**SSSD Config for RHEL 7.X**

1. Login to the server as ec2-user and switch to root using the command sudo su
2. vi /etc/sysconfig/network  
   HOSTNAME= adserver.com
3. vi /etc/hostname  
   Update the hostname in the file. For example **hostname.adservername.com**
4. Run the following commands to make the above file immutable during reboot:

chattr +i /etc/sysconfig/network

1. vi /etc/hosts  
   Add a line in the form of <private ip>  <hostname>  
     
   For example:  172.31.27.126 **hostname.adservername.com**
2. vi /etc/cloud/cloud.cfg

preserve\_hostname: true

1. vi /etc/resolv.conf  
   Update the domain and the name server to the following:  
   The file should look like this:

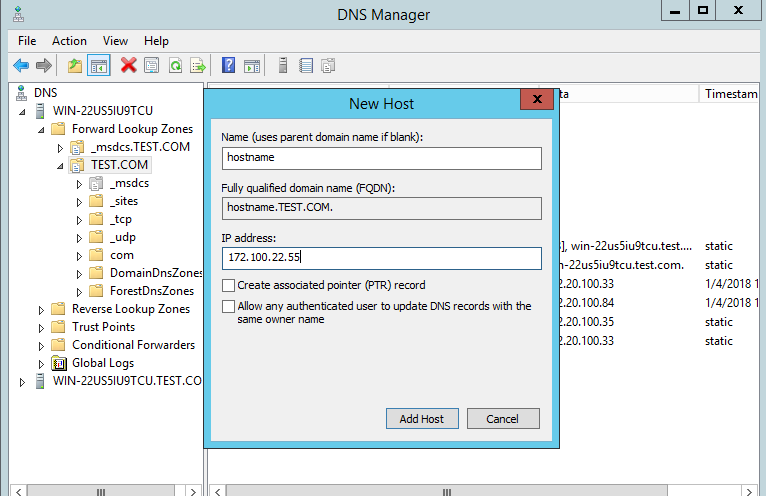
# Generated by NetworkManager

search ADSERVER.COM

nameserver 172.20.100.112 (AD Server IP)

1. chattr +i /etc/resolv.conf
2. hostnamectl set-hostname **hostname.adservername.com**
3. vi /etc/ssh/sshd\_config  
    PasswordAuthentication yes
4. Reboot the server by issuing reboot command  
     
   Optional if you have dns configured in Active directory.

1. On AD Server, Logon as Administrator
2. Go to **DNS Manager**, then click on **Forward Lookup Zones**, right click on adserver.com (AD domain), click on new Host
3. Add the hostname and private ip as shown in the below snapshot:



1. Now coming back to the your linux Server. Login as root
2. Run:  yum -y update
3. Run: yum -y install sssd realmd krb5-workstation oddjob oddjob-mkhomedir sssd samba-common-tools
4. Run:  realm join -U administrator@ ADSERVER.COM ADSERVER.COM --verbose  
     
   You will see the following output

[root@master1 ~]# realm join -U [administrator@ADSERVER.COM](mailto:administrator@ADSERVER.COM) ADSERVER.COM --verbose

\* Resolving: \_ldap.\_tcp.adserver.com

\* Performing LDAP DSE lookup on: 172.20.100.112

\* Successfully discovered: ADSERVER.COM

Password for [administrator@ADSERVER.COM](mailto:administrator@ADSERVER.COM):

\* Required files: /usr/sbin/oddjobd, /usr/libexec/oddjob/mkhomedir, /usr/sbin/sssd, /usr/bin/net

\* LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.HN7MBZ -U [administrator@ADSERVER.COM](mailto:administrator@ADSERVER.COM) ads join ADSERVER.COM

Enter [administrator@ADSERVER.COM's](mailto:administrator@ADSERVER.COM's) password:

Using short domain name -- ADSERVERCOM

Joined 'KASHIFALI' to dns domain 'ADSERVER.COM'

\* LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.HN7MBZ -U [administrator@ADSERVER.COM](mailto:administrator@ADSERVER.COM) ads keytab create

Enter [administrator@ADSERVER.COM's](mailto:administrator@ADSERVER.COM's) password:

\* /usr/bin/systemctl enable sssd.service

Created symlink from /etc/systemd/system/multi-user.target.wants/sssd.service to /usr/lib/systemd/system/sssd.service.

\* /usr/bin/systemctl restart sssd.service

\* /usr/bin/sh -c /usr/sbin/authconfig --update --enablesssd --enablesssdauth --enablemkhomedir --nostart && /usr/bin/systemctl enable oddjobd.service && /usr/bin/systemctl start oddjobd.service

\* Successfully enrolled machine in realm

1. vi /etc/sssd/sssd.conf

              Set the following parameter to False.

               use\_fully\_qualified\_names = False

1. reboot
2. After login try to search ad user from linux machine which is integrated with AD

[root@master1 ~]# id adtest

uid=1978401104(adtest) gid=1978400513(domain users) groups=1978400513(domain users),1978401106(joiners)