Smart Proxy - Feature #1809

Smart-Proxy control of IPA Server

08/06/2012 05:40 PM - Charlie Derwent

Status:	Closed		
Priority:	Normal		
Assignee:	Stephen Benjamin		
Category:	DNS		
Target version:	1.5.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Are there any plans to create a Smart-Proxy to manage the DNS, Host and Hostgroups portions of Red Hat's IPA / FreeIPA server from within Foreman?

API looks pretty fully featured
http://freeipa.org/developer-docs/

Would be good to support a sister project. Could potentially do some interesting things with certificate/service/ssh key management during provisioning too.

Related issues:

Related to Foreman - Feature #1685: Windows DNS: Secure connection using GSS-...	**Closed**	**06/14/2012**	
Related to Smart Proxy - Feature #4917: Smart-Proxy Realm Provider for Active...	**Resolved**	**03/27/2014**	
Has duplicate Foreman - Feature #2356: smart-proxy, FreeIPA subsystem support	**Duplicate**	**03/27/2013**	
Precedes Hammer CLI - Bug #4918: Add realm commands	**Closed**	**08/07/2012**	**08/07/2012**

Associated revisions

Revision 45e05273 - 04/02/2014 10:07 AM - Stephen Benjamin

fixes #1809 - freeipa integration to smartproxy

Revision 77f70152 - 04/02/2014 10:46 AM - Stephen Benjamin

fixes #1809 - foreman realm integration

Revision c58901fc - 04/03/2014 07:27 PM - Stephen Benjamin

fixes #1809 - templates for freeipa registration

History

#1 - 01/18/2013 10:53 AM - Dominic Cleal

Integrating machine joins via OTPs would be useful too: http://freeipa.org/page/Machine_join. This might work well as a plugin.

#2 - 03/20/2013 05:36 AM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Dominic Cleal

- Target version set to 26

#3 - 05/10/2013 09:07 AM - Dominic Cleal

- Target version changed from 26 to 1.3.0

#4 - 05/28/2013 09:02 AM - Guy Matz

I was just about to open up a redmine ticket for this very thing! Has anyone already started work on it? I'm almost done with my code . . .

#5 - 05/28/2013 09:07 AM - Dominic Cleal

Guy Matz wrote:

> I was just about to open up a redmine ticket for this very thing! Has anyone already started work on it? I'm almost done with my code . . .

Nope, we're banking on you :)

#6 - 09/16/2013 11:49 AM - Lukas Zapletal

- Description updated

- Target version deleted (1.3.0)

#7 - 11/21/2013 04:36 PM - Stephen Benjamin

Hi, Has there been any more work on this? I ended up doing this using hooks:
https://bitbin.de/blog/2013/11/foreman-freeipa-integration-guide/

Then I discovered this and that most of the work was already done to get it in the Smart Proxy :-D

I'd offer my help if you're interested. I was playing with this in my dev environment to implement a couple of different ideas -- like using the IPA XML RPC API instead, and pre-creating the service principals for Puppet (so FreeIPA can act as a CA)
http://github.com/stbenjam/smart-proxy/compare/WIP-realm-support

What do you think?

#8 - 11/21/2013 04:45 PM - Dominic Cleal

Stephen Benjamin wrote:

> Hi, Has there been any more work on this? I ended up doing this using hooks:
> https://bitbin.de/blog/2013/11/foreman-freeipa-integration-guide/

No more work done yet, but it's queued on the backlog probably for the sprint after this one.

> Then I discovered this and that most of the work was already done to get it in the Smart Proxy :-D
>
> I'd offer my help if you're interested. I was playing with this in my dev environment to implement a couple of different ideas -- like using the IPA XML RPC API instead, and pre-creating the service principals for Puppet (so FreeIPA can act as a CA)
> http://github.com/stbenjam/smart-proxy/compare/WIP-realm-support
>
> What do you think?

I'm not worried about using the XMLRPC API versus the ipa command if it's easily done. We've also got the rkerberos gem available for doing the "kinit" + keytab portion, which should let you then use GSSAPI.

Rob Crittenden has talked about even implementing the proxy's REST API in FreeIPA so we would register their service as a proxy and call it directly, without needing us to implement anything. I don't know what the status of that is, but we probably need to do this as an interim measure.

Regarding service principals, I'd like to see this added to FreeIPA's hostgroup feature, but again, we could do it here in the interim as it's low impact. This might mean we could set a user class parameter on the host object when it's created, and perhaps have it automatically create certain principals on the host? See the bottom of http://projects.theforeman.org/projects/foreman/wiki/RealmJoinIntegration.

But yes, I'm all for doing what you suggest!

#9 - 11/21/2013 11:57 PM - Stephen Benjamin

> I'm not worried about using the XMLRPC API versus the ipa command if it's easily done.

I suppose it's fine either way, the API is simpler IMHO - no screen scraping and comes with JSON back out of the box (which includes the generated OTP).

> We've also got the rkerberos gem available for doing the "kinit" + keytab portion, which should let you then use GSSAPI.

Yup, I saw that in Guy's code -- that's great! I was looking for a clean way to kinit in ruby.

> Rob Crittenden has talked about even implementing the proxy's REST API in FreeIPA so we would register their service as a proxy and call it directly, without needing us to implement anything. I don't know what the status of that is, but we probably need to do this as an interim measure.

There's a page on freeipa.org about it, implementing a limited RESTful API for Foreman

FreeIPA already has JSON-RPC and XML-RPC APIs... does adding a 3rd special purpose provisioning API make sense on their side? I guess that's up to them, but I think there's good reasons that it fits better in the smart proxy.

> Regarding service principals, I'd like to see this added to FreeIPA's hostgroup feature, but again, we could do it here in the interim as it's low impact. This might mean we could set a user class parameter on the host object when it's created, and perhaps have it automatically create certain principals on the host? See the bottom of http://projects.theforeman.org/projects/foreman/wiki/RealmJoinIntegration.

I see how classes fit with IPA groups, that's clever! How would service principals be tied to host groups? Like, a web_server hostgroup comes with HTTP principals? I think that could be useful in some cases, but maybe THAT belongs in FreeIPA as part of auto-member functionality...

My primary concern was about using FreeIPA as the CA for puppet, but now, I wonder if this doesn't belong in a certificate authority smart proxy as an entirely separate thing for later. Plenty of companies using other things for their PKI that could conceivably be used, not just FreeIPA and Puppet CA.

> But yes, I'm all for doing what you suggest!

Ok :-) Is Guy still active? I don't want to step on any toes.

#10 - 11/22/2013 09:08 AM - Dominic Cleal

Stephen Benjamin wrote:

> > Rob Crittenden has talked about even implementing the proxy's REST API in FreeIPA so we would register their service as a proxy and call it directly, without needing us to implement anything. I don't know what the status of that is, but we probably need to do this as an interim measure.
>
> There's a page on freeipa.org about it, implementing a limited RESTful API for Foreman

Interesting, do you have a link?

> FreeIPA already has JSON-RPC and XML-RPC APIs... does adding a 3rd special purpose provisioning API make sense on their side? I guess that's up to them, but I think there's good reasons that it fits better in the smart proxy.

Yeah, I'm happy doing it here for now. If it means we can drop it in a year or two's time, that's ok.

> > Regarding service principals, I'd like to see this added to FreeIPA's hostgroup feature, but again, we could do it here in the interim as it's low impact. This might mean we could set a user class parameter on the host object when it's created, and perhaps have it automatically create certain principals on the host? See the bottom of http://projects.theforeman.org/projects/foreman/wiki/RealmJoinIntegration.
>
> I see how classes fit with IPA groups, that's clever! How would service principals be tied to host groups? Like, a web_server hostgroup comes with HTTP principals? I think that could be useful in some cases, but maybe THAT belongs in FreeIPA as part of auto-member functionality...

Yep, that's what I think.. haven't raised it with the FreeIPA team yet.

> My primary concern was about using FreeIPA as the CA for puppet, but now, I wonder if this doesn't belong in a certificate authority smart proxy as an entirely separate thing for later. Plenty of companies using other things for their PKI that could conceivably be used, not just FreeIPA and Puppet CA.

Yes, I'd love to see proper CA integration when creating hosts.

> > But yes, I'm all for doing what you suggest!
>
> Ok :-) Is Guy still active? I don't want to step on any toes.

Not at the moment, so we can build on his work and get it included.

#11 - 11/22/2013 12:21 PM - Stephen Benjamin

Thanks for the info.

Link: http://www.freeipa.org/page/V3/Smart_Proxy

I've incorporated my changes on top of Guy's branch. Here's the relevant section that does the userclass bits for automember..

https://github.com/stbenjam/smart-proxy/compare/1809-add_IPA_support#diff-9c233f21af7db8e9df019aee97fec4b0R68

At the moment it accepts setting arbitrary IPA keys. So, you'd pass ipa_userclass=webservers from your example. How will we POST to the Smart Proxy? A custom JSON or the dump of the host GET (/api/hosts/<hostname>)? That doesn't include the hostgroup string.

#12 - 11/22/2013 12:41 PM - Dominic Cleal

Stephen Benjamin wrote:

> Thanks for the info.
>
> Link: http://www.freeipa.org/page/V3/Smart_Proxy

Thanks.

> I've incorporated my changes on top of Guy's branch. Here's the relevant section that does the userclass bits for automember..
>
> https://github.com/stbenjam/smart-proxy/compare/1809-add_IPA_support#diff-9c233f21af7db8e9df019aee97fec4b0R68
>
> At the moment it accepts setting arbitrary IPA keys. So, you'd pass ipa_userclass=webservers from your example. How will we POST to the Smart Proxy? A custom JSON or the dump of the host GET (/api/hosts/<hostname>)? That doesn't include the hostgroup string.

I'm a bit unsure about passing arbitrary data into it, as the API we use here will have to apply equally to Active Directory in the future (we're just adding a computer object there in the same way, probably using adcli).

The API on the smart proxy is custom, we don't pass any Foreman data as-is, but instead the orchestration layer in Foreman calls the ProxyAPI classes, which then pass whatever parameters are needed for the smart proxy API.

Whether Foreman's host group == IPA's host group I'm unsure though.. I'd assumed it would be separate and just happened to be called the same thing. Maybe IPA host classes are parameters on our host groups or hosts?

By the way, Guy's other branch for Foreman core is here: https://github.com/guymatz/foreman/tree/1809-add_IPA_support

#13 - 11/22/2013 01:31 PM - Stephen Benjamin

> I'm a bit unsure about passing arbitrary data into it, as the API we use here will have to apply equally to Active Directory in the future (we're just adding a computer object there in the same way, probably using adcli).

Ok, that makes sense.

> Whether Foreman's host group == IPA's host group I'm unsure though.. I'd assumed it would be separate and just happened to be called the same thing. Maybe IPA host classes are parameters on our host groups or hosts?

Ok, so how about we always post the host's parameters (global ones from the ENC) to a Realm proxy?

And the FreeIPA handler can act on those. FreeIPA automember rules can be based on any LDAP attribute so we might want to be a bit flexible. Perhaps ship a default mapping in settings.yml?

That leaves it open if the user wants to do auto member on some arbitrary parameter they give in Foreman.

Something like:

```
:freeipa_attribute_mapping:
  managedby: :owner_name
  userclass: :hostgroup
```

Does that makes sense?

#14 - 11/28/2013 04:54 PM - Dominic Cleal

- Status changed from Assigned to Ready For Testing

- Assignee changed from Dominic Cleal to Stephen Benjamin

- Target version set to 1.10.0

I'm unsure about free-form mapping, but will continue discussion on the PRs.

https://github.com/theforeman/foreman/pull/1061
https://github.com/theforeman/smart-proxy/pull/115

#15 - 12/04/2013 01:11 PM - Dominic Cleal

- Target version changed from 1.10.0 to 1.9.3

#16 - 01/09/2014 02:12 PM - Anonymous

- Target version changed from 1.9.3 to 1.9.2

#17 - 02/06/2014 12:12 PM - Anonymous

- Target version changed from 1.9.2 to 1.9.1

#18 - 02/20/2014 10:50 AM - Duncan Innes

Is there any work on this? Or is it going to keep dropping back from Sprint to Sprint?

Would be nice to tie in some of our IPA requirements through Foreman.

#19 - 02/20/2014 11:33 AM - Stephen Benjamin

Yea, there's some changes that I need to finish based on Dominic's feedback. I haven't had time, but maybe in the next few days. There's not much to finish.

There was also the open question of whether the FreeIPA guys were actually going to implement something on their side but I still don't understand their intentions at all. I'm going to finish the functionality in the foreman smart-proxy.

#20 - 02/20/2014 02:19 PM - Stephen Benjamin

I updated the PR's with the latest.

Some to-do's:

- Tests
- SmartProxy - should it support multiple realms or just one? Should be simple to make it support multiple
- Documentation for Manual
- Community Templates snippet for ipa registration w/ OTP

#21 - 02/21/2014 09:53 PM - Rob Crittenden

The IPA smartproxy design is this: http://www.freeipa.org/page/V3/Smart_Proxy

The IPA patch is under review at http://www.redhat.com/archives/freeipa-devel/2014-January/msg00213.html

#22 - 02/21/2014 10:36 PM - Stephen Benjamin

Ok, well, we should coordinate.

You'll need to rely on the code I've written in Foreman core to handle Realms, and as it stands your API is different than the one I've written.   I've no problem adapting to what you've done, it's also perfectly sane.

Just some point/questions:

- Your API needs to respond ["realm"] to GET /features

- Smart Proxy inputs are all parameters at the moment, and that's how my Smart Proxy FreeIPA API works:

e.g. hostname=string&password=string&random=boolean

I like JSON better, but it's just not how things are done for anything else.

- What is the output from the POST to create a host?

- If random is true, you'll return a random password? I don't see a use case in Foreman for letting the user specify an OTP.

- What the intention of force? I think that should probably be a global smart proxy setting, I don't see us adding this to Foreman since we don't for anything else. If any kind of record already exists, we bail. Unless we want something different for this -- like a "Force register" check-box (Dominic?

- Can you take inputs for "userclass" in the POST JSON (and later parameters if this changes) --> my version passes the hostgroup label, so you could do automember rules on the IPA side. This is a major feature of the idea behind realm integration, to be able to link IPA host groups to

Foreman host groups.

That's all I can think of now.

#23 - 02/22/2014 12:12 AM - Stephen Benjamin

I also recorded a short demo of what the functionality is in the PR's today, just to give you an idea of how it works from start to finish (Warning: Adobe Flash)

http://screencast.com/t/tBhNUbzlgHn

#24 - 02/25/2014 01:27 PM - Duncan Innes

As I understand it, the 'force' option is used to force creation of the record if a DNS A record can't be found. IPA demands that a DNS entry exists, but this overrides the requirement.

#25 - 02/25/2014 01:43 PM - Stephen Benjamin

Force should probably be the default without needing to send it then, since the realm API needs to be generic not IPA-specific.

It can be configurable on the smart proxy if you want. In the ruby one I wrote, I just default to sending force = 1. Forgot about that, since I wrote it a while ago.

#26 - 02/27/2014 04:48 PM - Rob Crittenden

I'm working on implementing the changes now.

I'm returning data as json. This is what adding a host looks like:

```
{
  "dn": "fqdn=hostname.example.com,cn=computers,cn=accounts,dc=example,dc=com",
  "fqdn": [
    "hostname.example.com"
  ],
  "has_keytab": false,
  "has_password": true,
  "ipauniqueid": [
    "5f5d467c-9fce-11e3-bcca-525400d17cb3"
  ],
  "managedby_host": [
    "hostname.example.com"
  ],
  "objectclass": [
    "ipaSshGroupOfPubKeys",
    "ipaobject",
    "ieee802device",
    "nshost",
    "top",
    "ipaservice",
    "pkiuser",
    "ipahost",
    "ipasshhost"
  ],
  "randompassword": "_i7@PhgpAnjn"
}
```

I switched to using POST data rather than URL parameters in fact to support passing the password without logging it. I'll switch back and consider dropping password.

I'm fine with defaulting to True for force.

I'll add an option for userclass.

#27 - 02/27/2014 05:41 PM - Stephen Benjamin

Cool!

So the smart proxy is POSTing the parameters -- so you can still POST, but just the raw parameters like:

```
param1=foo&param2=bar
```

And I'll update my side to accept that return JSON.

#28 - 02/27/2014 06:59 PM - Rob Crittenden

I checked out the other smartproxy APIs and they support JSON inputs. Is a POST even valid with no content, or are you suggesting creating a host with a GET?

#29 - 02/27/2014 07:30 PM - Stephen Benjamin

Which do you see that in?

None that I know of in the Smart Proxy are taking JSON inputs. It's the same format as doing a GET request, but you're posting the URL-encoded parameter string.

`https://stackoverflow.com/questions/14551194/how-are-parameters-sent-in-an-http-post-request`

#30 - 02/27/2014 09:24 PM - Rob Crittenden

Stephen and I hashed the question about format out in IRC, but to close the loop there is a reference to JSON at http://projects.theforeman.org/projects/smart-proxy/wiki/API

I've been testing with the same format he mentioned so we're fine.

I've hardcoded force to True.

I have a new upstream patch which adds the /feature URI and confirmed that userclass is supported:

$ curl -v http://localhost:8090/realm/example.com -X POST -d "hostname=host.example.com&userclass=foo"

#31 - 02/27/2014 11:14 PM - Stephen Benjamin

Great! What do you think about the realm name -- treat it case insensitively? In IPA the realm is uppercase - EXAMPLE.COM.

Can I give your code a try? Is it in git somewhere?

#32 - 02/28/2014 08:46 PM - Rob Crittenden

I have a COPR repo with the bits at http://copr.fedoraproject.org/coprs/rcritten/python-kerberos/

I've only tested in F-20 so far and you'll need a bunch of things from updates-testing as well. You'll also need python-qrcode which I missed in the Requires.

The initial installation failed for me with https://fedorahosted.org/freeipa/ticket/4084 which is supposed to be fixed, I'll re-open the ticket for investigation.

man ipa-smartproxy will give you what you need to set up the smart proxy post-install.

#33 - 03/03/2014 12:48 PM - Anonymous

- Target version changed from 1.9.1 to 1.9.0

#34 - 03/07/2014 09:33 AM - Stephen Benjamin

Rob - is it possible to package freeipa-server-foreman-smartproxy for previous versions of FreeIPA (and RH IdM)?

It would make it so we don't need to have two smart proxies doing the same thing. If not then I guess we'd need to keep the Foreman Smart Proxy implementation at least for a while.

#35 - 03/10/2014 05:47 PM - Rob Crittenden

No as it relies on functionality not available in previous releases, some in IPA and some in other areas of the distro. It needs a newer gss-proxy and python-kerberos, for example.

#36 - 03/11/2014 12:57 AM - Stephen Benjamin

Tested the code in the COPR repo, it works against my IPA branch for Foreman! This is awesome.

The only thing I'm a bit concerned about is the localhost requirement, I think it'd be better with client SSL auth, so then the freeipa-foreman-smartproxy could run anywhere. What do you think?

#37 - 03/11/2014 12:30 PM - Rob Crittenden

I agree but cherrypy doesn't yet support SSL client auth. There is an open bug and patch, https://bitbucket.org/cherrypy/cherrypy/issue/1001/adding-support-for-client-certificate

#38 - 03/20/2014 03:33 PM - Stephen Benjamin

One more thing needed...

we need the ability to update a host. In Foreman, a user can rebuild a server or change the Hostgroup -- so in that case, we need to re-request an OTP. I think after looking at this it's easiest to just use the "create" call.

If the smart proxy gets a new request and the server already exists, then just issue a new OTP and update the userclass.

That sound OK?

Unfortunately this needs more permissions, documented here:

https://github.com/theforeman/theforeman.org/pull/190/files?short_path=b09c3ed#diff-b09c3ed50d759f24f9f3a913a0f19e4e

#39 - 03/20/2014 05:48 PM - Rob Crittenden

By rebuild you mean re-provision right?

I think what you'd want to do is a host-disable <host> which will un-enroll it, then you can set a new password on it using host-mod. Similarly the userclass can be managed this way too.

Are you suggesting a new REST target for this?

#40 - 03/20/2014 06:02 PM - Stephen Benjamin

Exactly.

I don't think we need a new REST target...I was just using the same POST as create. I do host_find to see if it still existed, and if so calling host_mod, otherwise host_create.

Do I need to do host-disable first? It seems to work without.

#41 - 03/20/2014 06:21 PM - Stephen Benjamin

Oh, I see why to disable, since it revokes all the keytabs and things. I'll include that.

Also I noticed your proxy only accepts a downcase realm (example.com, not EXAMPLE.COM). Can you make it case insensitive? I always assumed the realm would be upper case, and I guess others might too.

#42 - 03/20/2014 06:25 PM - Stephen Benjamin

Actually, we might call the "update" method in cases where we're not reprovisioning... the user just simply updated the hostgroup for example...

#43 - 03/20/2014 07:28 PM - Rob Crittenden

Right, so how to distinguish the update vs the re-provision case?

I was actually registering the domain, not the realm, good catch. I'll fix up my version.

#44 - 03/20/2014 08:12 PM - Stephen Benjamin

We must do something similar for the Puppet certificates, since we should only blow them away on a rebuild. I'll take a look.

I can probably pass a parameter like "build=1" if the system is in build mode.

#45 - 03/21/2014 09:01 AM - Dominic Cleal

For Puppet certificates, we revoke the old cert when the host makes its request for the kickstart/provision template. Have a look at the unattended controller and host's handle_ca methods.

#46 - 03/26/2014 12:58 PM - Anonymous

- Target version changed from 1.9.0 to 1.8.4

#47 - 03/27/2014 01:32 PM - Dominic Cleal

- translation missing: en.field_release set to 4

#48 - 03/27/2014 06:32 PM - Stephen Benjamin

- Related to Feature #4917: Smart-Proxy Realm Provider for Active Directory added

#49 - 03/27/2014 06:53 PM - Dominic Cleal

- Precedes Bug #4918: Add realm commands added

#50 - 04/02/2014 10:52 AM - Anonymous

- *Status changed from Ready For Testing to Closed*
- *% Done changed from 0 to 100*

Applied in changeset 45e05273167548592e96c0c75b0e331631fbffeb.

#51 - 04/07/2014 10:41 AM - Dominic Cleal

Documentation on configuring the smart proxy: http://theforeman.org/manuals/1.5/index.html#4.3.11FreeIPARealm

Community templates have been updated, will be present in new 1.5 installations too. See:
https://github.com/theforeman/community-templates/tree/master/kickstart
https://github.com/theforeman/community-templates/blob/master/snippets/freeipa_register.erb

#52 - 04/22/2014 04:01 PM - Stephen Benjamin

API documentation updated: http://projects.theforeman.org/projects/smart-proxy/wiki/API