NFS Kerberos FreeIPA

-
-
- Kerberos
  - Kerberos

. :

- NFSv2 NFSv3
- FreeIPA

:

- Astra Linux Special Edition .10015-01 (1.7), .10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

" , CIFS, (..) ;"

" . 1 .10015-01 97 01-1" . 17.3. " "

Kerberos NFS :

- - ;
- - ;

, NFS . , , , , .

NFSv4. , Kerberos.

NFS (NFSv3 NFSv4) / (SYS Kerberos), .

- FreeIPA:
  - ipa0.ipadomain0.ru;
  - admin;
  - IP- , DNS;
-
  - host0.ipadomain0.ru;

. NFS

1. nfs-kernel-server:

```
sudo apt install nfs-kernel-server
```

2. , Kerberos:

```
sudo sed -i 's/^[[:space:]]*NEED_SVCGSSD[[:space:]]*=.*/NEED_SVCGSSD="
yes"/' /etc/default/nfs-kernel-server

sudo sed -i 's/^[[:space:]]*NEED_GSSD[[:space:]]*=.*/NEED_GSSD=yes/'
/etc/default/nfs-common
sudo sed -i 's/^[[:space:]]*NEED_IDMAPD[[:space:]]*=.*/NEED_IDMAPD=yes
/' /etc/default/nfs-common
```

3. nfs/<_> , :

   a. Kerberos :

```
kinit admin
```

   b. :

```
ipa service-add nfs/`hostname`
```

   c. Kerberos :

```
sudo kinit admin
```

> Kerberos , ( ).

   d. :

```
sudo ipa-getkeytab -s ipa0.ipadomain0.ru -p nfs/`hostname` -k /etc
/krb5.keytab
```

4. :

   a. , allow_weak_crypto = true [libdefaults] /etc/krb5.conf;

   b. ( ):

```
ldapmodify -x -D "cn=directory manager" -W -h ipa0.ipadomain0.ru
<< EOT
dn: cn=IPADOMAIN0.RU,cn=kerberos,dc=ipadomain0,dc=ru
changetype: modify
add: krbSupportedEncSaltTypes
krbSupportedEncSaltTypes: des-cbc-crc:normal
EOT
ldapmodify -x -D "cn=directory manager" -W -h ipa0.ipadomain0.ru
<< EOT
dn: cn=IPADOMAIN0.RU,cn=kerberos,dc=ipadomain0,dc=ru
add: krbSupportedEncSaltTypes
krbSupportedEncSaltTypes: des-cbc-crc:special
EOT
ldapmodify -x -D "cn=directory manager" -W -h ipa0.ipadomain0.ru
<< EOT
dn: cn=IPADOMAIN0.RU,cn=kerberos,dc=ipadomain0,dc=ru
add: krbDefaultEncSaltTypes
krbDefaultEncSaltTypes: des-cbc-crc:special
EOT
```

5. :

```
sudo systemctl daemon-reload
sudo systemctl restart nfs-kernel-server
```

6. () . /export:

```
sudo mkdir /export
sudo chmod 777 /export
```

/etc/exports. . man exports.

> NFSv4 . , . fsid=0. , , , .

(/home /export):

```
/ *(rw,fsid=0,no_subtree_check,sec=krb5:krb5i:krb5p)
/home gss/krb5i(rw,sync,no_subtree_check)
/export *(rw,sync,no_subtree_check,no_root_squash,sec=krb5:krb5i:krb5p)
```

- , "" NFSv4 Kerberos.
(root_squash). , , nobody:nogroup Kerberos- (. Kerberos). .

> , "" , .
> , "" Kerberos, .
> no_root_squash , . . Kerberos.

7. :

```
sudo exportfs -ra
```

8. , :

```
sudo showmount -e `hostname`
```

```
Export list for ipa0.ipadomain0.ru:
/home gss/krb5i
/export *
/ *
```

Kerberos

. FreeIPA

1. , :

```
sudo mkdir /mnt/nfs_mount
```

2. nfs-common:

```
sudo apt install nfs-common
```

3. :

```
sudo showmount -e ipa0.ipadomain0.ru
```

4. , Kerberos:

```
sudo sed -i 's/^[[:space:]]*NEED_GSSD[[:space:]]*=.*/NEED_SVCGSSD="yes"
/' /etc/default/nfs-common
sudo sed -i 's/^[[:space:]]*NEED_IDMAPD[[:space:]]*=.*/NEED_IDMAPD="yes"
/' /etc/default/nfs-common
```

5. ;
6. NFS- :
    a. NFS- :

```
kinit admin
ipa service-add nfs/`hostname`
```

    b. NFS- :

```
sudo kinit admin
sudo ipa-getkeytab -s ipa0.ipadomain0.ru -p nfs/`hostname` -k /etc
/krb5.keytab
```

7. Kerberos:

> NFSv4

:

```
sudo mount.nfs4 ipa0.ipadomain0.ru:/home/ /mnt/nfs_mount -o sec=krb5i
```

-v .

, :

a. , (vers=4.2), - , (sec=krb5i). :

```
mount -t nfs4
```

```
ipa0.ipadomain0.ru:/export on /mnt/nfs_mount type nfs4 (rw,
relatime,vers=4.2,rsize=524288,wsize=524288,namlen=255,hard,
proto=tcp,timeo=600,retrans=2,sec=krb5i,clientaddr=10.0.2.5,
local_lock=none,addr=10.0.2.100,user=admin)
```

- , , , , (mount).

b. , . NFSv4 Kerberos. , ( ) , ( ) .

```
'/mnt':
```

, , , . Kerberos, nobody:nogroup (Kerberos - . " Kerberos ").

NFSv4:

```
ls -l /
```

```
ls:     '/mnt/nfs_mount':
 96
drwxr-xr-x 2 root root 4096  11 11:54 bin
drwxr-xr-x 3 root root 4096  4 15:42 boot
drwxr-xr-x 18 root root 3940  1 14:35 dev
drwxr-xr-x 127 root root 12288  1 14:35 etc
d????????? ? ? ? ? ? export
...
```

8. . FreeIPA.

Kerberos

Kerberos , (, ,).

1. /etc/default/nfs-common - :

```
GSSDARGS="-n"
```

2. /usr/lib/systemd/scripts/nfs-utils_env.sh - :

```
echo GSSDARGS=\"$GSSDARGS\"
```

3. :

```
sudo systemctl restart nfs-utils
```

(sudo), , - nobody:nogroup.