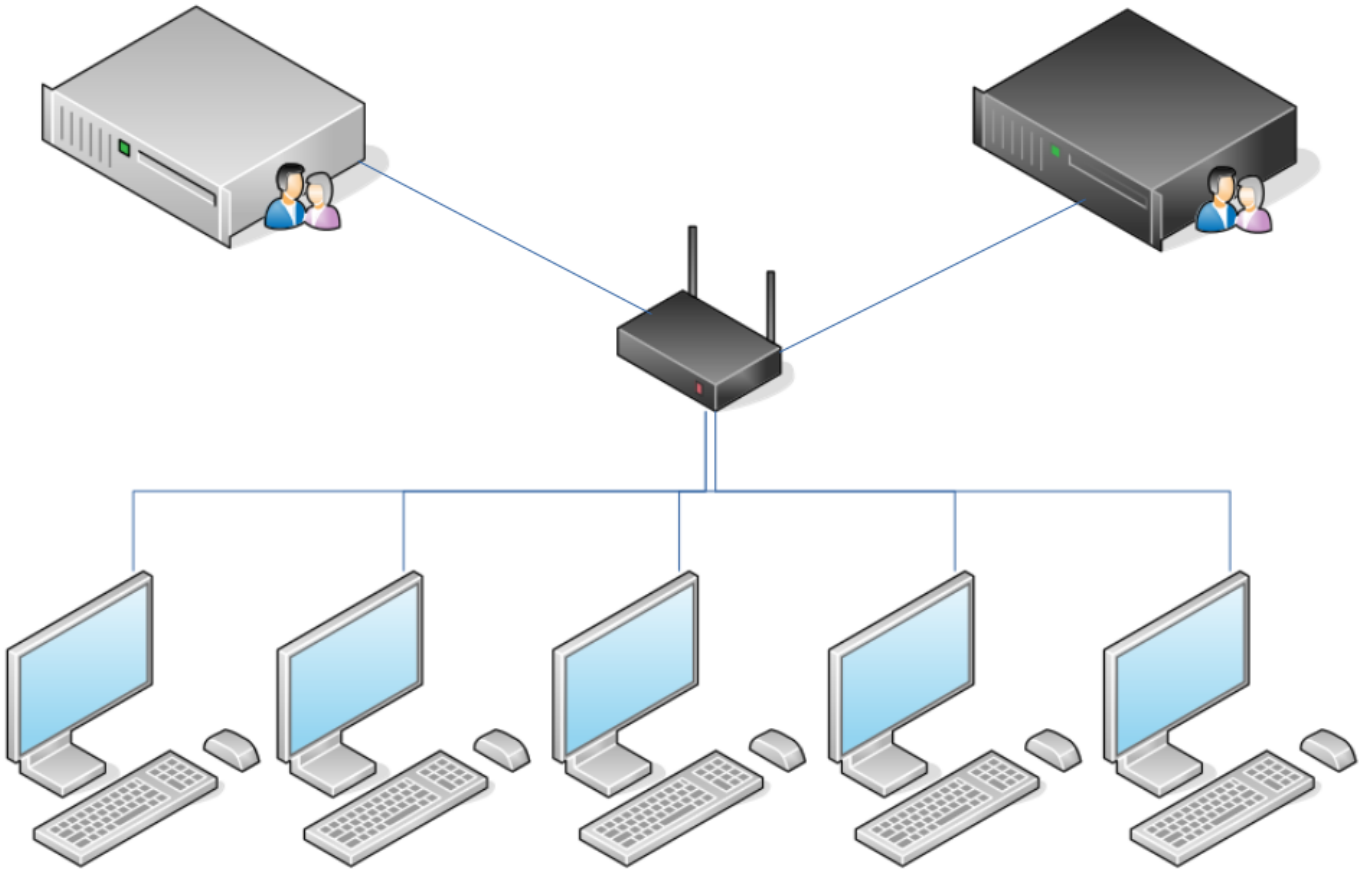
Active Directory Services (Hosting SAMBA on Linux Server)

I've always wanted to do magic. On clicking a button, all computers should display the same wallpaper on reboot. And, Yup! I did it (not in production of-course, Windows Licenses aren't cheap)

I installed Windows (trial) on five test-bed computers and added them to a domain created using Samba and two Domain Controllers. I Implemented group policies, apps to start on boot, theming, Windows Defender Options, Drive Maps, etc., etc. and etc. It was really fun.



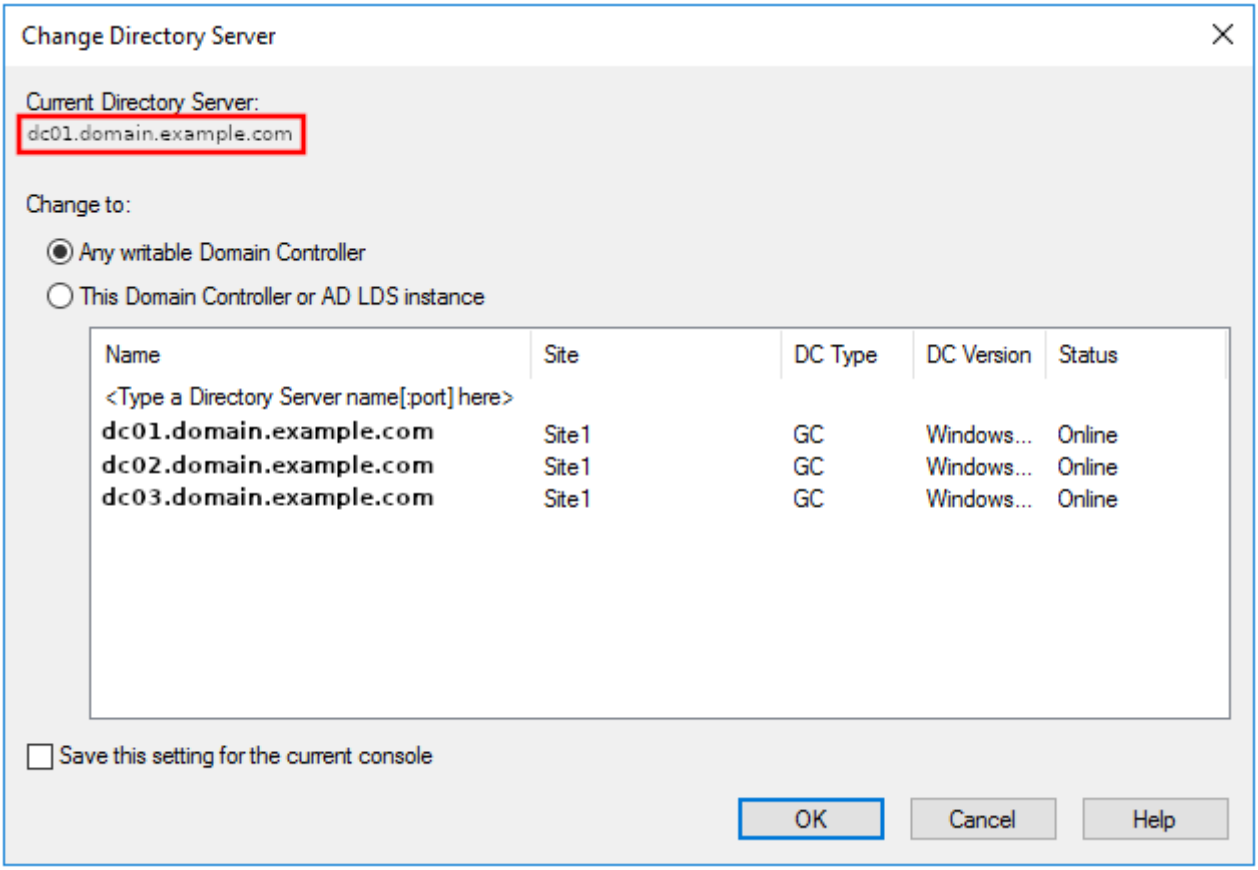
Setting Up the Primary Domain Controller

- I first prepared my Ubuntu Server for installation by following the steps on https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller
- Then, I installed Samba using the distribution specific packages for Ubuntu using `sudo apt-get install acl attr samba samba-dsdb-modules samba-vfs-modules winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user`
- Then, Provision a Domain using `samba-tool domain provision --realm DOMAIN.EXAMPLE.COM --use-rfc2307 --interactive`
- Configure Kerberos by running `cp /usr/local/samba/private/krb5.conf /etc/krb5.conf`

Setting Up a Fail-over Domain Controller

- Prepare your server for Installation (The first two steps of Setting up a Primary DC)
- Configure DNS Resolution properly and make sure the primary domain controller is reachable using its domain name. If you're unable to configure your DNS as needed (as in my case), just add the domain controller and it's IP to `/etc/hosts`
- Just configure the `/etc/krb5.conf` as shown in https://wiki.samba.org/index.php/Joining_a_Samba_DC_to_an_Existing_Active_Directory under the **Kerberos Section** and verify the settings using the `kinit` command. Just continue if verification fails (it happened with me)
- Then, run `sudo samba-tool domain join yourdomain.example.com DC -U"YOURDOMAIN\administrator" --option='idmap_ldb:use rfc2307 = yes'`. I used `--use-rfc2307` while deploying my Primary DC (the Samba guide instructs so)
- When I executed this command, I got issues. On real hard googling, I found out these issues were related to DNS and Samba Internal DNS resolves the primary domain controller to multiple IP Addresses. So I had to delete the incorrect addresses. You can use `samba-tool` or Windows RSAT for that.

Domain Controller Replication



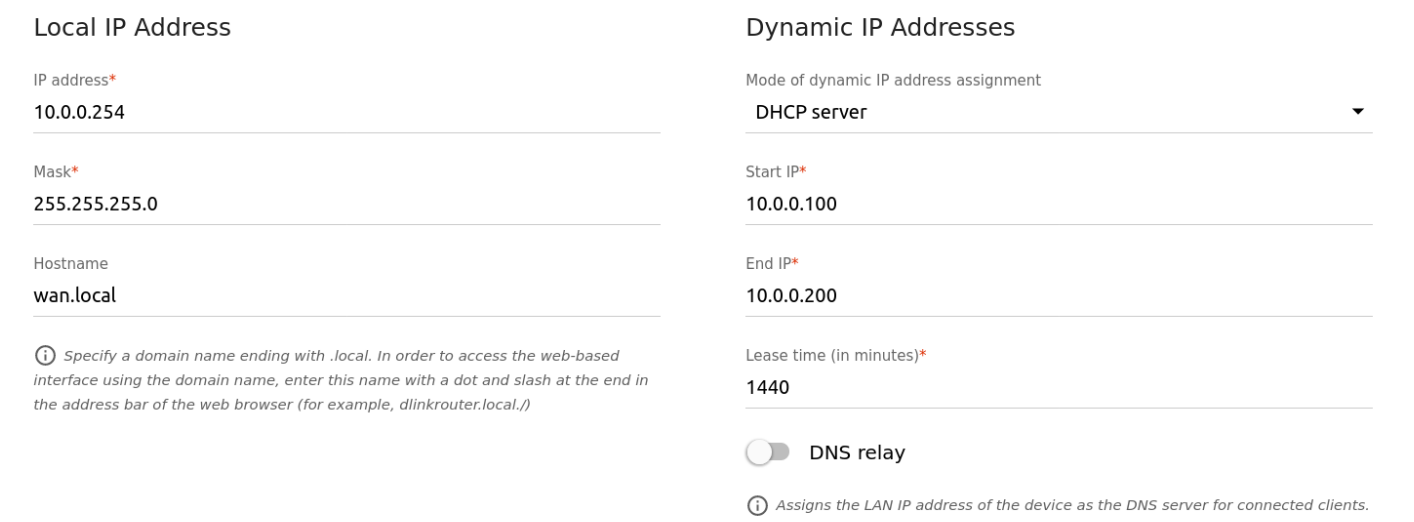
- For Group Policy and Users replication between both DCs, I used Rsync Based Unidirectional Replication
- This type of replication is really easy to setup. But, since it's unidirectional, making changes to Users, Groups or other settings on the Secondary DC will be overwritten by the primary one. So, you can only change the settings on the Primary DC and when the Primary DC is online.
- Also, as stated above, You need to make sure RSAT is writing changes to the Primary DC.

Samba Internal DNS and dnsmasq?

Samba and other DNS Services on the same server just don't get along, until forced. Samba is really really keen in listening on port 389 and others (for AD) and DNS on 53.

As Samba integrates either with Internal DNS or with Bind9, I assigned two IPs to my Server made SAMBA listen on one (assume 10.0.0.31) and dnsmasq (Pi-Hole) on the other (assume 10.0.0.51). Both at port 53.

As mentioned in this post, I have three DNS Servers, One of them is this and the other is the secondary domain controller and the third is the Primary DNS Server which is bare-metal. Then, I setup all devices to use the Samba DNS Endpoints (on both DCs) and the Primary DNS Server by adding **DHCP Options on the DHCP Server, which is my primary router**.



DHCP Options

Options	Options value	Force
15 Domain Name	atheesh.org	Yes
6 Domain Server	10.0.0.51,10.0.0.52,10.0.0.53	Yes
119 Domain Search	[illegible]	Yes

Now, Samba DNS Endpoints resolve all AD Domain computers but neither my internal domains nor Google, YouTube, etc. To Fix this (remember I had deployed the dnsmasq instance on the same server with another IP - 10.0.0.51) I configured Samba to use 10.0.0.51 as the DNS by using the `dns forwarder = 10.0.0.51` directive. It works.

> You can assign multiple IPs to an Interface on Ubuntu 18.04 and above by editing the netplan configuration at /etc/netplan/00-installer-config.yml

`/etc/samba/smb.conf`	`/etc/dnsmasq.d/99-bind-interface.conf`

```
# Global parameters
[global]
	dns forwarder = 10.0.0.51
    	interfaces = 10.0.0.31
    	bind interfaces only = yes
	netbios name = ***
	realm = ***.ATHEESH.ORG
	server role = active directory domain
controller
	workgroup = ***
	idmap_ldb:use rfc2307 = yes

[sysvol]
	path = /var/lib/samba/sysvol
	read only = No

[netlogon]
	path =
/var/lib/samba/sysvol/login.atheesh.org/scr
ipts
	read only = No

[Share001]
	path = /media/datadrive/***
	read only = No
	writeable = yes
	browseable = yes
	create mask = 0644
	directory mask = 0755
	valid users = @"DOMAIN\***"
	admin users = @"DOMAIN\***"

[Share002]
	path = /media/datadrive/***
	read only = No
        writeable = yes
        browseable = yes
        create mask = 0644
        directory mask = 0755
        valid users = @"DOMAIN\***"
        admin users = @"DOMAIN\***"

[Share003]
```

```
bind-interfaces
listen-address=10.0.0.51
```

Revision #11
Created 7 July 2022 08:44:32 by Atheesh
Updated 10 July 2022 16:09:10 by Atheesh