https://linoxide.com/ubuntu-how-to/setup-ubuntu-active-directory-domain-controller-samba/

How to Setup Active Directory Domain Controller on Ubuntu using Samba

October 24, 2016By [Saheetha Shameer](https://linoxide.com/author/saheethas/)Updated October 23, 2016

[**FACEBOOK**](http://www.facebook.com/sharer/sharer.php?u=https://linoxide.com/?p=14711)[**GOOGLE+**](https://plus.google.com/share?url=https://linoxide.com/?p=14711)[**TWITTER**](http://twitter.com/home?status=How+to+Setup+Active+Directory+Domain+Controller+on+Ubuntu+using+Samba:https://linoxide.com/?p=14711)[**PINTEREST**](http://pinterest.com/pin/create/button/?url=https://linoxide.com/?p=14711&media=)[**LINKEDIN**](http://www.linkedin.com/shareArticle?mini=true&url=https://linoxide.com/?p=14711&title=How+to+Setup+Active+Directory+Domain+Controller+on+Ubuntu+using+Samba)[**STUMBLEUPON**](http://www.stumbleupon.com/submit?url=https://linoxide.com/?p=14711&title=How+to+Setup+Active+Directory+Domain+Controller+on+Ubuntu+using+Samba)[**REDDIT**](http://reddit.com/submit?url=https://linoxide.com/?p=14711&title=How+to+Setup+Active+Directory+Domain+Controller+on+Ubuntu+using+Samba)[**EMAIL**](mailto:?subject=How+to+Setup+Active+Directory+Domain+Controller+on+Ubuntu+using+Samba&body=How+to+Setup+Active+Directory+Domain+Controller+on+Ubuntu+using+Samba:https://linoxide.com/?p=14711)

SAMBA is an open source implementation of the SMB file sharing protocol that provides file and print services to SMB / CIFS clients. It helps in successfully networking your Ubuntu system with Windows clients, thereby providing and integrating with services common to Windows environments. These services assist the sharing of data and information about the computers and users involved in the network, and may be classified under three major categories in terms of functionality

**File and Printer Sharing Services:** It uses the Server Message Block (SMB) protocol to facilitate the sharing of files, folders, volumes, and printers throughout the network.

**Directory Services:** It shares vital information about the computers and users of the network with the help of Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory.

**Authentication and Access:** It establishes the identity of a computer or user of the network and determines the information the computer or user is authorized to access using file permissions, group policies, and the Kerberos authentication service.

In this article, I'm explaining on how to setup an Active Directory Domain Controller with Samba on Ubuntu 16.04. Samba as an AD DC requires at least version 4.0.0.  I highly recommend to use the latest stable version of Samba as it will contain bugs fixes from previous releases and a lot of improved Microsoft Active Directory compatibility and additional features.

The major advantage of using this is that, we don't need to install separate Kerberos KDC. Samba includes an AD compatible KDC and its ships its own LDAP implementation for AD back ends.

**Pre-requisites**

* Make sure that your server is configured to use Static IP address. DHCP can cause trouble if the address changes.
* Update your resolv.conf with proper name servers.
* Update your /etc/hosts file with proper entries. Your hostname should resolve to the server IP.

Let's start with the pre-requisites. I'll show you, how I modified my server settings to satisfy our pre-conditions.

**1)** You need to configure your network interface for static IP.  Edit the  /etc/network/interfaces file with your server IP "96.126.107.141", domain controller name "nodenixbox.com" and other details as below:

root@ubuntu:~# cat /etc/network/interfaces  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/\*

# The loopback network interface  
auto lo  
iface lo inet loopback

# The primary network interface  
auto eth0  
**iface eth0 inet static**  
**address 96.126.107.141**  
**netmask 255.255.255.0**  
**network 96.126.107.0**  
**broadcast 96.126.107.255**  
**gateway 96.126.107.1**  
**dns-nameservers 96.126.107.141 8.8.8.8**  
**dns-search nodenixbox.com**

# This is an autoconfigured IPv6 interface  
iface eth0 inet6 auto

I changed iface eth0 inet dhcp to iface eth0 inet static and added these highlighted portions to my network configuration.

**2)** Edit your resolv.conf file to add your domain controller name.

root@ubuntu:~# cat /etc/resolv.conf  
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)  
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN  
nameserver 96.126.107.141  
nameserver 8.8.8.8  
nameserver 207.192.69.4  
search **nodenixbox.com**

**3)** Last but not least edit our /etc/hosts file and set "ubuntu.nodenixbox.com"  as your hostname as below:

root@ubuntu:~# cat /etc/hosts  
127.0.0.1 localhost  
#127.0.1.1 ubuntu.members.linode.com ubuntu  
96.126.107.141 ubuntu.nodenixbox.com ubuntu

# The following lines are desirable for IPv6 capable hosts  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters

root@ubuntu:~# echo ubuntu.nodenixbox.com > /etc/hostname

root@ubuntu:~# /etc/init.d/networking restart  
[ ok ] Restarting networking (via systemctl): networking.service.

Restart your network after these modifications.

So, we are ready to start with the installation of the packages.

**Packages installation**

First of all, we need to install all required packages for setting up our Domain controller Active directory. I run this command to update all my server software packages and install the required softwares.

root@ubuntu:~# apt-get update && apt-get upgrade -y

root@ubuntu:~# apt-get install git attr build-essential libacl1-dev libattr1-dev libblkid-dev libgnutls-dev libreadline-dev python-dev libpam0g-dev python-dnspython gdb pkg-config libpopt-dev libldap2-dev dnsutils libbsd-dev attr krb5-user docbook-xsl libcups2-dev acl ntp ntpdate winbind

During these package installation, you'll be asked for kerberos informations. You need to provide your Kerberos default realm and administrator server information. You can enter your default realm as nodenixbox.com and administrator server name as hostname.

**How to install and configure SAMBA**

You need to download the latest Samba packages using git repositories into the "samba4" folder.

root@ubuntu:~# git clone -b v4-1-stable git://git.samba.org/samba.git samba4  
Cloning into 'samba4'...  
remote: Counting objects: 1276826, done.  
remote: Compressing objects: 100% (280630/280630), done.  
remote: Total 1276826 (delta 992350), reused 1267276 (delta 984263)  
Receiving objects: 100% (1276826/1276826), 249.03 MiB | 10.51 MiB/s, done.  
Resolving deltas: 100% (992350/992350), done.  
Checking connectivity... done.

Once downloaded you can enter into the "samba4" folder and configure your Samba package.

root@ubuntu:~#cd samba4  
root@ubuntu:~#./configure --enable-debug --enable-selftest  
root@ubuntu:~#make  
root@ubuntu:~/samba4# make  
WAF\_MAKE=1 python ./buildtools/bin/waf build  
Waf: Entering directory `/root/samba4/bin'  
Selected embedded Heimdal build  
Waf: Leaving directory `/root/samba4/bin'  
'build' finished successfully (6.288s)  
root@ubuntu:~#make install

The SAMBA compilation may take a while to complete. Once it's done, confirm with the SAMBA and SMB client version. Both these versions should match.

root@ubuntu:~# /usr/local/samba/sbin/samba -V  
Version 4.1.23  
root@ubuntu:~# /usr/local/samba/bin/smbclient -V  
Version 4.1.23

**Provisioning the Samba Active Directory**

Next step is to provision your domain. You can simply run this command to provision your domain.

root@ubuntu:~/samba4# /usr/local/samba/bin/samba-tool domain provision --realm=**nodenixbox.com** --domain=nodenixbox --adminpass="password" --server-role=dc --dns-backend=**SAMBA\_INTERNAL**  
Looking up IPv4 addresses  
Looking up IPv6 addresses  
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=nodenixbox,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=nodenixbox,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  
Once the above files are installed, your Samba4 server will be ready to use  
**Server Role: active directory domain controller**  
**Hostname: ubuntu**  
**NetBIOS Domain: NODENIXBOX**  
**DNS Domain: nodenixbox.com**  
**DOMAIN SID: S-1-5-21-4019752003-3807572232-1148719748**

Some uses Bind9 as backend DNS, but SAMBA contains its own fully functional DNS server. Here, I'm using SAMBA\_INTERNAL. We need to start the SAMBA service after setting this domain. You can run this command to start SAMBA.

root@ubuntu:~# /usr/local/samba/sbin/samba  
root@ubuntu:~#

**Testing your Samba Domain Controller**

We can run "smbclient", to check if Samba provides the AD DC default shares "netlogon" and "sysvol", that were created in your "smb.conf" during provisioning.

root@ubuntu:~# /usr/local/samba/bin/smbclient -L localhost -U%  
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.3.11-Ubuntu]

Sharename Type Comment  
--------- ---- -------  
print$ Disk Printer Drivers  
IPC$ IPC IPC Service (ubuntu server (Samba, Ubuntu))  
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.3.11-Ubuntu]

Server Comment  
--------- -------  
UBUNTU ubuntu server (Samba, Ubuntu)

Workgroup Master  
--------- -------  
WORKGROUP UBUNTU

To test whether the authentication is working, you should try to connect to the "netlogon" share, using the Domain Administrator account that was created during provisioning.

root@ubuntu:~/samba4# /usr/local/samba/bin/smbclient //localhost/netlogon -UAdministrator -c 'ls'  
Enter Administrator's password:  
Domain=[NODENIXBOX] OS=[Unix] Server=[Samba 4.1.23] . D 0 Sun Oct 16 09:30:02 2016  
.. D 0 Sun Oct 16 09:31:09 2016

47431 blocks of size 524288. 40274 blocks available

**Configure SAMBA\_INTERNAL DNS**

A working DNS is essential for the proper operation of an Active Directory. Without the right DNS entries, Kerberos won't work, which in turn means that many of the basic features won't work. It is always worth spending some extra time ensuring your DNS setup to ensure it's properly done.

We need to edit our /etc/resolv.conf with our domain name as below:

root@ubuntu:~#echo domain nodenixbox.com >> /etc/resolv.conf

Your Domain Controller requires a name server that is able to resolve queries to Active Directory zones. Because this is your first Domain Controller in your AD forest.

You also need to edit your samba configuration file  "/usr/local/samba/etc/smb.conf" and add google nameserver to the dns\_forwarder.

root@ubuntu:~# cat /usr/local/samba/etc/smb.conf  
# Global parameters  
[global] workgroup = NODENIXBOX  
realm = NODENIXBOX.COM  
netbios name = UBUNTU  
server role = active directory domain controller  
dns forwarder = 8.8.8.8

**Testing your DNS**

To confirm DNS, is working properly, run the following commands and compare the output

root@ubuntu:~# host -t SRV \_ldap.\_tcp.nodenixbox.com  
\_ldap.\_tcp.nodenixbox.com has SRV record 0 100 389 ubuntu.nodenixbox.com

root@ubuntu:~# host -t SRV \_kerberos.\_udp.nodenixbox.com.  
\_kerberos.\_udp.nodenixbox.com has SRV record 0 100 88 ubuntu.nodenixbox.com.

root@ubuntu:~# host -t A ubuntu.nodenixbox.com  
ubuntu.nodenixbox.com has address 96.126.107.141

**Configure Kerberos**

Kerberos is an important part of Active Directory. Typically the configuration is done in /etc/krb5.conf. During provisioning, a working sample configuration will be created at /usr/local/samba/share/setup/krb5.conf . You can replace your krb5.conf file with the sample by copying or creating a symlink.

root@ubuntu:~# ln -s /usr/local/samba/share/setup/krb5.conf /etc/krb5.conf

You will need to edit this file and modify the default\_realm with your DC name as below:

root@ubuntu:~# cat //etc/krb5.conf  
[libdefaults] default\_realm = NODENIXBOX.COM  
dns\_lookup\_realm = false  
dns\_lookup\_kdc = true

The realm name should be in UPPERCASE.

**Testing Kerberos**

You can use kinit to test your Kerberos configuration.  Run this command as below for testing:

root@ubuntu:~# kinit administrator@NODENIXBOX.COM  
Password for administrator@NODENIXBOX.COM:  
Warning: Your password will expire in 41 days on Sun 27 Nov 2016 09:31:07 AM UTC

You need to disable the password expiry for the active directory administrator user by running this command to avoid future authentication problems.

root@ubuntu:~# /usr/local/samba/bin/samba-tool user setexpiry administrator --noexpiry  
Expiry for user 'administrator' disabled.

Note: You must always specify your realm in uppercase letters. To verify the Kerberos working, you can run this.

root@ubuntu:~# klist -e  
Ticket cache: FILE:/tmp/krb5cc\_0  
Default principal: administrator@NODENIXBOX.COM

Valid starting Expires Service principal  
10/17/2016 04:19:31 10/17/2016 14:19:31 krbtgt/NODENIXBOX.COM@NODENIXBOX.COM  
renew until 10/18/2016 04:19:19, Etype (skey, tkt): arcfour-hmac, arcfour-hmac

**Creating your user home folder**

Now, you can create your user home folders and set proper permissions and ownerships.

root@ubuntu:~# mkdir -m 770 /Users  
root@ubuntu:~# chmod g+s /Users  
root@ubuntu:~# chown root:users /Users

Next, you need to edit your SMB configuration file "/usr/local/samba/etc/smb.conf" as below:

[Users] directory\_mode: parameter = 0700  
read only = no  
path = /Users  
csc policy = documents

**Configure NTP**

Active Directory requires close time synchronization between all participant machines for Kerberos to work properly. It's highly recommended to use NTP on your Domain Controller for time synchronization. This[documentation](https://wiki.samba.org/index.php/Time_Synchronisation)  will provide you with all necessary information, to configure NTP on an AD Domain Controller.

**Conclusion**

Finally, we've created our Active directory Domain controller on an Ubuntu 16.04 server. You can create your own DC Active directory and share  over the network. A major advantage of this configuration is the ability to centralize user and machine credentials. It has several other benefits. Some of the key benefits are as below:

* It maintains a list of users who can access the network in an active directory and determines which files users can access and what they can do with these files.
* In addition to security and convenience, domain controllers provide speed by freeing up individual PC resources from performing server functions which ultimately improves client machine performance.
* It also provides complete security log which is required for System Security and Audit.