Samba 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

:

- (Astra Linux Special Edition -);
- , .

wiki.samba.org

Active Directory (AD) (). , , .
Samba . , (AD) . Samba AD.

NT4 (Primary Domain Controller, PDC) , , (Backup Domain Controllers, BDC).
AD , FSMO, , AD, , " " .

, - Windows AD DC 10.0.2.10 dc1.samdom.example.com

Kerberos . . .

Astra Linux:

- IP- (, 10.0.2.250);
- DNS IP- DNS (.., , 10.0.2.10). /etc/resolv.conf :

  search samdom.example.com
  nameserver 10.0.2.10

- , dc2.samdom.example.com:

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

- /etc/hosts IP- , , :

  10.0.2.253 dc2.samdom.example.com dc2

- Windows AD DNS Astra Linux IP- Astra Linux (. Windows AD). . Samba AD;
- dnsutils, dig DNS:

```
sudo apt install dnsutils
```

, DNS-, , ;

DNS host, IP- :

```
host -t A dc2.samdom.example.com
```

```
dc2.samdom.example.com has address 10.0.2.253
```

DNS

, (DC) DNS AD. DC, DNS.
DNS, :

DNS . BIND9 DNS- Samba AD.

'nameserver' '/etc/resolv.conf' Windows AD DC, , DC Kerberos KDC

AD DC

Samba Windows . Joining a Windows DC to a Samba domain.

Astra Linux (-) Windows AD.

Samba . . Samba AD. , :

- ;
- samba;
- Windows AD.

. . .

(knowledge consistency checker, KCC) Samba DC DC AD. 15- .

samdom.example.com (DC), DNS DNS BIND9_DLZ:

1. :

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

2. :

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

3. :

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

4. samba, :

```
sudo rm /etc/samba/smb.conf
```

5. . samba-tool domain join:

--site=SITE	AD DC .
--option="interfaces=lo eth0" --option="bind interfaces only=yes"	, Samba . samba-tool IP- .
--option='idmap_ldb:use rfc2307 = yes'	--use-rfc2307, .

samba-tool domain join . man samba-tool :

```
samba-tool domain join --help
```

:

```
sudo samba-tool domain join samdom.example.com DC -U"SAMDOM\administrato
r" --dns-backend=BIND9_DLZ
```

, :

```
Finding a writeable DC for domain 'samdom.example.com'
Found DC dc1.samdom.example.com
Password for [SAMDOM\administrator]:
workgroup is SAMDOMsudo ap
realm is samdom.example.com
Adding CN=DC2,OU=Domain Controllers,DC=samdom,DC=example,DC=com
Adding CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=samdom,DC=example,DC=com
Adding CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=samdom,DC=example,
DC=com
Adding SPNs to CN=DC2,OU=Domain Controllers,DC=samdom,DC=example,DC=com
Setting account password for DC2$
Enabling account
Calling bare provision
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
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Provision OK for domain DN DC=samdom,DC=example,DC=com
Starting replication
Schema-DN[CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com] objects[402/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com] objects[804/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com] objects[1206/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=samdom,DC=example,DC=com] objects[1550/1550] linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[402/1618] linked_values[0/0]
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[804/1618] linked_values[0/0]
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[1206/1618] linked_values[0/0]
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[1608/1618] linked_values[0/0]
Partition[CN=Configuration,DC=samdom,DC=example,DC=com] objects[1618/1618] linked_values[42/0]
Replicating critical objects from the base DN of the domain
Partition[DC=samdom,DC=example,DC=com] objects[100/100] linked_values[23/0]
Partition[DC=samdom,DC=example,DC=com] objects[386/286] linked_values[23/0]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=samdom,DC=example,DC=com
Partition[DC=DomainDnsZones,DC=samdom,DC=example,DC=com] objects[44/44] linked_values[0/0]
Replicating DC=ForestDnsZones,DC=samdom,DC=example,DC=com
Partition[DC=ForestDnsZones,DC=samdom,DC=example,DC=com] objects[19/19] linked_values[0/0]
Committing SAM database
Sending DsReplicaUpdateRefs for all the replicated partitions
Setting isSynchronized and dsServiceName
```

Setting up secrets database
Joined domain SAMDOM (SID S-1-5-21-469703510-2364959079-1506205053) as a DC

6. :

```
systemctl unmask samba-ad-dc
systemctl enable samba-ad-dc
```

7. DNS (. DNS- BIND9) samba:

```
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
```

8. DNS:

```
sudo systemctl restart bind9
```

9. samba:

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

, : DNS, LDAP, Kerberos.

DNS

:

```
host -t A somedom.example.com
```

```
samdom.example.com has address 10.0.2.250
samdom.example.com has address 10.0.2.10
```

DNS . dig (, dnsutils), dc1.samdom.example.com dc2.samdom.example.com:

> dig samdom.example.com @dc1.samdom.example.com +nocookie
> dig samdom.example.com @dc2.samdom.example.com

NOERROR ANSWER SECTION :

> ...
> ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25455
> ...
> ;; ANSWER SECTION:
> samdom.example.com 600 IN A 10.0.2.250
> samdom.example.com 600 IN A 10.0.2.10
> ...

DNS :

```
dig SRV _ldap._tcp.samdom.example.com @dc1.samdom.example.com +nocookie
dig SRV _ldap._tcp.samdom.example.com @dc2.samdom.example.com
```

NOERROR ANSWER SECTION ADDITIONAL SECTION :

```
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54924
...
;; ANSWER SECTION:
_ldap._tcp.samdom.example.com. 900 IN SRV 0 100 389 dc2.samdom.example.com.
_ldap._tcp.samdom.example.com. 600 IN SRV 0 100 389 dc1.samdom.example.com.
;; ADDITIONAL SECTION:
dc2.samdom.example.com. 900 IN A 10.0.2.250
dc1.samdom.example.com. 3600 IN A 10.0.2.10
...
```

, DNS Kerberos:

```
dig SRV _kerberos._tcp.samdom.example.com @dc1.samdom.example.com +nocookie
dig SRV _kerberos._tcp.samdom.example.com @dc2.samdom.example.com
```

NOERROR ANSWER SECTION ADDITIONAL SECTION :

```
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54924
...
;; ANSWER SECTION:
_ldap._tcp.samdom.example.com. 900 IN SRV 0 100 389 dc2.samdom.example.com.
_ldap._tcp.samdom.example.com. 600 IN SRV 0 100 389 dc1.samdom.example.com.
;; ADDITIONAL SECTION:
dc1.samdom.example.com. 3600 IN A 10.0.2.10
dc2.samdom.example.com. 900 IN A 10.0.2.250
...
```

LDAP

LDAP :

```
sudo samba-tool drs showrepl
```

:

```
Default-First-Site-Name\DC2
DSA Options: 0x00000001
DSA object GUID: 303f45ca-3a45-4169-ad71-0903ac3e7ab9
DSA invocationId: 4750cc0a-ba23-4492-a1cd-3c66f5b3b073

==== INBOUND NEIGHBORS ====

CN=Configuration,DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Fri Dec  6 10:27:20 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Fri Dec  6 10:27:20 2019 MSK

DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Fri Dec  6 10:27:20 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Fri Dec  6 10:27:20 2019 MSK

DC=DomainDnsZones,DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Fri Dec  6 10:27:20 2019 MSK was successful
```

```
                0 consecutive failure(s).
                Last success @ Fri Dec  6 10:27:20 2019 MSK

CN=Schema,CN=Configuration,DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Fri Dec  6 10:27:20 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Fri Dec  6 10:27:20 2019 MSK

DC=ForestDnsZones,DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Fri Dec  6 10:27:20 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Fri Dec  6 10:27:20 2019 MSK

==== OUTBOUND NEIGHBORS ====

CN=Configuration,DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Fri Dec  6 08:27:31 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Fri Dec  6 08:27:31 2019 MSK

DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Thu Dec  5 17:24:10 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Thu Dec  5 17:24:10 2019 MSK

DC=DomainDnsZones,DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Thu Dec  5 17:24:10 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Thu Dec  5 17:24:10 2019 MSK

CN=Schema,CN=Configuration,DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Thu Dec  5 17:24:10 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Thu Dec  5 17:24:10 2019 MSK

DC=ForestDnsZones,DC=samdom,DC=example,dc=com
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: ce07ab44-222f-4882-b4f5-ed382f6b2047
                Last attempt @ Thu Dec  5 17:24:10 2019 MSK was successful
                0 consecutive failure(s).
                Last success @ Thu Dec  5 17:24:10 2019 MSK

==== KCC CONNECTION OBJECTS ====

Connection --
        Connection name: 49744c99-ca35-4811-af8f-73119e8b31f5
        Enabled        : TRUE
        Server DNS name : DC1.windomain.le
        Server DN name  : CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,
CN=Configuration,DC=samdom,DC=example,dc=com
                TransportType: RPC
                options: 0x00000001
Warning: No NC replicated for Connection!
```

:

Warning: No NC replicated for Connection!

Samba, .

. .

, , , , .

, ldapcmp, . . samba-tool ldapcmp.

Kerberos

Kerberos Kerberos, Windows AD (administrator):

```
kinit administrator
```

klist:

```
klist
```

. Samba AD

Sysvol Samba . DC .

, Samba DC 'xidNumber' 'idmap.ldb'.
, 'idmap.ldb' , DC .
, , :

- /var/lib/samba/private/idmap.ldb DC :

```
tdbbackup -s .bak /var/lib/samba/private/idmap.ldb
```

/var/lib/samba/private/idmap.ldb.bak.

- /var/lib/samba/private/ DC, , .bak, .
- (ACL) Sysvol DC:

```
samba-tool ntacl sysvolreset
```

Winbindd Samba AD DC

. . Winbindd Samba AD DC.

. Samba AD

Sysvol

Samba Sysvol. . Sysvol.

DC Sysvol -, GPO , Sysvol DC, samba-tool ntacl sysvolreset .

. :

- ;
- Samba;
- BIND, BIND9_DLZ

.