Samba AD

Astra: . Astra Linux Samba AD Windows AD

:

- Astra Linux Special Edition .10015-01 (1.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

Samba AD DC "provisioning", "".

(Astra Linux Special Edition -) . smbd , winbind,nmbd, krb5-kdc samba-ad-dc. , , . .

wiki.samba.org

Samba, 4.0, (domain controller, DC) Active Directory (AD).

Samba DC AD
DC .

, Samba DC , AD. Samba NT4 Samba AD.

Samba AD, DC

- fly-admin-ad-server . Astra Linux Samba AD Windows AD.
- . Samba DC Active Directory.

Samba AD DC :

- LDAP AD. . Samba AD DC OpenLDAP LDAP;
- Kerberos Key Distribution Center (KDC). MIT KDC Heimdal KDC;
  Astra Linux Samba MIT KDC, ;
- DNS;
- DNS (DNS BIND9).

- AD DC. , PDC BDC, NT4 . AD, ;
- DNS- AD. (realm) Kerberos AD ;

> AD DNS-, . Samba DNS AD Kerberos.

(FQDN), dc2.samdom.example.com:

```
sudo hostnamectl set-hostname dc2.samdom.example.com
```

- . . AD;
- (, resolvconf), DNS /etc/resolv.conf.
AD DC DNS, DNS AD . DNS, /etc/resolv.conf :

> search samdom.example.com
> nameserver 10.0.2.254

- , /etc/hosts DC (fully-qualified domain name, FQDN) DC IP- DC. :

> 127.0.0.1 localhost.localdomain localhost
> 10.0.2.254 DC.samdom.example.com DC

IP- 127.0.0.1 IP-, DC. :

```
host `hostname`
```

Samba ()

Samba ():

- , Samba :

```
ps ax | egrep "samba|smbd|nmbd|winbindd|rkb5-kdc"
```

  - samba, smbd, nmbd, winbindd, :

```
sudo systemctl stop smbd nmbd winbind krb5-kdc
sudo systemctl mask smbd nmbd winbind krb5-kdc
```

```
:

  • (apt install winbind) winbind 'd';
  • (ps fax | grep winbindd) winbindd 'dd';
  • (sytemsctl status winbind) winbind 'd';
```

- Samba smb.conf file. :

```
sudo smbd -b | grep "CONFIGFILE"
```

```
CONFIGFILE: /usr/local/samba/etc/samba/smb.conf
```

- Samba (*.tdb *.ldb). :

```
sudo smbd -b | egrep "LOCKDIR|STATEDIR|CACHEDIR|PRIVATE_DIR"
```

```
LOCKDIR: /usr/local/samba/var/lock/
STATEDIR: /usr/local/samba/var/locks/
CACHEDIR: /usr/local/samba/var/cache/
PRIVATE_DIR: /usr/local/samba/private/
```

, , Samba DC.

- Kerberos /etc/krb5.conf file, :

```
sudo rm /etc/krb5.conf
```

Samba

samba Astra Linux, synaptic,

```
sudo apt install samba
```

samba smbd " ".

samba . samba AD samba :

```
sudo apt install samba winbind libpam-winbind libnss-winbind libpam-krb5
krb5-config krb5-user krb5-kdc bind9
```

- bind9 - DNS.

Samba AD DC

, , Samba:

```
sudo systemctl stop winbind smbd nmbd krb5-kdc
sudo systemctl mask winbind smbd nmbd krb5-kdc
sudo rm /etc/samba/smb.conf
```

samba-tool domain provision. . .:

```
samba-tool domain provision --help
```

AD NIS (NIS extensions), samba-tool domain provision --use-rfc2307.
AD Unix:

- (UID);
- ;
- .

NIS , AD.

. :

- RFC2307 AD
- idmap config = ad

:

--use-rfc2307	--use-rfc2307	NIS
Realm	--realm	Kerberos. , DNS AD . : samdom.example.com.
Domain	--domain	NetBIOS. DNS AD. , samdom.example.com samdom.
Server Role	--server-role	DC.
DNS backend	--dns-backend	DNS. DC AD - DNS. NONE BIND9_FLATFILE .
DNS forwarder IP address		DNS SAMBA_INTERNAL DNS. . DNS.
Administrator password	--adminpass	. , . . Microsoft TechNet: .

, samba-tool domain provision:

--option="interfaces=lo eth0" --option="bind interfaces only=yes": , Samba . samba-tool .

- NONE DNS, ;
- DNS BiIND, BIND9_FLATFILE, ;
- DC AD DC , (Join) DC.

Samba

:

```
sudo samba-tool domain provision --use-rfc2307 --interactive

#       Samba
sudo systemctl unmask samba-ad-dc
sudo systemctl enable samba-ad-dc
```

```
#     samba   DNS
echo 'include "/var/lib/samba/bind-dns/named.conf";' | sudo tee -a /etc/bind
/named.conf
sudo chown -R root:bind /var/lib/samba/bind-dns
sudo systemctl restart bind9

#    Samba
sudo systemctl start samba-ad-dc
```

:

```
#    Kerberos
Realm [SAMDOM.EXAMPLE.COM]: SAMDOM.EXAMPLE.COM

#
Domain [SAMDOM]: SAMDOM

#
Server Role (dc, member, standalone) [dc]: dc

#   DNS
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: BIND9_DLZ

#  IP-    DNS
DNS forwarder IP address (write 'none' to disable forwarding) [10.0.2.254]: 8.8.8.8

#
Administrator password: Passw0rd
Retype password: Passw0rd

Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=samdom,DC=example,DC=com
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=samdom,DC=example,DC=com
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role: active directory domain controller
Hostname: DC
NetBIOS Domain: SAMDOM
DNS Domain: samdom.example.com
DOMAIN SID: S-1-5-21-2614513918-2685075268-614796884
```

samba-tool domain provision, , .

Samba

Samba :

- : dc
- NIS:
- DNS: DNS BIND9_DLZ
- Kerberos DNS AD: samdom.example.com
- NetBIOS: SAMDOM
- : Passw0rd
- 10.0.2.0/24
- Samba 10.0.2.254

:

```
sudo samba-tool domain provision --server-role=dc --use-rfc2307 --dns-backend=BIND9_DLZ --realm=SAMDOM.EXAMPLE.COM --domain=SAMDOM --adminpass=Passw0rd
```

:

```
#      :
sudo systemctl unmask samba-ad-dc
sudo systemctl enable samba-ad-dc

#     samba   DNS
echo 'include "/var/lib/samba/bind-dns/named.conf";' | sudo tee -a /etc/bind/named.conf
sudo chown -R root:bind /var/lib/samba/bind-dns
sudo systemctl restart bind9

#      Kerberos
sudo cp -b /var/lib/samba/private/krb5.conf /etc/krb5.conf

#    Samba
sudo systemctl start samba-ad-dc
```

Samba AD. , AD , , , , .

samba-tool dns zonecreate :

```
samba-tool dns zonecreate samdom.example.com 2.0.10.in-addr.arpa -U Administrator
---------------------------------------------------------------------------
Password for [administrator@SAMDOM.EXAMPLE.COM]:
Zone 2.0.10.in-addr.arpa created successfully
```

, .
Samba BIND.

Kerberos . . Astra Linux.

DNS

AD DNS , , , LDAP Kerberos. DNS, DNS AD.

DHCP, , . DHCP

DHCP, - /etc/resolv.conf.
:

- DNS AD (search),
- IP- DC nameserver.

:

```
search samdom.example.com
nameserver 10.0.2.254
```

DNS , , IP- .

, IP- DHCP, DNS . . DNS FreeIPA;

, , :

1. DHCP ;
2. . . DNS.

Kerberos

AD, Kerberos , , .

Kerberos . Kerberos

Samba /var/lib/samba/private/krb5.conf Kerberos, DC.

Kerberos , .

Kerberos Kerberos (KDC) (SRV). , , , , (. DNS- BIND9).

netlogon sysvol, DC. , DC:

```
smbclient -L localhost -U%
```

```
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]

Sharename Type Comment
--------- ---- -------
netlogon Disk
sysvol Disk
IPC$ IPC IPC Service (Samba x.y.z)
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]

Server Comment
--------- -------

Workgroup Master
--------- -------
```

, netlogon :

```
smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

```
Enter Administrator's password:
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]
. D 0 Tue Nov 1 08:40:00 2016
.. D 0 Tue Nov 1 08:40:00 2016

49386 blocks of size 524288. 42093 blocks available
```

, .

Samba AD DC Samba samba-tool.

:

dbcheck	AD
delegation	
dns	DNS
domain	
drs	(Directory Replication Services, DRS)
dsacl	DS
fsmo	(Flexible Single Master Operations, FSMO)
gpo	
group	
ldapcmp	ldap
ntacl	ACL
processes	(setproctitle).
rodc	(Read-Only Domain Controller, RODC)
sites	
spn	(Service Principal Name, SPN)
testparm	
time	
user	
visualize	Samba

man:

```
man samba-tool
```

```
samba-tool -h
```

wbinfo

samba winbindd.

wbinfo,
AD.

:

wbinfo -u	
wbinfo -g	
wbinfo -i _	
wbinfo -? wbinfo --help	

-

, AD Linux-.
Linux- Active Directory Samba AD DC .

Samba AD DC

Samba /etc/samba/smb.conf winbind ( ):

```
[global]
    netbios name = DHCP
    realm = SAMDOM.EXAMPLE.COM
    server role = active directory domain controller
    server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate
    workgroup = SAMDOM
    idmap_ldb:use rfc2307 = yes

    template shell = /bin/bash
    winbind use default domain = true
    winbind offline logon = false
    winbind nss info = rfc2307

    winbind enum users = yes
    winbind enum groups = yes
```

```
testparm
```

samba.

:

```
pam-auth-update
```

, PAM.
- winbind, "".
"Tab", "", .

/etc/nsswitch.conf winbind password group:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

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
```

AD
/etc/pam.d/common-password `password [success=1 default=ignore]  pam_winbind.so use_authtok try_first_passfile`
`use_authtok` statement:

password [success=1 default=ignore] pam_winbind.so ~~use_authtok~~ try_first_pass

:

, Samba AD DC , , Samba DC :

- , , , DC, , ;
- DC ;
- , , Samba, , , ;
- DC . DC . , AD DC , , , 20 , ;
- mandatory smb signing is enforced on the DC.

Samba DC , DC VM, .

Samba DC , , (virtual file system, VFS) access (control lists, ACL) Windows.
ACL POSIX Samba DC , .

Samba, Samba.

.:

- Samba
- Samba

(,), Samba, DC , Winbindd .
.: Configuring Winbindd on a Samba AD DC.

.: Samba AD DC

.