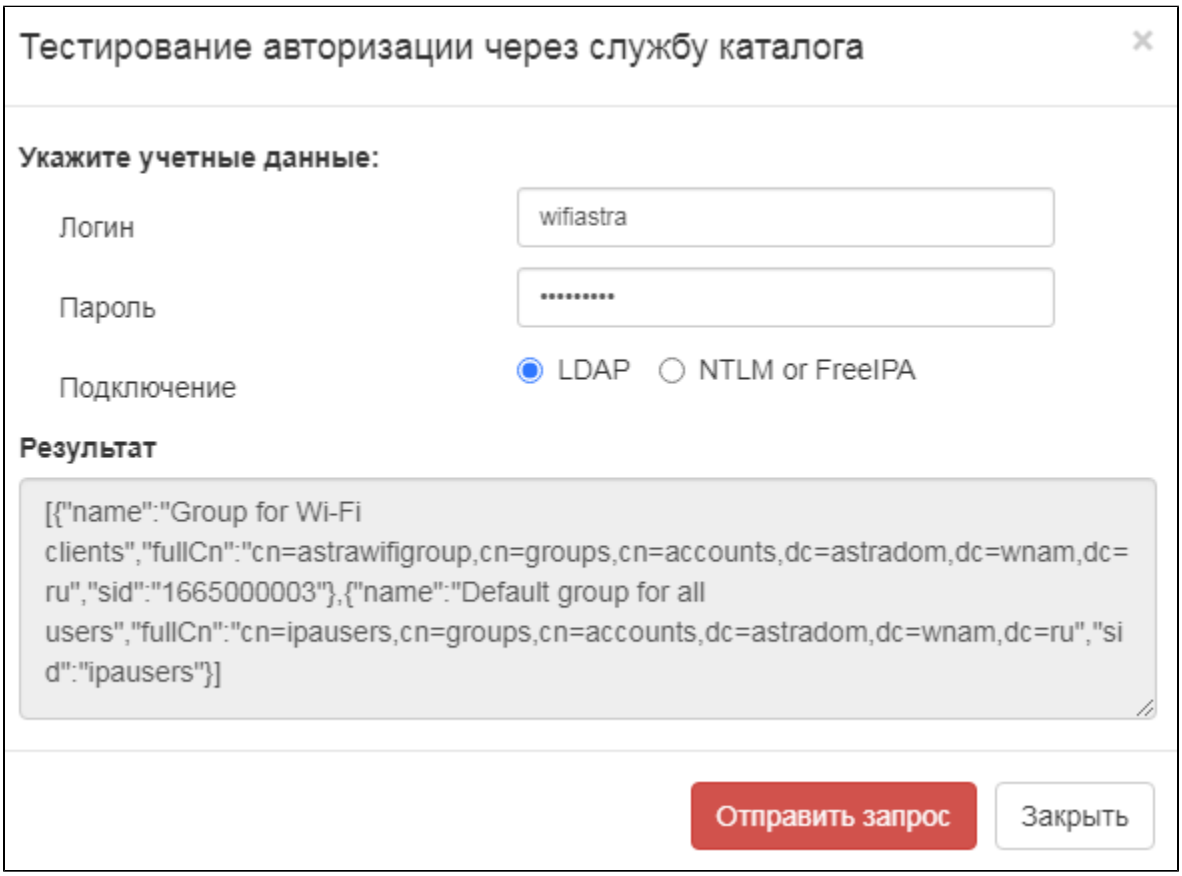
:

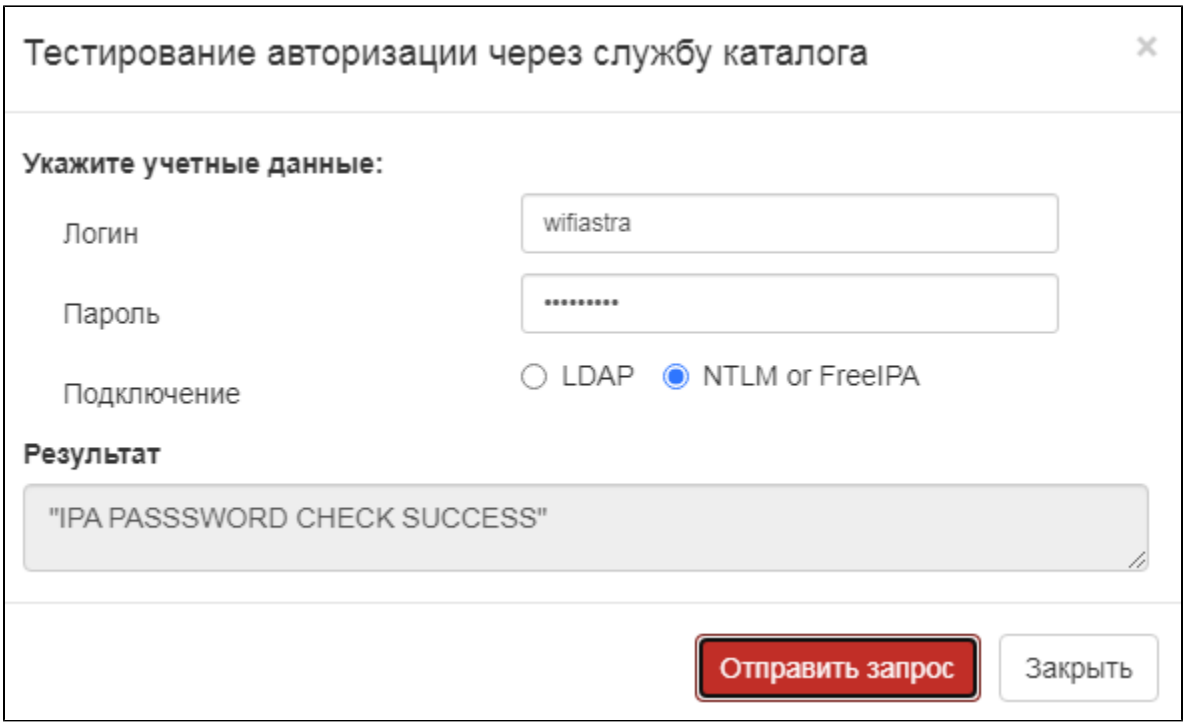


:


Служба каталога
Назад
Тест авторизации
Переподключиться
Имя домена
astradom.wnam.ru
Имя контроллера домена
wnam16-astra.astradom.wnam.ru
Группы
Обновить список групп
Сохранить список групп
Имя группы Путь группы в каталоге
Group for Wi-Fi clients cn=astrawifigroup,cn=groups,cn=accounts,dc=astradom,dc=wnam,dc=ru
Trusts administrators group cn=trust admins,cn=groups,cn=accounts,dc=astradom,dc=wnam,dc=ru
Limited admins who can edit other users cn=editors,cn=groups,cn=accounts,dc=astradom,dc=wnam,dc=ru
Account administrators group cn=admins,cn=groups,cn=accounts,dc=astradom,dc=wnam,dc=ru
Default group for all users cn=ipausers,cn=groups,cn=accounts,dc=astradom,dc=wnam,dc=ru

LDAP :


Тестирование авторизации через службу каталога
Укажите учетные данные:
Логин
wifiastra
Пароль
Подключение
LDAP
NTLM or FreeIPA
Результат
[{"name":"Group for Wi-Fi clients","fullCn":"cn=astrawifigroup,cn=groups,cn=accounts,dc=astradom,dc=wnam,dc=ru","sid":"1665000003"},{"name":"Default group for all users","fullCn":"cn=ipausers,cn=groups,cn=accounts,dc=astradom,dc=wnam,dc=ru","sid":"ipausers"}]
Отправить запрос
Закрыть



, FreeIPA WNAM. , /home/wnam/adctool/logs/console.log.