Identity and Access Management

- Foreman Smart Proxy - FreeIPA DNS
- IPA - Basic Commands
- IPA - Fast and Dirty

Foreman Smart Proxy - FreeIPA DNS

The SmartProxy DNS module can update any DNS server that complies with the ISC Dynamic DNS Update standard. Updates can also be made using GSS-TSIG, additional providers are available for managing libvirt's embedded DNS server, and Microsoft Active Directory using dnscmd, for static DNS records.

This guide will focus on FreeIPA and kerberos for SmartProxy DNS management.

FreeIPA configuration

A service principal is required for the Smart Proxy

`foremanproxy/proxy.example.com@EXAMPLE.COM`.

Create a new service principal for the SmartProxy. On any IPA server or controller node:

`ipa service-add foremanproxy/proxy.example.com@EXAMPLE.COM`.

On the SmartProxy host, get the keytab file

`ipa-getkeytab -p foremanproxy/proxy.example.com@EXAMPLE.COM -s ipa-server.example.com -k /etc/foreman-proxy/dns.keytab`

Set permissions and owner for the keytab.

`chmod 0600 /etc/foreman-proxy/dns.keytab && chown foreman-proxy /etc/foreman-proxy/dns.keytab`

In the FreeIPA web UI, go to the DNS zone, then to the Settings tab, verify that "Dynamic update" is set to "True", and add the following to the BIND update policy a new grant:

```
grant foremanproxy\047proxy.example.com@EXAMPLE.COM wildcard * ANY;
```

ACLs should be updated for both forward and reverse zones.
Note the `\047` is written verbatim, and don't forget the semicolon.

Proxy configuration

Update the proxy DNS configuration file (`/etc/foreman-proxy/settings.d/dns.yml`) with the following setting:

```
:use_provider: dns_nsupdate_gss
```

And the DNS GSS configuration file (`/etc/foreman-proxy/settings.d/dns_nsupdate_gss.yml`) with:

```
:dns_server: 127.0.0.1 or ip of DNS
:dns_tsig_keytab: /etc/foreman-proxy/dns.keytab
:dns_tsig_principal: foremanproxy/proxy.example.com@EXAMPLE.COM
```

Ensure the `dns_key` setting is not specified, or is commented out.

Restart the smart proxy service.

`systemctl restart foreman-proxy`

check the log file for any errors or warnings.

`tail -fn100 /var/log/foreman-proxy/proxy.log`

Update Foreman

After adding a Smart Proxy plugin, you must instruct Foreman to rescan the configuration.

In Foreman, Go to the Smart Proxies Use the Actions drop-down menu and select “Refresh Features” .

Add the Smart Proxy as a DNS proxy on the subnets and domains as needed.

IPA - Basic Commands

A basic list of command to manage FreeIPA services.

DNS

Add new a record and reverse record.

An A record is used to map an FQDN to an IP address. The A record is created using the following:

`ipa dnsrecord-add <forward-zone>  <short-name> --a-rec <IP of A record>`

The reverse, or pointer, record is used to map the IP to a hostname. The command to create a pointer is:

`ipa dnsrecord-add <reverse-zone> <num> --ptr-rec <host-FQDN>.`

Note the trailing dot. This is very important.

This is an example of adding server1.i.example.com with the IP of 192.168.4.11 to the FreeIPA DNS.

```
ipa dnsrecord-add i.example.com  server1 --a-rec 192.168.4.11
ipa dnsrecord-add 4.168.192.in-addr.arpa 11 --ptr-rec server1.i.example.com.
```

Hosts

Remove a failed or dead host.

```
ipa host-del server1 --updatedns
```

Including the `--updatedns` option will also remove all of the linked DNS entries for this host.

Services

The service must include the service / FQDN of the host.

```
ipa service-add nfs/server1.i.example.com
```

Users

Add a new user *lab1*

```
ipa user-add lab1
```

Change the new user's password

```
ipa passwd lab1
```

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.