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

---

ip: 192.168.0.102
gateway:192.168.0.1
dns: 8.8.8.8

---

and the client address

---

ip:192.168.0.103
gateway: 192.168.0.1
dns:192.168.0.102 [server address]

restart the connection to take effect:

5) nmcli device down <NIC/device> / ifdown <NIC>

6) nmcli device up <NIC/device> / ifup <NIC>

[important note if you give the client dns to the server address you have to install packages from local repository unless you have a second nic connected to the internet because in order to work with online repository you need a public dns like 8.8.8.8 but if you use the local repo in the client its all fine]

[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.it.local"
2) => exec bash

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

=> vim /etc/hosts
[add this line

192.168.0.102 ipa.it.local ipa
192.168.0.103 client1.it.local client1
]

step4: test with ping commnad

1)=> ping ipa.it.local

step5: update the server repository

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

step(add): reboot the system

1) =>reboot

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

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

[or you can remove all the online repo and add only the local yum repo then the command is]

2) => yum install 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] [you can login with just the user and password but to login with kerberos you have to issue the command]
[server]
1)=> kinit admin
[password:] [same password for installation during FreeIPA]
2)=> klist

step12: reboot the system again

2)=> reboot

step16: Go to the administration page and login with username and password
[server]

username: admin
password: <admin_password>

[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: setting reverse dns discovery

[server]

in the administration page go to

[NETWORK SERVICES] →[DNS] → [DNS ZONES] → [ADD.ARPA] → [ADD]

RECORD NAME : **103** //because the last number of ip is 103 [192.168.0.**103**]

RECORD TYPE: PTR

HOSTNAME: client1.it.local**.**

[remember the (.) after the client.it.local in the hostname is important]
Thats all the server configuration now we have to configure the client