

FreeIPA

1.6.3209 WNAME adctool FreeIPA :

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

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

:

- (): astradom.wname.ru;
- (): wname16-astra.astradom.wname.ru;
- , adctool: wname-15.astradom.wname.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 'wname/wname16-astra.astradom.wname.ru'
```

ldif.txt , (- Qwerty123):

```
dn: krbprincipalname=wname/wname16-astra.astradom.wname.ru@ASTRADOM.WNAME.RU,  
cn=services,cn=accounts,dc=astradom,dc=wname,dc=ru  
changetype: modify  
add: objectClass  
objectClass: simpleSecurityObject  
-  
add: userPassword  
userPassword: Qwerty123
```

:

```
ldapmodify -f ldif.txt -D 'cn=Directory Manager' -W -H ldap://wname16-astra.  
astradom.wname.ru -Z
```

wifiastra (ipa-adtrust-install,):

FreeIPA

Administrator

Идентификация

Политика

Аутентификация

Сетевые службы

IPA-сервер

Пользователи

Узлы

Службы

Группы

Представления ID

Автоучастник

Активные пользователи > wifiastra

✓ Пользователь: wifiastra

Параметры

wifiastra является участником:

Привилегии Parsec

Минимальные категории конфиденциальности

Максимальные категории конфиденциальности

Маска аудита успеха

Маска аудита отказа

Группы пользователей (2)

Сетевые группы

Роли

Правила HBAC

Правила Sudo

Обновить

Вернуть

Сохранить

Действия

Параметры идентификации

Параметры учётной записи

Должность

Имя *

Фамилия *

Полное имя *

Отображаемое имя

Инициалы

GECOS

Класс

Имя учётной записи пользователя

Пароль

Окончание действия пароля

UID

ID группы

Псевдоним учётной записи

Имя учётной записи

Пароль

Окончание действия пароля

UID

ID группы

Псевдоним учётной записи

Удалить

Добавить

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

FreeIPA

Administrator

Идентификация

Политика

Аутентификация

Сетевые службы

IPA-сервер

Пользователи

Узлы

Службы

Группы

Представления ID

Автоучастник

Службы > wnam/wnam16-astra.astradom.wnam.ru@ASTRADOM.WNAM.RU

Служба: wnam/wnam16-astra.astradom.wnam.ru@ASTRADOM.WNAM.RU

wnam/wnam16-astra... является участником: wnam/wnam16-astra... управляется:

Параметры

Роли (1)

Узлы (1)

Обновить

Вернуть

Сохранить

Действия

Параметры службы

Подготовка

Псевдоним учётной записи

Служба

Имя узла

Псевдоним учётной записи

Служба

Имя узла

Удалить

Добавить

Состояние

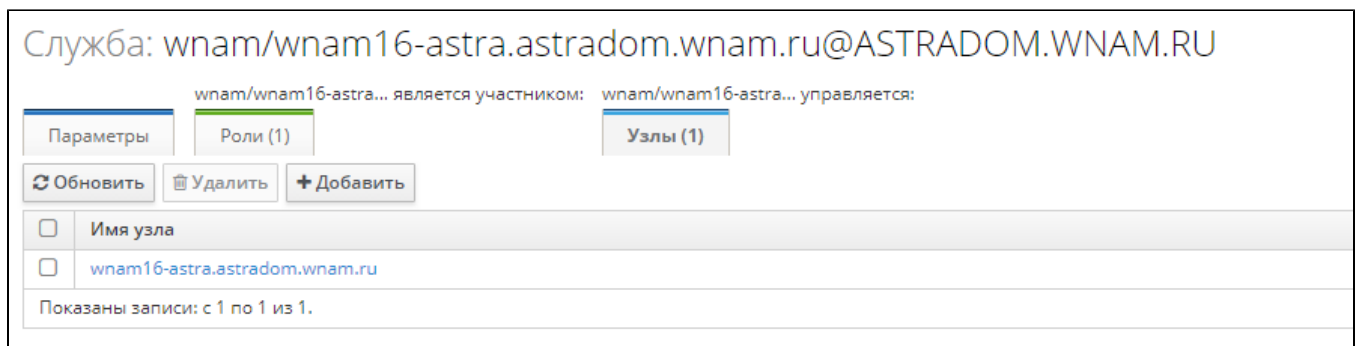
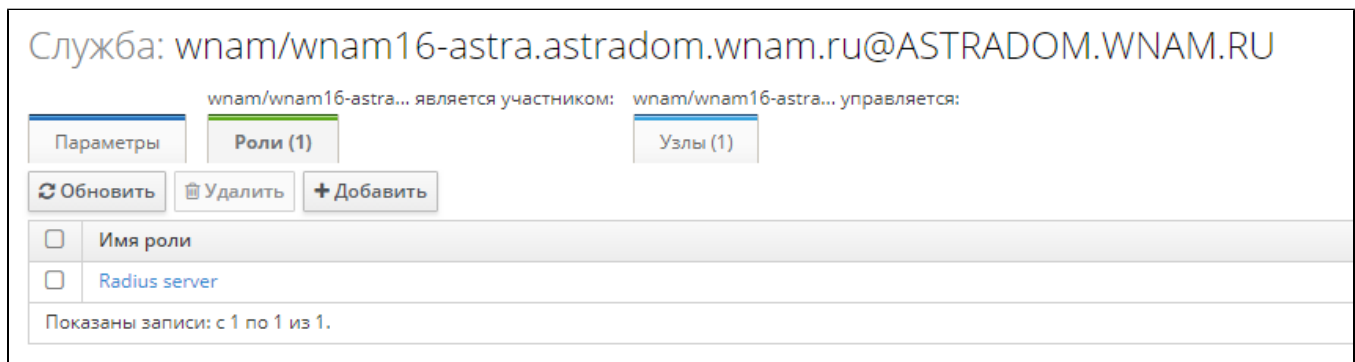
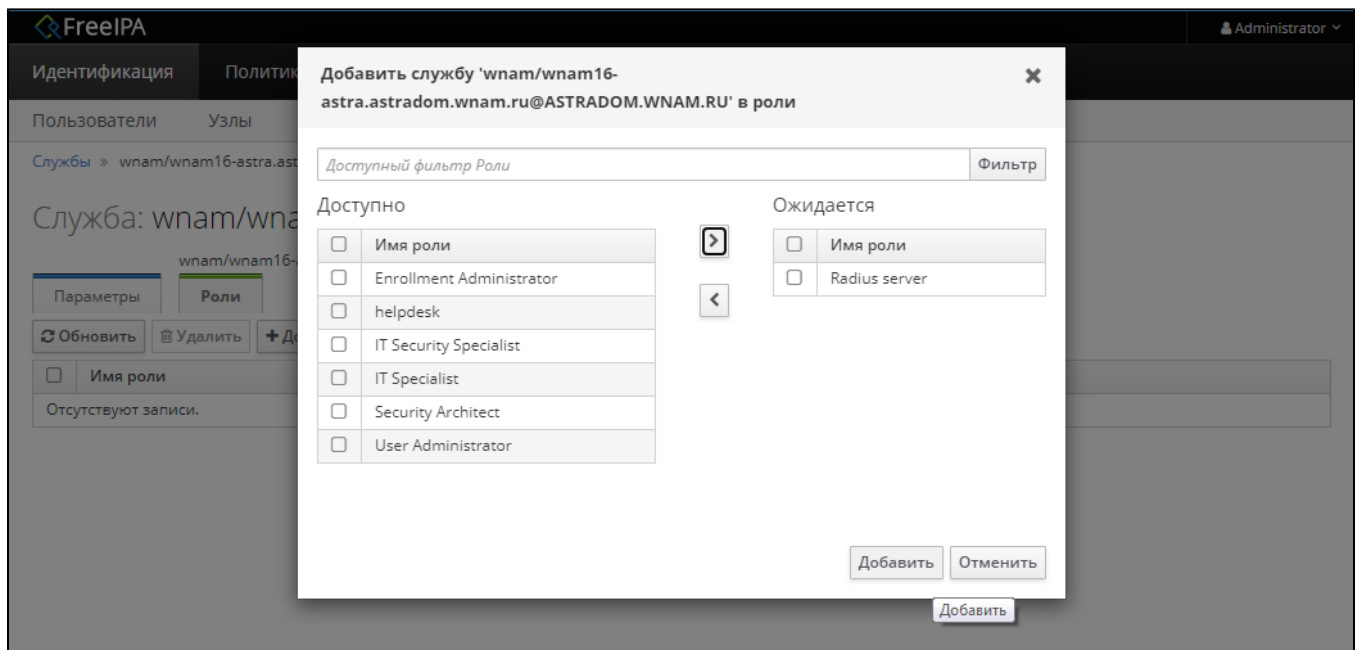
Сертификат службы

Состояние

Сертификаты

Имеется ключ Kerberos, служба подготовлена к работе

Добавить



2. WNAM

WNAM "" "" " FreeIPA":

Службы каталогов

Статус сервиса

Время работы: 131 days, 10:17:45

Перезапустить

Подключить новый домен AD

Подключить новый домен FreeIPA

Показать 10 записей

Поиск:

Домен	Коннекторы	Важных групп	Важных атрибутов	Контроллер
В таблице отсутствуют данные				

Записи с 0 до 0 из 0 записей

Предыдущая

Следующая

:

•
•
•

/home/wnam/adctool/config.json.

Создание подключения к FreeIPA



Контроллер домена (FQDN)

wnam16-astra.astradom.wnam.ru

Сервисная учётная запись

wnam/wnam16-astra.astradom.wnam.ru

Пароль

Подключиться

Отмена

:

Службы каталогов

Статус сервиса

Время работы: 15:22:52

Перезапустить

Подключить новый домен AD

Подключить новый домен FreeIPA

Показать 10 записей

Поиск:

Домен	Коннекторы	Важных групп	Важных атрибутов	Контроллер
astradom.wnam.ru	IPA/LDAP	0	0	wnam16-astra.astradom.wnam.ru

:

Служба каталога

[Назад](#)[Тест авторизации](#)[Переключиться](#)

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=admin,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](#)

Тестирование авторизации через службу каталога

Укажите учетные данные:

Логин

wifiastra

Пароль

.....

Подключение

☐ LDAP

☒ NTLM or FreeIPA

Результат

"IPA PASSSSWORD CHECK SUCCESS"

Отправить запрос

Заккрыть

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