

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.

Revision #1

Created 2 April 2019 12:43:12 by Michael Cleary

Updated 16 February 2022 23:58:51 by Michael Cleary