Samba 4 Active Directory Domain Controller on Ubuntu 18.04 Server

6 minute read

This post will outline how to install an Active Directory(AD) Domain Controller on Ubuntu Server 18.04. Yes, that's right...Active Directory on a linux host. Not a backup domain controller but a functional AD that you can create users with, join computers to, and set up group policy.

Network configuration

Hostname	Domain	IP Address
dc1	ad.ricosharp.com	192.168.122.70

Configure networking

Configure system hostname

```
~]$ sudo hostnamectl set-hostname dc1
```

Edit the hosts files so the hostname resolves to its IP address

```
~]$ sudo nano /etc/hosts
# Add this line to /etc/hosts so that dc1 resolves to 192.168.122.70
192.168.122.70  dc1 dc1.ad.ricosharp.com
```

Note that Ubuntu 18.04 is now using netplan to configure IP addresses on systems. I will outline a basic configuration in a future post

Update system and install required packages

Update and reboot the system

```
~]$ sudo apt update -y
~]$ sudo apt upgrade -y
~]$ sudo reboot
```

Install relevant samba, winbind, and kerberos packages. The installation will prompt for kerberos settings and will give an error at the end of installation. Ignore this for now and accept the defaults. This will be configured properly later as part of the AD installation.

```
~]$ sudo apt install samba smbclient winbind libpam-winbind libnss-winbind krb5-kdc libpam-krb5 -
y
```

Rename samba and kerberos files. You need to start from a clean environment when starting the samba AD setup.

```
~]$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
~]$ sudo mv /etc/krb5.conf /etc/krb5.conf.orig
```

Run the samba AD setup

All the default settings are fine. The only change I make is to set the DNS forwarder to 8.8.8.8. You can also use a different DNS backend. But this is out of the scope of this post for a simple setup.

```
~]$ sudo samba-tool domain provision --use-rfc2307 --interactive
Realm [AD.RICOSHARP.COM]:
 Domain [AD]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
 DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.53]: 8.8.8.8
Administrator password:
Retype password:
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=ad,DC=ricosharp,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=ad,DC=ricosharp,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 AD has been generated at
/var/lib/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        AD
DNS Domain:            ad.ricosharp.com
DOMAIN SID:            S-1-5-21-2060062981-3252955935-809771608
```

Copy the provisioned kerberos configuration file to the kerberos configuration file location

```
~]$ sudo cp /var/lib/samba/private/krb5.conf /etc
```

Test the configuration

Samba can now be run. But before setting up with systemd, start samba and run some tests with DNS.

```
~]$ sudo samba
```

Test DNS

```
~]$ host -t SRV _ldap._tcp.ad.ricosharp.com
Host _ldap._tcp.ad.ricosharp.com not found: 3(NXDOMAIN)
~]$ host -t SRV _kerberos._udp.ad.ricosharp.com
Host _kerberos._udp.ad.ricosharp.com not found: 3(NXDOMAIN)
~]$ host -t A dc1.ad.ricosharp.com
dc1.ad.ricosharp.com has address 192.168.122.70
```

This is not good as without DNS, AD will fail to run properly. If we run netstat to see what processes are listening on port 53, we can see that systemd-resolve is running in addition to samba.

```
~]$ sudo netstat -tulpn | grep :53
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      688/systemd-
resolve
tcp6       0      0 :::53                   :::*                    LISTEN      4368/samba
udp        0      0 127.0.0.53:53           0.0.0.0:*                           688/systemd-
resolve
udp6       0      0 :::53                   :::*                                4368/samba
```

A quick and dirty way to make sure that samba is the only process listening to DNS queries is to disable the systemd-resolved service.

```
~]$ sudo systemctl stop systemd-resolved
~]$ sudo systemctl disable systemd-resolved
~]$ sudo unlink /etc/resolv.conf
~]$ sudo nano /etc/resolv.conf
nameserver 192.168.122.70
search ad.ricosharp.com
~]$ sudo reboot
```

Test DNS again. It looks like everything is now working.

```
~]$ sudo samba
~]$ host -t SRV _ldap._tcp.ad.ricosharp.com
_ldap._tcp.ad.ricosharp.com has SRV record 0 100 389 dc1.ad.ricosharp.com.
~]$ host -t SRV _kerberos.udp.ad.ricosharp.com
Host _kerberos.udp.ad.ricosharp.com not found: 3(NXDOMAIN)
~]$ host -t A dc1.ad.ricosharp.com
dc1.ad.ricosharp.com has address 192.168.122.70
```

Let's also go ahead and test kerberos authentication. Everything here looks in order.

```
~]$ kinit Administrator
Password for Administrator@AD.RICOSHARP.COM:
Warning: Your password will expire in 41 days on Sat 05 Oct 2019 04:12:28 PM UTC
~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: Administrator@AD.RICOSHARP.COM

Valid starting       Expires              Service principal
08/24/2019 16:42:07  08/25/2019 02:42:07  krbtgt/AD.RICOSHARP.COM@AD.RICOSHARP.COM
        renew until 08/25/2019 16:42:04
```

Configure samba AD to start with systemd

Now that this is running, kill samba again so we can begin the process using systemd

```
~]$ sudo ps -aux | grep samba
root      1134  0.0  2.1 542992 44676 ?        Ss   16:34   0:00 samba
root      1135  0.0  1.2 542992 25568 ?        S    16:34   0:00 samba
root      1136  0.0  1.8 547144 37744 ?        S    16:34   0:00 samba
root      1137  0.0  1.1 542996 22948 ?        S    16:34   0:00 samba
root      1138  0.0  1.4 542992 28740 ?        S    16:34   0:00 samba
root      1140  0.0  1.2 542992 25104 ?        S    16:34   0:00 samba
root      1141  0.5  1.5 542992 32564 ?        S    16:34   0:01 samba
root      1142  0.0  1.2 542992 25708 ?        S    16:34   0:00 samba
root      1143  0.0  1.4 542992 29244 ?        S    16:34   0:00 samba
root      1144  0.0  1.4 542992 28820 ?        S    16:34   0:00 samba
root      1145  0.0  1.2 542992 25568 ?        S    16:34   0:00 samba
root      1146  0.0  1.2 542992 25044 ?        S    16:34   0:00 samba
root      1147  0.0  1.8 542992 38052 ?        S    16:34   0:00 samba
root      1148  0.0  1.3 542992 27584 ?        S    16:34   0:00 samba
root      1149  0.0  1.5 543412 31340 ?        S    16:34   0:00 samba
root      1150  0.0  1.1 542996 22948 ?        S    16:34   0:00 samba
rico      1198  0.0  0.0  13136  1004 pts/0    S+   16:38   0:00 grep --color=auto samba

~]$ sudo kill 1134
~]$ sudo ps -aux | grep samba
rico      1203  0.0  0.0  13136  1152 pts/0    S+   16:38   0:00 grep --color=auto samba
```

Mask the smbd, nmbd, winbind services and unmask the samba-ad-dc service

```
~]$ sudo systemctl mask smbd nmbd winbind
~]$ sudo systemctl disable smbd nmbd winbind
~]$ sudo systemctl stop smbd nmbd winbind
~]$ sudo systemctl unmask samba-ad-dc
~]$ sudo systemctl start samba-ad-dc
~]$ sudo systemctl enable samba-ad-dc
```

Reboot and test

```
~]$ sudo reboot
~]$ sudo systemctl status samba-ad-dc
```

Join a computer to the domain

To join the domain on a Windows 10 computer, do the following:

Note: Make sure that your DNS is pointing to dc1 (192.168.122.70)

1. Go to Start > Settings
2. Click Accounts
3. Access Work or School
4. Click Connect
5. Click Join this device to a local Active Directory domain
6. Type ad.ricosharp.com and enter the Administrator username/password for the domain
7. Select Skip to Add an account
8. Select Restart Now

An alternative way, and the way that I'm most used to is this:

1. Open the File Explorer
2. Right click This PC > Properties
3. Select Change settings under the Computer name, domain, and workgroup settings section
4. Click the Change button
5. Select Domain and enter ad.ricosharp.com
6. Click ok, enter an Administrator username/password for the domain and reboot

Create a user account

There are two ways you can manage user accounts. Firstly, you can use samba-tool. For example, to create a new user called user1, issue the following command:

```
~]$ sudo samba-tool user create user1
```

The second way is to install the Remote System Administration Tools (RSAT) on a Windows 10 computer. You can download the RSAT from here (https://www.microsoft.com/en-us/download/details.aspx?id=45520)

Once installed, open Active Directory Users and Computers from Start > Windows Administrative Tools. Expand the active directory domain name (ad.ricosharp.com) and open the Users organizational unit. Right click and select New > User.

References

Setting up Samba as an Active Directory Domain Controller
(https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller)

Managing the Samba AD DC Service Using Systemd
(https://wiki.samba.org/index.php/Managing_the_Samba_AD_DC_Service_Using_Systemd)

Updated: August 24, 2019