FreeIPA FreeIPA

-
- DNS
  -
- sssd
  -
- Kerberos-
  -
- SSSD
  -
-

:

- 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

, :

- , ;
- Astra Linux Special Edition , , ;

:

- ipa0.ipadomain0.ru IP- 100.0.2.100. "" ;
  - host0.ipadomain0.ru "" ipadomain0.ru. "" hostx.ipadomain1.ru;
- ipa0.ipadomain1.ru IP- 100.0.2.110. "" ;
  - host0.ipadomain1.ru "" ipadomain1.ru. . , , , ;

- , (host0), . , , . , .

:

- dnsutils sssd-tools (DNS) SSSD:

```
sudo apt install dnsutils sssd-tools
```

- ssh, :

```
sudo apt install ssh
sudo systemctl enable --now ssh
```

DNS

"" IP- "" .

, DNS "" .

"" .

WEB- FreeIPA:

- " " - "DNS" - " DNS" - "";
- "" _ (ipadomain1.ru.) ;
- " " IP- "" (- 10.0.2.110).

"" ( ):

```
kinit admin
ipa dnsforwardzone-add ipadomain1.ru --forward-
policy=first --forwarder=10.0.2.110
```

, , "" IP- "" , , , host:

```
host ipa0.ipadomain1.ru
```

(dnsutils) dig:

```
dig ipadomain1.ru
dig ipa0.ipadomain1.ru
dig SRV _ldap._tcp.ipadomain1.ru
dig SRV _kerberos._tcp.ipadomain1.ru
```

sssd

SSSD "" SSSD "" .

, "" /etc/ipa/ca.crt. /etc/ipa/ca-other.crt.
"" ssh :

```
sudo scp -q admin@ipa0.ipadomain1.ru:/etc/ipa/ca.crt
/etc/ipa/ca-other.crt
```

sssd (/etc/sssd/sssd.conf) , "" (ipa_hostname "" . host0 hostx).

sssd, "" , "" , "ipa_server_mode = True" "_srv_".

[sssd] "" .

, :

```
[domain/ipadomain0.ru]
    cache_credentials = True
    krb5_store_password_if_offline = True
    ipa_domain = ipadomain0.ru
    id_provider = ipa
    auth_provider = ipa
    access_provider = ipa
    ipa_hostname = _srv_, host0.ipadomain0.ru
    chpass_provider = ipa
    ipa_server = ipa0.ipadomain0.ru
    default_shell = /bin/bash
    ldap_tls_cacert = /etc/ipa/ca.crt

[domain/ipadomain1.ru]
    cache_credentials = True
    krb5_store_password_if_offline = True
    ipa_domain = ipadomain1.ru
    id_provider = ipa
    auth_provider = ipa
    access_provider = ipa
    ipa_hostname = hostx.ipadomain1.ru
    chpass_provider = ipa
    ipa_server = _srv_, ipa0.ipadomain1.ru
    default_shell = /bin/bash
    # ipa_server_mode = True #
    ldap_tls_cacert = /etc/ipa/ca-other.crt
```

```
[sssd]
services = sudo, nss, ifp, pam, ssh
domains = ipadomain0.ru, ipadomain1.ru

[nss]
memcache_timeout = 600
homedir_substring = /home

[pam]

[sudo]

[autofs]

[ssh]

[pac]

[ifp]
allowed_uids = 0, 33, 114, 999

[secrets]

[session_recording]
```

sssd:

```
sudo systemctl restart sssd
```

, sssd :

```
sudo systemctl status sssd
```

```
 sssd.service - System Security Services Daemon
Loaded: loaded (/lib/systemd/system/sssd.service;
enabled; vendor preset: enabled)
Active: active (running) since Thu 2020-02-06 13:45:
07 MSK; 14min ago
Main PID: 5601 (sssd)
Tasks: 9 (limit: 4915)
CGroup: /system.slice/sssd.service
5601 /usr/sbin/sssd -i --logger=files
5603 /usr/lib/x86_64-linux-gnu/sssd/sssd_be --domain
ipadomain0.ru --uid 0 --gid 0 --logger=files
5604 /usr/lib/x86_64-linux-gnu/sssd/sssd_be --domain
ipadomain1.ru --uid 0 --gid 0 --logger=files
5605 /usr/lib/x86_64-linux-gnu/sssd/sssd_sudo --uid
0 --gid 0 --logger=files
5606 /usr/lib/x86_64-linux-gnu/sssd/sssd_nss --uid 0
--gid 0 --logger=files
5607 /usr/lib/x86_64-linux-gnu/sssd/sssd_ifp --uid 0
--gid 0 --logger=files
5608 /usr/lib/x86_64-linux-gnu/sssd/sssd_pam --uid 0
--gid 0 --logger=files
5609 /usr/lib/x86_64-linux-gnu/sssd/sssd_ssh --uid 0
--gid 0 --logger=files
5610 /usr/lib/x86_64-linux-gnu/sssd/sssd_pac --uid 0
--gid 0 --logger=files
```

sssd-tools, sssctl:

```
sudo sssctl domain-list
```

```
ipadomain0.ru
ipadomain1.ru
```

```
sudo sssctl domain-status ipadomain1.ru
```

```
Online status: Offline

Active servers:
IPA: ipa1.ipadomain1.ru

Discovered IPA servers:
- ipa1.ipadomain1.ru
- ipa1.ipadomain1.ru
```

, c "" , "offline". , "" , , .

Kerberos-

Kerberos "" "" , . :

- /var/lib/ipa-client/pki/kdc-ca-bundle.pem
- /var/lib/ipa-client/pki/ca-bundle.pem

:

- /var/lib/ipa-client/pki/kdc-ca-bundle-other.pem
- /var/lib/ipa-client/pki/ca-bundle-other.pem

"" ssh, :

```
sudo scp -q admin@host0.ipadomain1.ru:/var/lib/ipa-
client/pki/kdc-ca-bundle.pem /var/lib/ipa-client/pki
/kdc-ca-bundle-other.pem
sudo scp -q admin@host0.ipadomain1.ru:/var/lib/ipa-
client/pki/ca-bundle.pem /var/lib/ipa-client/pki/ca-
bundle-other.pem
```

, "" Kerberos "", "" :

```
kinit admin@IPADOMAIN1.RU
```

:

```
sudo klist -A
```

```
Ticket cache: KEYRING:persistent:0:krb_ccache_cY1rfoy
Default principal: admin@IPADOMAIN1.RU

Valid starting Expires Service principal
07.02.2020 11:17:51 08.02.2020 11:15:20 ldap/ipa0.
ipadomain1.ru@IPADOMAIN1.RU
```

```
07.02.2020 11:17:51 08.02.2020 11:15:20 ldap/ipa0.
ipadomain1.ru@
07.02.2020 11:16:45 08.02.2020 11:15:20 host/host0.
ipadomain1.ru@IPADOMAIN1.RU
07.02.2020 11:16:45 08.02.2020 11:15:20 host/host0.
ipadomain1.ru@
07.02.2020 11:15:22 08.02.2020 11:15:20 krbtgt
/IPADOMAIN1.RU@IPADOMAIN1.RU

Ticket cache: KEYRING:persistent:0:0
Default principal: admin@IPADOMAIN0.RU

Valid starting Expires Service principal
07.02.2020 11:07:04 08.02.2020 11:07:04 krbtgt
/IPADOMAIN0.RU@IPADOMAIN0.RU
```

SSSD

, "" ,

1. "" . WEB- : "" - "" - "", "" :

```
kinit admin
ipa host-add hostx.ipadomain1.ru --force
```

IP-, IP- (--force).

2. Kerberos "" :

```
sudo kinit admin@IPADOMAIN1.RU
sudo ipa-getkeytab -k /etc/krb5.keytab -s ipa0.
ipadomain1.ru -p host/hostx.ipadomain1.
ru@IPADOMAIN1.RU --cacert=/var/lib/ipa-client
/pki/ca-bundle-other.pem
```

:
-k /etc/krb5.keytab - , ;
-s ipa0.ipadomain1.ru - "" , ;
-p host/hostX.ipadomain1.ru@IPADOMAIN1.RU - , ;
--cacert=/var/lib/ipa-client/pki/ca-bundle-other.pem - "" "" , "" Kerberos.

, Kerberos , sssd, , :

```
sudo systemctl restart sssd
```

WEB- "" , :

```
sudo klist -k /etc/krb5.keytab
```

```
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
----
-----------------------------------------------------
---------------------
```

```
2 host/host0.ipadomain0.ru@IPADOMAIN0.RU
3 host/hostx.ipadomain1.ru@IPADOMAIN1.RU
```

, sssd "Online":

```
sudo sssctl domain-status ipadomain1.ru
```

```
Online status: Online

Active servers:
IPA: ipa0.ipadomain1.ru

Discovered IPA servers:
- ipa0.ipadomain1.ru
- ipa0.ipadomain1.ru
```

, . "" ipadomain0.ru:

```
id ipauser01
```

```
uid=96001(ipauser01) gid=96001(ipauser01) =96001
(ipauser01)
```

"" ipadomain1.ru:

```
id ipauser11
```

```
uid=312001(ipauser11) gid=312001(ipauser11) =312001
(ipauser11)
```

, , "" .

sssd,

debug_level = 0x37F0

"" /etc/sssd/sssd.conf sssd. /var/log/sssd , .

Kerberos kinit :

```
KRB5_TRACE=/dev/stdout kinit -V admin@IPADOMAIN1.RU
```