Follow below steps to join the linux server in AD using samba:

**Step 1**: Verify the samba and Krb5 packages are installed on the given server:

* **rpm -qa | grep samba**

samba4-libs-4.0.0-66.el6\_6.rc4.x86\_64

samba-client-3.6.23-20.el6.x86\_64

samba-common-3.6.23-20.el6.x86\_64

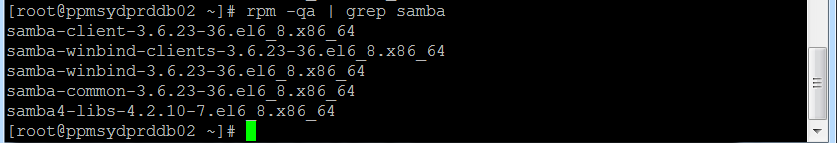
samba-winbind-3.6.23-20.el6.x86\_64

samba-winbind-clients-3.6.23-20.el6.x86\_64

Note: If any thing is missing install as per below example:

Yum install samba-winbind

Yum install samba-winbind-clients



* **rpm -qa | grep krb**

pam\_krb5-2.3.11-9.el6.x86\_64

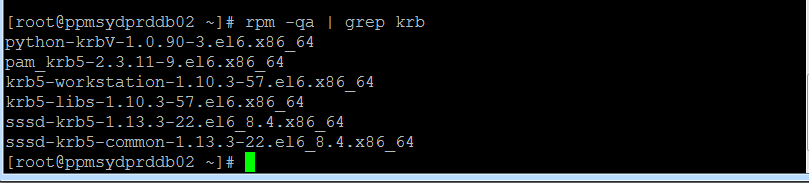
sssd-krb5-common-1.12.4-47.el6.x86\_64

krb5-workstation-1.10.3-42.el6.x86\_64

krb5-libs-1.10.3-42.el6.x86\_64

python-krbV-1.0.90-3.el6.x86\_64

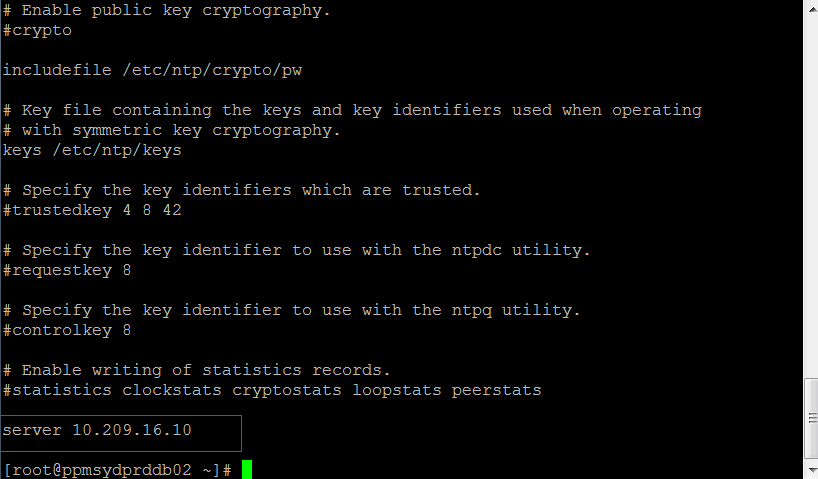
sssd-krb5-1.12.4-47.el6.x86\_64



**Step2** : Time Synchronization : AD will be verifying the time matching during the authentication. So we need to point the ntpd process to as server on our network. Update the NTP/DC server details.

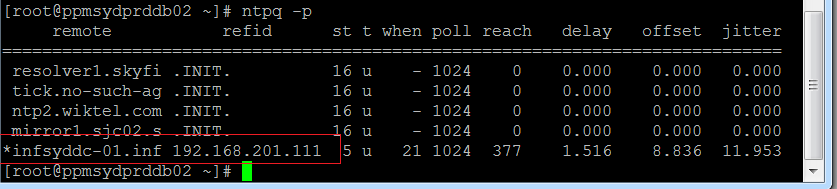
Note: Here we are using the DC server as NTP server.

vi /etc/ntp.conf

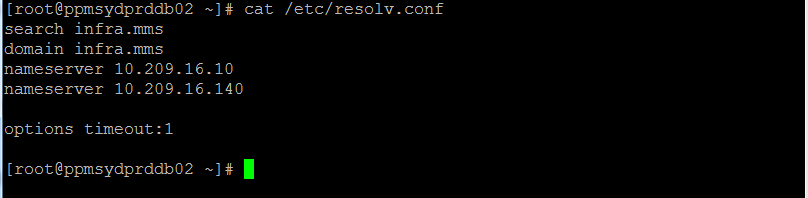


Check whether it pointing out right DC:

ntpq -p



**Step 3**: Add the DC servers to /etc/resolv.conf as shown



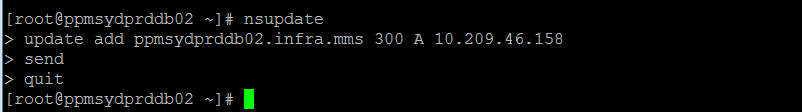
**Step 4:**

Use nsupdate to create and execute DNS update operations on a host record to a name server:

> update add ppmsydprddb02.infra.mms 300 A 10.209.46.158

> send

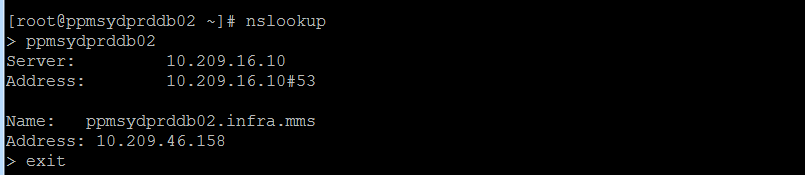
> exit



Verify the DNS record:

nslookup

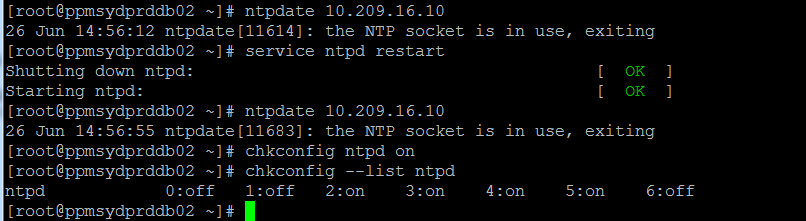
> ppmsydprddb02



ntpdate does not read the ntp.conf file. To synchronize one-time, pass the IP address of the server on the command line:

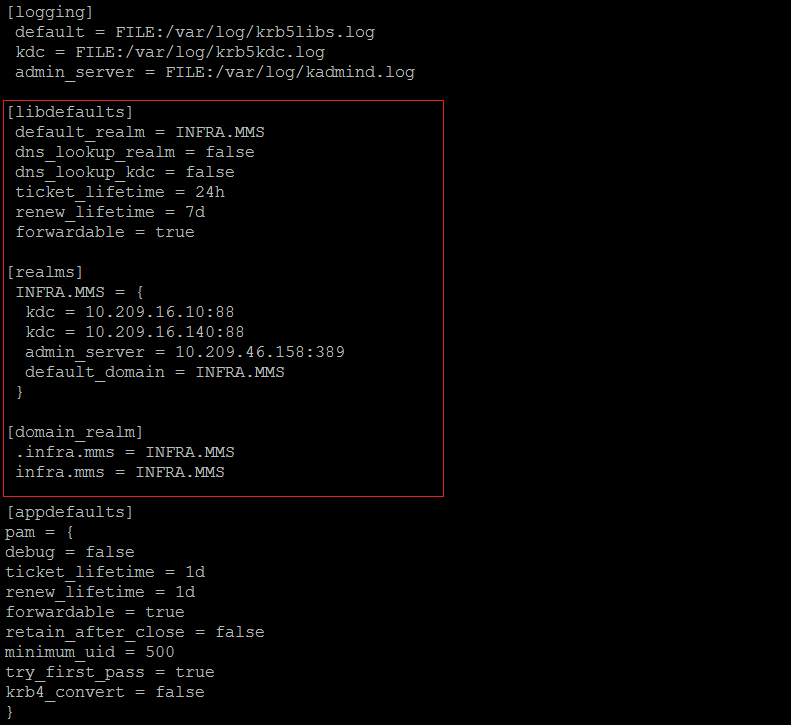
Follow the below steps

1. ntpdate 10.209.16.10
2. service ntpd restart.
3. chkconfig ntpd on
4. chkconfig --list ntpd



**Step 5:**

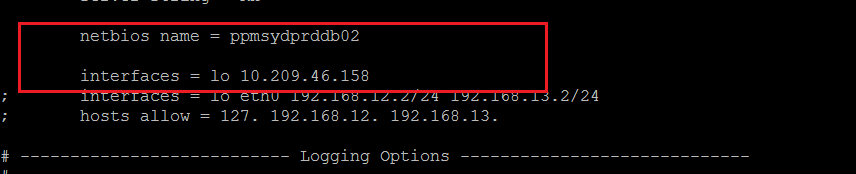
Update the Kerberos config file with respective to DC server details:



**Step 6 :**

Copy samba conf file from any other server of provided by application team as reference and update the server details (change the Name and IP).

vi /etc/samba/smb.conf

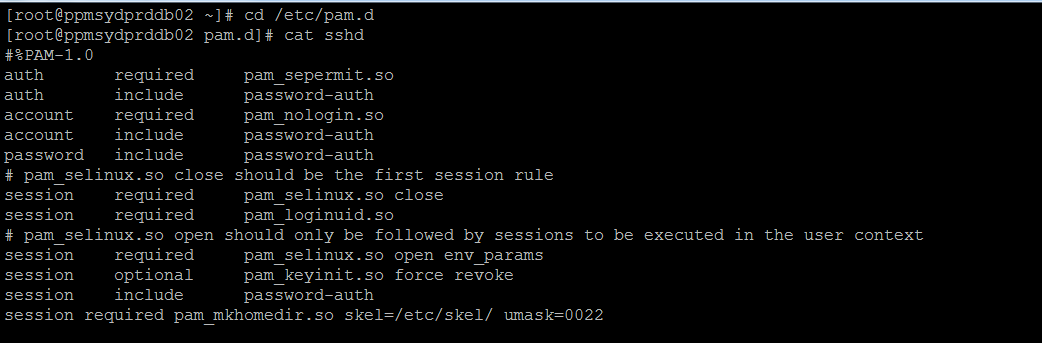


**Step 7 :**

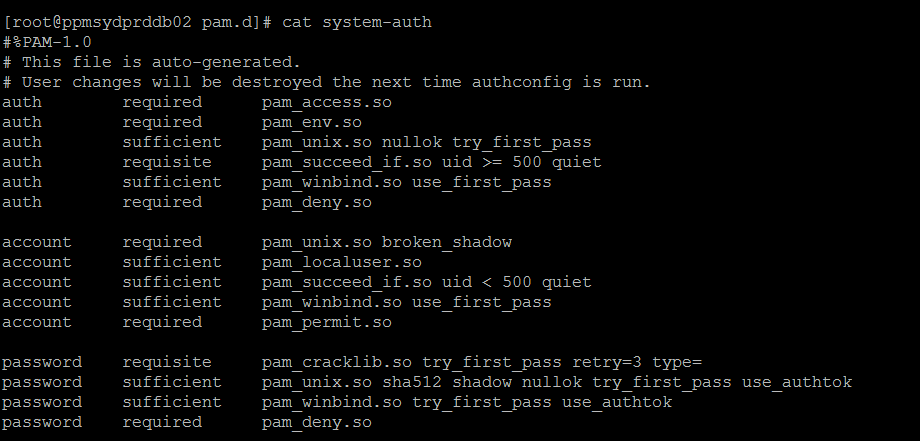
cd /etc/pam.d

copy the below files from reference server provided by the application team and update it

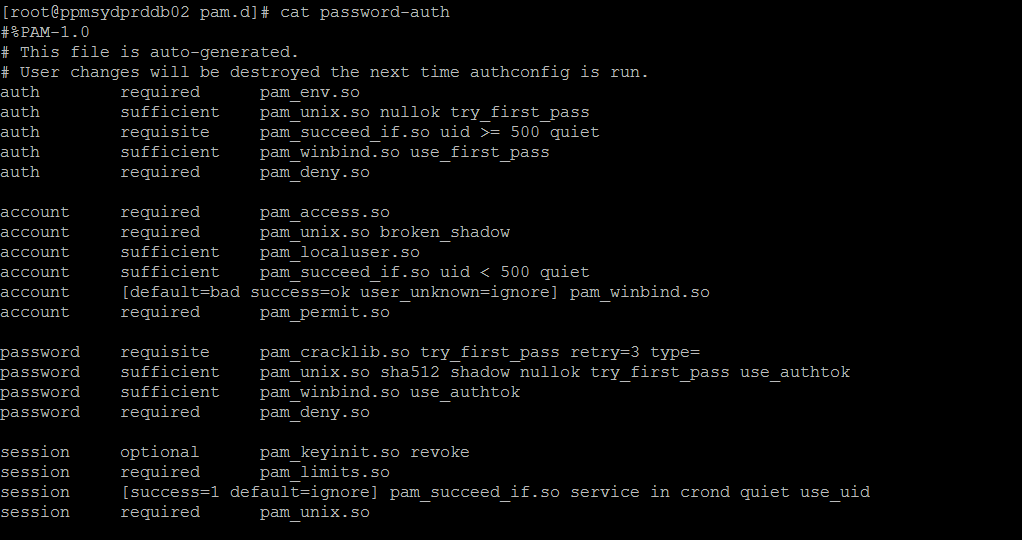
1. sshd(vi sshd)



1. system-auth( vi system-auth)



1. password-auth( vi password-auth)



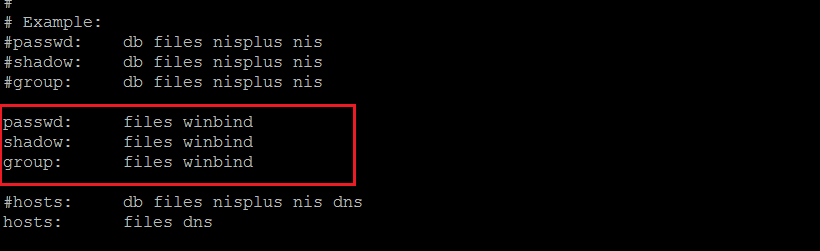
**Step 8**: Allow winbind to handle authentication:

vi /etc/nsswitch.conf

passwd: files winbind

shadow: files winbind

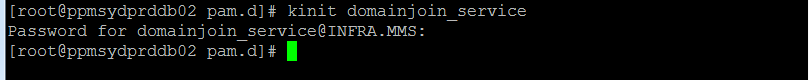
group: files winbind



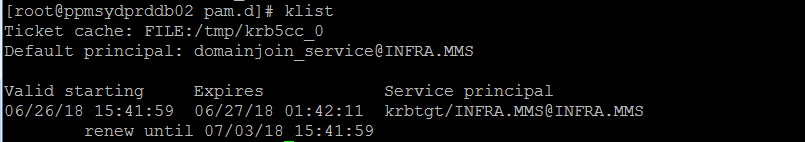
**Step 9**: Test Kerberos Authentication:

Follow the below steps:

1. kinit domainjoin\_service



1. klist will show the domainjoin\_service which we have joined in earlier step



**Step 10**: Join the domain:

1. net ads join -U domainjoin\_service( with above password)



1. Restart the winbind services:

service winbind restart

1. Once it is joined you should able to login using your account:



--------------------------------**If errors :invalid permissions on socket directory**------------------------------------

/var/lib/samba/winbindd\_privileged

/var/lib/samba/

drwxr-x---. 2 root wbpriv 4096 Nov 1 15:48 winbindd\_privileged

# chown root:wbpriv winbindd\_privileged

# chmod 750 winbindd\_privileged

########### Sudo configuration:

# vi /etc/ssh/sshd\_config

AllowGroups linux\_admins

AllowGroups ec2-user

AllowGroups ucmdb\_grp\_linux

AllowGroups infrasis\_grp

AllowGroups "arcsight users"

# vi /etc/sudoers

%linux\_admins ALL=NOPASSWD: /bin/su - root\*

%ucmdb\_grp\_linux ALL=NOPASSWD: /bin/netstat\*

%ucmdb\_grp\_linux ALL=NOPASSWD: /usr/sbin/dmidecode\*

vi /etc/sudoers.d/db

%arcsight\ users ALL=NOPASSWD: /bin/su - root\*

# service sshd restart

vi /etc/sysconfig/network-scripts/ifcfg-eth0