IPA - Fast and Dirty

This guide explains how to deploy FreeIPA the quickest way possible.

This is not for production.

You will need a fresh install of CentOS 7. The latest edition will be fine.

As root, update the server and install the requirements.

```
yum update -y
yum install -y ipa-server bind-dyndb-ldap ipa-server-dns
```

Open the firewall ports and reload the firewall.

```
firewall-cmd --permanent --add-service={http,https,ftp,ldap,ldaps,kerberos,kpasswd,dns,ntp}
firewall-cmd --reload
```

Run the IPA Server install.

```
ipa-server-install --setup-dns --allow-zone-overlap
kinit admin
```

Follow the install prompts. Answer each item. If you don't know, choose the default option.

```
kinit admin
<enter password entered durring ipa setup>
klist # to view the ticket.
```

Check the IPA Server status.

```
ipactl status
```

Example:

```
# ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
```

```
named Service: RUNNING
ipa_memcached Service: RUNNING
httpd Service: RUNNING
pki-tomcatd Service: RUNNING
ipa-otpd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

If there were no errors, then you have a running IPA Server. Log in to the IPA server to begin management tasks. To use the web interface go to https://<fqdn of the IPA server.

To setup a simple method for transferring the CA certificate is ftp. In this example vsftpd is used. The firewall ports were already opened during the IPA setup.

```
yum install -y vsftpd
systemctl enable --now vsftpd # or systemctl enable vsftpd; systemctl start vsftpd
cp /etc/ipa/ca.crt /var/ftp/pub
```

Now non-IPA clients will be able to securely access the LDAP. Add this certificate to web browsers or other application to trust web services that use the IPA sever as a CA.

Revision #3
Created 6 April 2019 20:31:44 by Michael Cleary
Updated 16 February 2022 23:58:51 by Michael Cleary