


FreeIPA - Active Directory

- **FreeIPA:**
 -
 -
 - **DNS**
 -
 -
 - **AD**
 -
- **AD**


 :

- Astra Linux

- Active Directory (AD), :
 - windomain.ad (FreeIPA Windows AD);
 - , NETBIOS WINDOMAIN;
 - :
 - winserver;
 - IP- (<IP-__AD>);
 - Windows Server 2008 R2 Windows, ;

 . - AD.

- AD Administrator, ;


 ipa trust-add AD


 AD , Domain Admins, , CIFS 3221225506.

- FreeIPA FreeIPA:
 - ipadomain.ipa;
 - , NETBIOS IPADOMAIN;
 - FreeIPA:
 - Astra Linux;
 - ipaserver;
 - IP- (<IP-__FreeIPA>);
 - FreeIPA admin ;
- winserver ipaserver ,

ping <IP-__FreeIPA>

ping <IP-__AD>

 FreeIPA Windows AD (broadcast zone). .

 AD FreeIPA , 2 2 .

FreeIPA , FreeIPA **FreeIPA Astra Linux** fly-admin-freeipa-server astra-freeipa-server. FreeIPA , , freeipa-server-trust-ad ().



FreeIPA

FreeIPA:

FreeIPA

```
kinit admin
id admin
getent passwd admin
```



FreeIPA



samba



ipa-adtrust-install, freeipa-server-trust-ad.

FreeIPA :

```
sudo ipa-adtrust-install
```

:

1. «y», , «».
2. IPA.
3. , Enter.
4. «y».

DNS

:

- FreeIPA:

```
ipa dnsforwardzone-add <__Windows_AD> --forwarder=<IP-__AD> --forward-policy=only
```

- Windows AD:

```
dnscmd 127.0.0.1 /ZoneAdd <__FreeIPA> /Forwarder <IP-__FreeIPA>
```

FreeIPA . FreeIPA DNS (Astra Linux Special Edition x.7), DNS Windows AD , "ipa: WARNING: DNSSEC: "... SOA" DNSSEC ..."

1. Windows AD DNS, AD DNS, DNSSEC - - .
2. FreeIPA Windows AD :

```
dig dnskey windomain.ad. @<IP-__Windows_AD> +noall +answer
```

:

```
; <<>> DiG 9.11.3-lubuntu1.11-Debian <<>> dnskey srv.rbt. @10.7.21.21 +noall +answer
;; global options: +cmd
windomain.ad. 3600 IN DNSKEY 256 3 8 AwEAAcARV
/UHxAmt2ESvWxGHgoIgtEasYABj5i4kJfcs+Tiuy+jbTgKf
kZx8LDyTBAIEC9ZX8enlR1ZNzUS1TlxZKGJ2IHqJU2BobiiQ0qFVSDLL
0+GbOCLP7npDB00PhqgOcaF8j3m2+TtP2ssqaGbPrT5Ya+nkRwr0G6ik e3m6uTRD
windomain.ad. 3600 IN DNSKEY 256 3 8
AwEAAZIBjJ7fkvudTvuPBNA9K8glJhplKf8SJ2Ppchg2bpE7W/6hVxqP
zdnrpjaaPYsXuIMQFqIRz2QtKJ1VhKldnzOm6Tpa4Wsr+dX5XUUTkV72
k4Hl+QVKPCGpthqIb8j60kYa7PXRKMDv4Jw+U96YsQbA621/M10/8UZB bD3iJ0x9
windomain.ad. 3600 IN DNSKEY 257 3 8
AwEAAa+KDuNaIQ5ChuMYDIS4Y6GQtXiQJ1qtU7+CDwn2zgVPyoqilDLc 18IIWyGRDsGU2NUXnem704dwghGpUQ9XbzJCKzueC
/dQSUS5mdZjhvrM +/knsCizku7/0x5B9U3Kj91lpAe5CPUY7rldKQtYYINiAmnJprIuUbBs
jogC4IYTA6mMmEW2cvOmuNfpAB4IxnFZLmXA41E0DR3JCVLsnxQ20Gq1 TErWsd7st458RKpp4mEt1mU2JYWltJYA82lp0WLqXOO1B
/ievLWESnvH oyGclg01zm4Lhc9Opd3zNRQYea4IFN2WHXIkOThqlA291Gw4gw85eBhs xdnPd2dDHts=
windomain.ad. 3600 IN DNSKEY 257 3 8 AwEAAb6hMq89Tf4Cf5ND6R
/R8FYcbHd5uyxUo2p0lvLkw8VWL1/Ix8Xp abymJ6a8lMKU39CKfp/lxMxWbPicOpT72vnoDhfbck9017EwI40PmMI3
51acR5EtdQwtwz44aNm07QlXSdYJLYrvEq76M3jn20lwFgb+oSQZFA2U 9b9
/ssc8uBzLuCMC7DbHFU7V4hb36LlheqnNecYtilOg5MckEfU01MCg SwoNBdlpkyi+S5hszIaSI5Q28DVBA
/lDdF7zRIFlvs7DdAwPdrODhx/o QjN40cQZj+DAVeR/vZnGUK+LBQ+gXTjOqfECJKyVOuljzL+IwBb74xzO 9c1N10/Uz+E=
```

3. /etc/bind/bind.keys managed-keys : . .:

```
windomain.ad. initial-key 257 3 8 "AwEAAa+KDuNaIQ5ChuMYDIS4Y6GQtXiQJ1qtU7+CDwn2zgVPyoqilDLc
18IIWyGRDsGU2NUXnem704dwghGpUQ9XbzJCKzueC/dQSUS5mdZjhvrM
+/knsCizku7/0x5B9U3Kj91lpAe5CPUY7rldKQtYYINiAmnJprIuUbBs
jogC4IYTA6mMmEW2cvOmuNfpAB4IxnFZLmXA41E0DR3JCVLsnxQ20Gq1
TErWsd7st458RKpp4mEt1mU2JYWltJYA82lp0WLqXOO1B/ievLWESnvH
oyGclg01zm4Lhc9Opd3zNRQYea4IFN2WHXIkOThqlA291Gw4gw85eBhs
xdnPd2dDHts=" ;
windomwin.ad. initial-key 257 3 8 "AwEAAb6hMq89Tf4Cf5ND6R/R8FYcbHd5uyxUo2p0lvLkw8VWL1/Ix8Xp
abymJ6a8lMKU39CKfp/lxMxWbPicOpT72vnoDhfbck9017EwI40PmMI3
51acR5EtdQwtwz44aNm07QlXSdYJLYrvEq76M3jn20lwFgb+oSQZFA2U
9b9/ssc8uBzLuCMC7DbHFU7V4hb36LlheqnNecYtilOg5MckEfU01MCg
SwoNBdlpkyi+S5hszIaSI5Q28DVBA/lDdF7zRIFlvs7DdAwPdrODhx/o
QjN40cQZj+DAVeR/vZnGUK+LBQ+gXTjOqfECJKyVOuljzL+IwBb74xzO
9c1N10/Uz+E=" ;
```

4. bind9-pkcs11:

```
sudo systemctl restart bind9-pkcs11
```

.

FreeIPA:

- #1, :

```
ping -c 3 winserver.windomain.ad
```

- #2, :

```
dig SRV _ldap._tcp.ipadomain.ipa
```

- #3, :

```
dig SRV _ldap._tcp.windomain.ad
```

- #4, samba



```
-k :
    (), Kerberos. , , samba .
    , localadmin kinit admin@ipadomain.ipa, smbclient -k, , localadmin Kerberos.
    admin@ipadomain.ipa () - , admin .

    () samba .
```

```
:
- admin() ;
- admin, admin;
- , samba.
( ):
```

```
sudo login admin
kinit
smbclient -k -L ipaserver.ipadomain.ipa
exit
```

(admin):

```
sudo kinit
sudo smbclient -k -L ipaserver.ipadomain.ipa
```

Windows AD (PowerShell):

```
Resolve-DnsName -Name _ldap._tcp.ipadomain.ru -Type any
Resolve-DnsName -Name _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.
ipadomain.ru -Type any
```

(login- sudo) .

, .. Active Directory, :

- FreeIPA Active Directory, AD;
- AD FreeIPA;
- AD FreeIPA.

(-) FreeIPA , sudo (. samba):

```
ipa trust-add --type=ad <__Windows_AD> --admin <__Windows_AD>
```

Windows AD.

:

```
ipa trust-fetch-domains <__Windows_AD>
```

, :


```
ipa trustdomain-find <__Windows_AD>
```

- :

```
ipa group-add --desc='ad domain external map' ad_admins_external --
external
ipa group-add --desc='ad domain users' ad_admins
```

```
ipa group-add-member ad_admins_external --external 'windomain.ad\Domain
Admins'
( «member_user» «member_group» «»)
ipa group-add-member ad_admins --groups ad_admins_external
```

• :

 ipa group-add --desc='ad domain external map' ad_admins_external --external
ipa group-add --desc='ad domain users' ad_admins
ipa group-add-member ad_admins_external --external 'windomain.ad\
(«member_user» «member_group» «»)
ipa group-add-member ad_admins --groups ad_admins_external

AD

AD CMD (PowerShell!):

```
c:\> wmic useraccount get name,sid
```

IPA:

```
ipa group-show ad_admins_external --raw
```

/share_dir, AD «share_name»:

```
sudo mkdir /share_dir
sudo net conf setparm 'share_name' 'comment' 'Trust test share'
sudo net conf setparm 'share_name' 'read only' 'no'
sudo net conf setparm 'share_name' 'valid users' "@ad_admins"
sudo net conf setparm 'share_name' 'path' '/share_dir'
```

, , :

```
smbclient -k -L ipaserver.ipadomain.ipa
```

, AD winserver.

AD

AD FreeIPA, , AD.

, <_AD>@<_>, , winuser@windomain.ad.

, Windows , Windows , , AD . , , /etc/krb5.conf [realms] :

 [realms]
IPADOMAIN.IPA = {
.....

auth_to_local = RULE:[1:\$1@\$0](^.*@WINDOMAIN.AD\$s)/@WINDOMAIN.AD/@windomain.ad/
auth_to_local = DEFAULT

.....
}

<_AD>@<_AD>, <_AD> , , :winuser@WINDOMAIN.AD.