Cluster Account Creation and Management

[**Introduction:**](#_syap4nq0cy4e) **1**

[FreeIPA:](#_ofgu4gbhv6ht) 1

[**Configuring DNS for FreeIPA**](#_wwx5238pxbpv) **2**

[**Installing FreeIPA:**](#_jdgf6te5y3ti) **2**

[Installing the FreeIP Server:](#_uawm6y5ofw09) 2

[Option 1 (Making Puppet Module):](#_hatcs76af2yc) 2

[Option 2 (Following a tutorial):](#_z9qtnras2h7y) 2

[Option 3 (The short cut method):](#_4io7v9cngzt8) 3

[Post set up procedure:](#_ucfw5b3kbr2s) 4

[Installing the FreeIP Client:](#_8pl3574i3flu) 5

[**Adding New Accounts Using FreeIPA:**](#_8fkgdacg82hg) **5**

# Introduction:

An essential feature of any computing system is the creation and management of user accounts. You need to be able to create an account in one place and have it visible in many. Users need to be able to change their password from any machine. Linux provides many different systems to perform this functionality. It the past the administrators had to patch together different systems and worry about future capability. The project/package FreeIPA nows includes all the needed functionality. It also includes both a command line interface and GUI for management,

## FreeIPA:

Web site: <https://www.freeipa.org/page/Main_Page>

|  |
| --- |
| FreeIPA is an Identity management system. It aims to provide an easily managed Identity, Policy, and Audit (IPA). FreeIPA is the upstream open-source project for Red Hat Identity Manager.   * Integrated security information management solution combining Linux (Fedora), 389 Directory Server, MIT Kerberos, NTP, DNS, Dogtag certificate system, SSSD and others. * Built on top of well known Open Source components and standard protocols * Strong focus on ease of management and automation of installation and configuration tasks. * Full multi master replication for higher redundancy and scalability * Extensible management interfaces (CLI, Web UI, XMLRPC and JSONRPC API) and Python SDK |

# Configuring DNS for FreeIPA

Proper DNS configuation

# Installing FreeIPA:

## Installing the FreeIP Server:

FreeIPA is a client/server architecture. You first install the server component and then the client.

### Option 1 (Making Puppet Module):

There is a community Puppet module that handles FreeIPA installation:

|  |
| --- |
| <https://forge.puppet.com/sgnl05/sssd> |

I have not worked with this module but it does get a rating of 5.0/5.0 on forge.puppet.com.

### Option 2 (Following a tutorial):

For the server installation, one of the better ones I found is:

|  |
| --- |
| <https://www.itzgeek.com/how-tos/linux/centos-how-tos/configure-freeipa-server-on-centos-7-rhel-7-debian-9-fedora-27.html> |

The changes to this tutorial I recommend are:

1. Make sure **dnsmasq** is **installed, started and enabled**.

|  |
| --- |
| # Check for dnsmasq installation  rpm -qa | grep dnsmasq |

1. If **dnsmasq** is **not installed**:

|  |
| --- |
| yum install dnsmasq |

1. **Enable** and **start** **dnsmasq**:

|  |
| --- |
| # Enable dnsmasq  systemctl enable dnsmasq  # Start dnsmasq  systemctl start dnsmasq |

1. Because of software conflicts between the epel and osg repositories, you want to install the software with the osg repository temporarily disabled:

|  |
| --- |
| yum clean all  yum install --disablerepo=osg ipa-server ipa-server-dns bind-dyndb-ldap |

1. **Skip** the part about starting and enablng named:

|  |
| --- |
| systemctl start named systemctl enable named |

1. Then use the following values:

|  |
| --- |
| Do you want to configure integrated DNS (BIND)? [no]: **no**  Server host name [ipa.itzgeek.local]: **htc180.najah.edu**  Please confirm the domain name [itzgeek.local]: **najah.edu**  Please provide a realm name [ITZGEEK.LOCAL]: **HTC.NAJAH.EDU** |

1. **You can safely ignore:**

|  |
| --- |
| WARNING: Realm name does not match the domain name.  You will not be able to establish trusts with Active Directory unless  the realm name of the IPA server matches its domain name. |

### Option 3 (The short cut method):

|  |
| --- |
| These commands **should** work. They were tested on a Virtual Machine in Colorado. |

Make sure **dnsmasq** is **installed, started and enabled**.

|  |
| --- |
| # Check for dnsmasq installation  rpm -qa | grep dnsmasq |

If **dnsmasq** is **not installed**:

|  |
| --- |
| yum install dnsmasq |

**Enable** and **start** **dnsmasq**:

|  |
| --- |
| # Enable dnsmasq  systemctl enable dnsmasq  # Start dnsmasq  systemctl start dnsmasq |

Now **install** the **FreeIPA** **server** software:

|  |
| --- |
| yum clean all  yum install --disablerepo=osg ipa-server ipa-server-dns bind-dyndb-ldap |

And now configure FreeIPA server:

|  |
| --- |
| ipa-server-install -p OurPassword -a OurPassword -r NAJAH.EDU \  --hostname=htc180.najah.edu -n najah.edu -N -U \  --ip-address=171.16.9.180 |

### Post set up procedure:

After the installation, you will need to create the file:

**/etc/dnsmasq.d/kerberos.conf:**

|  |
| --- |
| srv-host = \_kerberos-master.\_tcp.najah.edu. 86400 IN SRV 0 100 88 htc180.najah.edu.  srv-host = \_kerberos-master.\_udp.najah.edu. 86400 IN SRV 0 100 88 htc180.najah.edu.  srv-host = \_kerberos.\_tcp.najah.edu. 86400 IN SRV 0 100 88 htc180.najah.edu.  srv-host = \_kerberos.\_udp.najah.edu. 86400 IN SRV 0 100 88 htc180.najah.edu.  srv-host = \_kpasswd.\_tcp.najah.edu. 86400 IN SRV 0 100 464 htc180.najah.edu.  srv-host = \_kpasswd.\_udp.najah.edu. 86400 IN SRV 0 100 464 htc180.najah.edu.  srv-host = \_ldap.\_tcp.najah.edu. 86400 IN SRV 0 100 389 htc180.najah.edu.  txt-record = \_kerberos.najah.edu. 86400 IN TXT "NAJAH.EDU" |

And restart dnsmasq:

|  |
| --- |
| systemctl restart dnsmasq  systemctl status dnsmasq |

This system requires firewall setttings:

|  |
| --- |
| for SER in ntp http https ldap ldaps kerberos kpasswd; do firewall-cmd --permanent --add-service=$SER; done firewall-cmd --permanent --add-port=53/udp firewall-cmd --permanent --add-port=53/tcp firewall-cmd --reload |

|  |
| --- |
| WARNING: Now that we are all working on the same server, it is important to coordinate these changes with the rest of the group. There is very likely someone working on security and/or firewall settings. |

## Installing the FreeIP Client:

A bunch of stuff to get DNS working properly. We need help from Mr. Adas with the documentation.

|  |
| --- |
| ipa-client-install --domain=najah.edu --server=htc180.najah.edu -U -p admin \  -w OurPassword |

# Adding New Accounts Using FreeIPA:

Mr. Adas: Please reveal all?