

Samba AD DC

•
•
•

wiki.samba.org

• , , (demoting).
• , :

- , ;
- , - ;
- , ,

• , :

- , , FSMO (flexible single master operations):

samba-tool fsmo show

- , , FSMO, DC. . [FSMO](#)
- , , DNS DC, (IP-, objectGUID). , DC2:



ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationId=*)' --cross-ncs objectguid | grep -A1 DC2
dn: CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=samdom,DC=example,DC=com
objectGUID: c14a774f-9732-4ec2-b9fa-2156c95c4e48

• , :

samba-tool domain demote -Uadministrator

• , :

Using DC1.samdom.example.com as partner server for the demotion
Password for [SAMDOM\administrator]:
Deactivating inbound replication
Asking partner server DC1.samdom.example.com to synchronize from us
Changing userControl and container
Removing Sysvol reference: CN=DC2,CN=Enterprise,CN=Microsoft System Volumes,CN=System,CN=Configuration,DC=samdom,DC=example,DC=com
Removing Sysvol reference: CN=DC2,CN=samdom.example.com,CN=Microsoft System Volumes,CN=System,CN=Configuration,DC=samdom,DC=example,DC=com
Removing Sysvol reference: CN=DC2,CN=Domain System Volumes (SYSVOL share),CN=File Replication Service,CN=System,DC=samdom,DC=example,DC=com
Removing Sysvol reference: CN=DC2,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=samdom,DC=example,DC=com
Demote successful

- samba

• , DNS:

- DNS (BIND9_DLZ DNS);
- , DNS.

• , , , ,



' (,) ' 'DC.'

Samba 4.4 .
Samba 4.4.0 . . [Samba](#).

DC:

-
- , Samba 4.4 :

```
samba --version
```

- , FSMO (flexible single master operations):

```
samba-tool fsmo show
```

- , FSMO, . . [FSMO](#).
- ,
- , , DNS DC, (, IP-, objectGUID). , DC2:

```
ldbsearch -H /usr/local/samba/private/sam.ldb '(invocationId=*)' --cross-ncs  
objectguid | grep -A1 DC2
```

```
dn: CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,  
CN=Configuration,DC=samdom,DC=example,DC=com  
objectGUID: c14a774f-9732-4ec2-b9fa-2156c95c4e48
```

, , DC2:

```
samba-tool domain demote --remove-other-dead-server=DC2
```

:

Removing nTDSConnection: CN=04baf417-eb41-4f31-a5f1-c739f0e92b1b,CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=samdom,DC=example,DC=com

Removing nTSDSA: CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=samdom,DC=example,DC=com (and any children)

Removing RID Set: CN=RID Set,CN=DC2,OU=Domain Controllers,DC=samdom,DC=example,DC=com

Removing computer account: CN=DC2,OU=Domain Controllers,DC=samdom,DC=example,DC=com (and any child objects)

Removing Samba-specific DNS service account: CN=dns-DC2,CN=Users,DC=samdom,DC=example,DC=com

updating [samdom.example.com](#) keeping 3 values, removing 1 values

updating DC=_kerberos._tcp.Default-First-Site-Name._sites,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_ldap._tcp.Default-First-Site-Name._sites,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_gc._tcp.Default-First-Site-Name._sites,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_kerberos._tcp,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_kerberos._udp,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_kpasswd._tcp,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_kpasswd._udp,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_ldap._tcp,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_gc._tcp,DC=[samdom.example.com](#),CN=MicrosoftDNS,DC=DomainDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_ldap._tcp.4d5258b9-0cd7-4d78-bdd7-99ebe6b19751.domains,DC=_msdcs.[samdom.example.com](#),CN=MicrosoftDNS,DC=ForestDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_kerberos._tcp.Default-First-Site-Name._sites.dc,DC=_msdcs.[samdom.example.com](#),CN=MicrosoftDNS,DC=ForestDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_ldap._tcp.Default-First-Site-Name._sites.dc,DC=_msdcs.[samdom.example.com](#),CN=MicrosoftDNS,DC=ForestDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_ldap._tcp.Default-First-Site-Name._sites.gc,DC=_msdcs.[samdom.example.com](#),CN=MicrosoftDNS,DC=ForestDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=c14a774f-9732-4ec2-b9fa-2156c95c4e48,DC=_msdcs.[samdom.example.com](#),CN=MicrosoftDNS,DC=ForestDnsZones,DC=samdom,DC=example,DC=com keeping 0 values, removing 1 values

updating DC=_kerberos._tcp.dc,DC=_msdcs.[samdom.example.com](#),CN=MicrosoftDNS,DC=ForestDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_ldap._tcp.dc,DC=_msdcs.[samdom.example.com](#),CN=MicrosoftDNS,DC=ForestDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

updating DC=_ldap._tcp.gc,DC=_msdcs.[samdom.example.com](#),CN=MicrosoftDNS,DC=ForestDnsZones,DC=samdom,DC=example,DC=com keeping 1 values, removing 1 values

Removing Sysvol reference: CN=DC2,CN=Enterprise,CN=Microsoft System Volumes,CN=System,CN=Configuration,DC=samdom,DC=example,DC=com

Removing Sysvol reference: CN=DC2,CN=[samdom.example.com](#),CN=Microsoft System Volumes,CN=System,CN=Configuration,DC=samdom,DC=example,DC=com

Removing Sysvol reference: CN=DC2,CN=Domain System Volumes (SYSVOL share),CN=File Replication Service,CN=System,DC=samdom,DC=example,DC=com

Removing Sysvol reference: CN=DC2,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=samdom,DC=example,DC=com



In case that the demoted DC ran a DNS service for the Active Directory (AD) zones, verify that domain members and DCs do no longer use this host to resolve the AD DNS zones.

, DNS:

- , DNS.