SETTING IPA SERVER ON CENTOS

[centralized authentication system]

steps for installing ipa server:

step1: setting up a static ip address for the server and the host

1)In this lab the server address is 10.0.0.1
and the client address is 10.0.0.2

[see the ip address section for the process of giving a static ip address]

step2: set a static host name of the server using 'hostnamectl' command

[server]

1) => hostnamectl set-hostname "ipa.test.server"
2) => exec bash

step2: edit the "/etc/hosts" of the server

=> vim /etc/hosts
[add this line

10.0.0.1 ipa.test.server ipa
]

step4: test with ping commnad

1)=> ping ipa.test.server

step5: update the server repository

1) =>yum update -y
or [if you use local repository]
yum update disablerepo="*" enablerepo='myrepo'

step6: install “free-Ipa” packages in server machine

[server]
1) => yum install disablerepo="*" enablerepo='myrepo' ipa-server bind-dyndb-ldap ipa-server-dns -y

step8: install IPA server in server machine

[server]
1) => ipa-server-install --setup-dns

8-1: Do you want to configure integreted DNS?
=>yes
8-2: Server Host name [ipa.test.system]
=>[Enter]
8-3: Please confirm Domain name [test.system]?
=>[Enter]
8-4: Please provide a realm name [TEST.SYSTEM]?
=>[Enter]
8-5: Directory manager password?
=><give_a_password>
example: admin@ipa
8-6: IPA admin Password?
=><give_a_password>
example: admin@redhat
8-7: Do you want to configure DNS Forwarders?
=>yes
8-8: Do you want these servers as DNS Forwarders?
=>yes
8-9: Do you want to search for missing reverse zone?
=>no
8-10: Continue to configure the system with these values?
=>yes

step9: Configure users Home Directory and firewall

[server]

1) =>authconfig –enablemkhomedir –update

step10: adding service to firewall

1) =>firewall-cmd –premanent –add-service=’freeipa-ldap’

1) =>firewall-cmd –premanent –add-service=’ntp’
1) =>firewall-cmd –premanent –add-service=’http’
1) =>firewall-cmd –premanent –add-service=’https’
1) =>firewall-cmd –premanent –add-service=’ldap’
1) =>firewall-cmd –premanent –add-service=’ldaps’
1) =>firewall-cmd –premanent –add-service=’kerberos’
1) =>firewall-cmd –premanent –add-service=’kpasswd’
1) =>firewall-cmd –premanent –add-service=’dns’
2) => firewall-cmd –reload

step11: checking if everything running

1)=>ipactl status

step10: adding port to firewall

1) =>firewall-cmd --permanent --zone=public
–add-port={80/tcp,443/tcp,302/tcp,636/tcp,88/tcp,464/tcp,53/tcp,88/udp,464/udp,53/udp,123/udp}
2) => firewall-cmd –reload

step12: initialize the admin user [varify weather the admin user get token from the kerberos]
[server]
1)=> kinit admin
[password: admin@redhat] [same password for installation during FreeIPA]
2)=> klist

step13: adding client to the domain
[client]
1)=> ipa-client-install –mkfomedir –server=ipa.test.system –domain test.system –realm TEST.SYSTEM –force-ntp –ssh-trust-dns

13-1:
Proceed with fixed values and no DNS discovcery?
=>yes
13-2:
Continue to configure the system with these values?
=>yes

step14: logout the server and login with admin domain
[server]

username: admin@test.system
password: admin@redhat /<admin_password>

step15: check the user
[server]

=>whoami

step16: Go to the administration page

[server]

[go to web browser to url "http://ipa.test.system"]

step16: create a user in the administration page
[server]

username: <give a username> / ex: ipa1
Firstname: ipa
lastname : user1
password : <give_password> /ex: redhat@ipa1

step16: go to the client machine and login with new user credential

username: <username> ex:ipa1
password: <password_for_the_user> ex:redhat@ipa1