Free IPA

Link –

<https://www.linuxtechi.com/install-configure-freeipa-centos-7-server/>

https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/linux\_domain\_identity\_authentication\_and\_policy\_guide/managing-idm-cli

**FreeIPA** is a free and open source identity management tool, it is the upstream project for Red Hat identity manager. Using FreeIPA tool, we can easily manage **centralized authentication** along with account management, policy (host-based access control) and audit. FreeIPA also provides the services like **DNS** and **PKI**.

* 389 Directory Server(LDAP)
* MIT Kerberos
* SSSD
* Dogtag (Certificate System)
* NTP & DNS

In this article we will demonstrate how to install and configure FreeIPA tool on CentOS 7 Server. Following are the details of my test Lab Server (CentOS7),

* IP Address = 192.168.0.102
* Hostanme = ipa.linuxtechi.lan

**Step:1 Set static Hostname and apply updates**

Set the static host name of your server using the hostnamectl command,

[root@localhost ~]# hostnamectl set-hostname "ipa.linuxtechi.lan"

[root@localhost ~]# exec bash

[root@ipa ~]# yum update -y;reboot

#### Step:2 Update the hosts file (/etc/hosts)

Run the below echo command to update /etc/hosts file, replace the ip address and hostname as per your setup.

[root@ipa ~]# echo -e "192.168.0.102\tipa.linuxtechi.lan\t ip" >> /etc/hosts

#### Step:3 Install FreeIPA packages using yum command

FreeIPA packages and its dependencies are available in the default package repositories. As we are planning to install integrated DNS of FreeIPA, so we will also install “**ipa-server-dns**”

Run the below command to install FreeIPA and its dependencies

[root@ipa ~]# yum install ipa-server ipa-server-dns -y

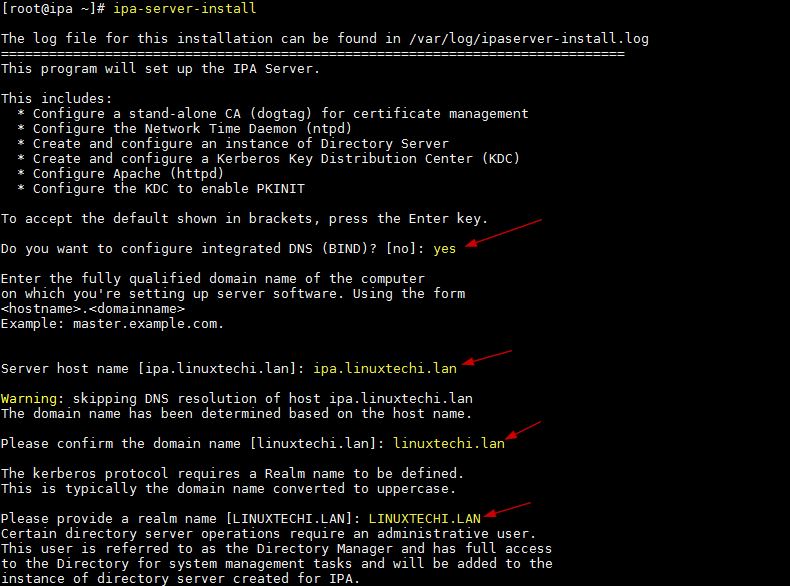
#### Step:4 Start the FreeIPA Installation setup using “ipa-server-install”

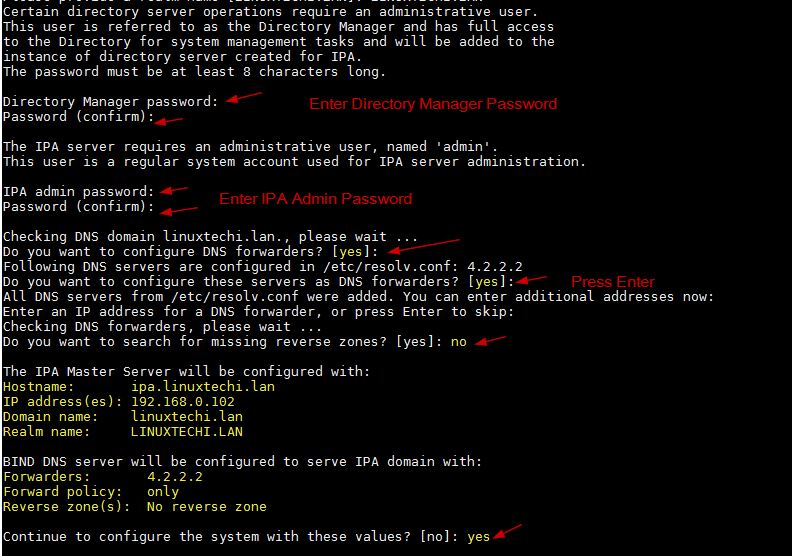
Once the packages are installed successfully then use the below command to start the freeipa installation setup,

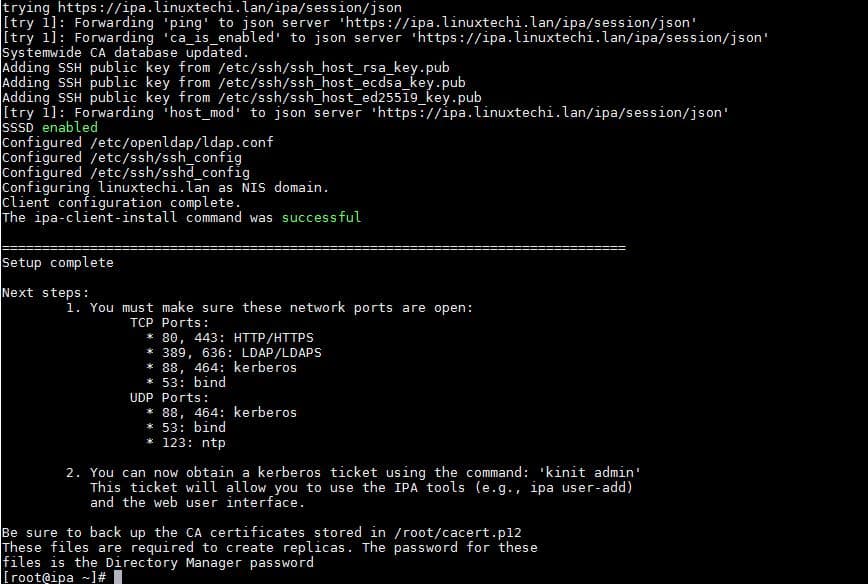
It will prompt couple of things like to configure Integrated DNS, Host name, Domain Name and Realm Name

[root@ipa ~]# ipa-server-install

Output of above command would be something like below







Run the below command to allow User’s home directory creation automatically after authentication (or login)

[root@ipa ~]# authconfig --enablemkhomedir --update

#### Step:5 Allow FreeIPA ports in OS Firewall

[root@ipa ~]# firewall-cmd --add-service=freeipa-ldap

[root@ipa ~]# firewall-cmd --add-service=freeipa-ldap --permanent

[root@ipa ~]# firewall-cmd --reload

#### Step:6 Verification & Access FreeIPA admin portal

[root@ipa ~]# ipactl status

Directory Service: RUNNING

krb5kdc Service: RUNNING

kadmin Service: RUNNING

named Service: RUNNING

httpd Service: RUNNING

ipa-custodia Service: RUNNING

ntpd Service: RUNNING

pki-tomcatd Service: RUNNING

ipa-otpd Service: RUNNING

ipa-dnskeysyncd Service: RUNNING

ipa: INFO: The ipactl command was successful

Let’s verify whether admin user will get token via Kerberos using the kinit command, use the same password of admin user that we supplied during FreeIPA installation.

[root@ipa ~]# kinit admin

Password for admin@LINUXTECHI.LAN:

[root@ipa ~]# klist

Ticket cache: KEYRING:persistent:0:0

Default principal: admin@LINUXTECHI.LAN

Valid starting       Expires              Service principal

11/26/2018 07:39:00  11/27/2018 07:38:55  krbtgt/LINUXTECHI.LAN@LINUXTECHI.LAN

[root@ipa ~]#

Access the FreeIPA admin portal using the URL:

https://ipa.linuxtechi.lan/ipa/ui

Use the user name as admin and the password that we specify during the installation.

**ipa user-add** command adds a new user:

$ ipa user-add *user\_name*

the **ipa help topics** command:

$ ipa help topics

$ ipa help commands

To list all users:

$ ipa user-find

To list user groups whose specified attributes contain *keyword*:

$ ipa group-find *keyword*

When searching user groups, you can also limit the search results to groups that contain a particular user:

$ ipa group-find --user=*user\_name*

You can also search for groups that do not contain a particular user:

$ ipa group-find --no-user=*user\_name*

Use the **ipa \*-show** command to display details about a particular IdM entry. For example:

$ ipa host-show *server.example.com*

Host name: server.example.com

Principal name: host/server.example.com@EXAMPLE.COM

To adjust the limits globally for all queries, use the **ipa config-mod** command and add the --searchrecordslimit and --searchtimelimit options. For example:

$ ipa config-mod --searchrecordslimit=500 --searchtimelimit=5

From the command line, you can also adjust the limits only for a specific query. To do this, add the --sizelimit or --timelimit options to the command. For example:

$ ipa user-find --sizelimit=200 --timelimit=120