Astra Linux Special Edition 1.5 Windows AD SSO

Astra Linux Windows. SAMBA, Winbind, Apache Postgresql.

- Astra Linux Windows
  - (root)
  -
  -
  -
  - Apache Postgresql Kerberos

:

- Astra Linux Special Edition .10015-01 (1.5)

, AD ALD .

! samba, AD , /var/cache/samba/* /var/lib/samba/*

Astra Linux Windows

:

:

```
 - dc
 – dev.local
 - Windows Server 2008 R2.
ip - 192.168.1.1
```

-:

```
 – ws3
 - Astra Linux 1.5 SE.   ALD    .       :  ,   Fly,    ,  , .
ip - 192.168.1.3
```

(root)

root:

```
$sudo passwd –u root
```

root:

```
$sudo passwd root
```

root . su root-. root, sudo.

root !

/etc/hosts :

/etc/hosts

```
192.168.1.3        ws3.dev.local ws3
127.0.0.1        localhost
```

127.0.1.1 ws3 .

, /etc/hostname :

/etc/hostname

```
ws3
```

ip-. /etc/network/interfaces :

/etc/network/interfaces

```
auto eth0
iface eth0 inet static
address 192.168.1.3
gateway 192.168.1.1
netmask 255.255.255.0
```

/etc/resolv.conf :

/etc/resolv.conf

```
domain dev.local
search dev.local
nameserver 192.168.1.1
```

:

```
service networking restart
```

:

```
ip a
```

icmp , ws3 :

```
ping dc.dev.local
```

:

```
systemctl stop ntp
ntpdate dc.dev.local
systemctl start ntp
```

samba, winbind, ntp, apache2 postgresql:

```
dpkg -l samba winbind ntp apache2 postgresql
```

( ):

```
apt-get install nscd nslcd libpam-winbind libpam-krb5 libapache2-mod-auth-kerb php5 php5-pgsql php5-sybase php5-ldap libsasl2-modules-ldap libsasl2-modules-gssapi-mit krb5-user
```

:

```
ldconfig
```

/etc/krb5.conf :

```
[libdefaults]
    default_realm = DEV.LOCAL
    krb4_config = /etc/krb.conf
    krb4_realms = /etc/krb.realms
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    v4_instance_resolve = false
    v4_name_convert = {
        host = {
            rcmd = host
            ftp = ftp
        }
        plain = {
            something = something-else
        }
    }
    fcc-mit-ticketflags = true
    [realms]
    DEV.LOCAL = {
        kdc = dc.dev.local
        admin_server = dc.dev.local
        default_domain = dev.local
    }
    [domain_realm]
    .dev.local = DEV.LOCAL
    dev.local = DEV.LOCAL
    [login]
    krb4_convert = true
    krb4_get_tickets = false
```

/etc/samba/smb.conf. - , :

```
[global]
workgroup = DEV
realm = DEV.LOCAL
os level = 0
invalid users = root
load printers = no
show add printer wizard = no
printcap name = /dev/null
disable spoolss = yes
dns proxy = no
security = ads
kerberos method = secrets and keytab
dedicated keytab file = /etc/krb5.keytab
encrypt passwords = true
domain logons = no
socket options = TCP_NODELAY
local master = no
domain master = no
preferred master = no
idmap config * : range = 10000-20000
idmap config * : backend = tdb
template shell = /bin/bash
template homedir = /home/%D/%U
winbind enum groups = yes
winbind enum users = yes
winbind use default domain = yes
winbind offline logon = yes
winbind refresh tickets = yes
```

samba, /var/cache/samba/* /var/lib/samba/*

, samba, :

```
testparm
```

/etc/security/limits.conf. :

/etc/security/limits.conf

```
* - nofile 65536
root - nofile 65536
```

:

```
ulimit -n 65536
```

/etc/nsswitch.conf:

```
passwd: compat winbind
group: compat winbind
shadow: compat
hosts: files dns
networks: files
protocols: db files
services: db files
ethers: db files
rpc: db files
netgroup: nis
```

/etc/pam.d/common-session. :

```
session optional pam_mkhomedir.so skel=/etc/skel/ umask=0077
```

:

```
service samba restart
service winbind restart
service ntp restart
service nscd restart
service nslcd restart
```

Astra Linux windows ( ):

```
net ads join -U Administrator
```

/etc/krb5.keytab. :

```
net ads keytab list
```

/etc/krb5.keytab:

```
chmod 0644 /etc/krb5.keytab
```

:

```
insserv -v /etc/init.d/apache2
insserv -v /etc/init.d/samba
```

Postgresql :

```
chkconfig --list postgresql
```

:

```
reboot
```

:

```
service samba status
service winbind status
service nscd status
```

```
service nslcd status
service apache2 status
service postgresql status
```

, :

```
net ads testjoin
wbinfo –p
wbinfo –t
wbinfo –u
getent passwd | grep DEV
```

Kerberos. tgt :

```
kinit Administrator
klist
kdestroy
```

Apache Postgresql Kerberos

/etc/apache2/sites-available/default. Kerberos:

```
<Directory /var/www/>
    AuthType Kerberos
    KrbServiceName host/ws3.dev.local@DEV.LOCAL
    Krb5Keytab /etc/krb5.keytab
    KrbMethodK5Passwd off
    KrbLocalUserMapping on
    KrbSaveCredentials on
    Require valid-user
</Directory>
```

, KrbServiceName, /etc/krb5.keytab. :

```
net ads keytab list
```

www-data, Apache, macdb :

```
usermod -a -G shadow www-data
setfacl -d -m u:www-data:r /etc/parsec/macdb
setfacl -R -m u:www-data:r /etc/parsec/macdb
setfacl -m u:www-data:rx /etc/parsec/macdb
setfacl -m u:www-data:r /etc/krb5.keytab
```

, -, :

```
pdpl-user -z domain_user
```

Apache:

```
service apache2 restart
```

/etc/postgresql/9.4/main/postgresql.conf.:

```
listen_addresses = '*'
krb_server_keyfile = '/etc/krb5.keytab'
krb_caseins_users = off
```

/etc/postgresql/9.4/main/pg_hba.conf:

```
local all all peer
host all all 192.168.1.0/24 gss
```

postgres, Postgresql, macdb :

```
usermod -a -G shadow postgres
setfacl -d -m u:postgres:r /etc/parsec/macdb
setfacl -R -m u:postgres:r /etc/parsec/macdb
setfacl -m u:postgres:rx /etc/parsec/macdb
setfacl -m u:postgres:r /etc/krb5.keytab
```

Postgresql:

```
service postgresql restart
```

dc ws3, :

```
setspn -A postgres/ws3.dev.local ws3
```

root , :

```
usermod –e 1 root
```