

Foreman - Bug #1745

If FQDN for puppetmaster starts with "puppet" Foreman strips the domain.

07/11/2012 11:51 AM - Brian Gupta

Status:	Closed	Fixed in Releases: Found in Releases: Red Hat JIRA:
Priority:	Normal	
Assignee:	Jeremy Kitchen	
Category:	Puppet integration	
Target version:	1.3.0	
Difficulty:		
Triaged:		
Bugzilla link:		
Pull request:		
Description		
<p>Historically the reason this is there because many people incidentally signed the certs on their puppet masters with just "puppet", so Ohad put this in as a workaround.</p> <p>Now that smart-proxy let's one set the "name" of the puppetmaster, I don't think we should be mess with the proxy_puppet or proxy_puppet_ca hostname.</p> <p>IE: Remove the following code from models/smart_proxy.rb</p> <pre>def to_s hostname =~ /^puppet\.\/ ? "puppet" : hostname end</pre> <p>Thoughts?</p>		
Related issues:		
Has duplicate Foreman - Bug #1060: Problem with puppet-master variable		Duplicate 07/21/2011

Associated revisions

Revision f5d4e70a - 09/02/2013 08:36 AM - Jeremy Kitchen

fixes #1745 - make puppetmaster hostname/domain stripping behaviour configurable

History

#1 - 07/11/2012 11:55 AM - Greg Sutcliffe

Seconded - let's leave the hostname that comes from the Proxy URL alone. In the future, we could extend this further, perhaps by read the dnsaltnames from the masters certificate, but for now, this is an easy fix for some unexpected behaviour.

#2 - 07/11/2012 02:37 PM - Sam Kottler

Or maybe we can just validation that the string is "puppet" and not "puppet**"

#3 - 07/11/2012 02:39 PM - Sam Kottler

Sam Kottler wrote:

Or maybe we can just validate that the string is "puppet" and not "puppet**"

#4 - 07/30/2012 01:19 PM - Sam Kottler

Just triaging this, but can we remove it?

#5 - 11/16/2012 02:24 AM - Ohad Levy

- Priority changed from High to Normal

- Target version set to Bug scrub

I think the main reason is that from puppet certname point of view:

puppet is in the cert
fqdn is in the cert
puppet.domain is not (unless your server name is puppet).

#6 - 11/16/2012 02:25 AM - Ohad Levy

- Status changed from New to Need more information

- Assignee deleted (Ohad Levy)

opinions?

#7 - 11/16/2012 03:39 AM - Brian Gupta

Personally I would change the behavior to not do any thing funky with the puppetmaster names, (which should be clear since that is what I propose in this ticket.) However, since there may be legacy installations that use this, and we probably don't want to force people to go redo all their certs, perhaps the answer is to just change the default behavior as I proposed and to create a new setting to revert to the legacy behavior. (But again leave the default "principal of least surprise.")

The other option is to poll -users, and see if anyone is relying on the legacy behavior?

-Brian

#8 - 11/16/2012 03:53 AM - Dominic Cleal

Ohad Levy wrote:

I think the main reason is that from puppet certname point of view:

puppet is in the cert
fqdn is in the cert
puppet.domain is not (unless your server name is puppet).

puppet.domain is in the list of alt names for a puppet master. I think this was always the case, but may have been introduced when they moved from certdnsnames to dns_alt_names (due to a CVE).

#9 - 11/19/2012 05:49 AM - Greg Sutcliffe

Dominic Cleal wrote:

puppet.domain is in the list of alt names for a puppet master. I think this was always the case, but may have been introduced when they moved from certdnsnames to dns_alt_names (due to a CVE).

That doesn't mean it's in your site DNS. Messing with what a user specifies in the proxy name just causes confusion. I'm happy with stripping this behaviour.

Brian has a point. However, I'm not sure how likely it is that people **rely** on this behaviour (they might use it accidentally, but how difficult is it to add a DNS record?). It seems like a lot of work to support both methods via a Setting - do we want to do that?

#10 - 11/19/2012 08:47 AM - Brian Gupta

I don't believe it's simply a matter of adding a DNS record. The behavior the original fix worked around is that the certificate needs to match the name as called. At least in some versions of puppet, the puppetmaster certname that got generated included its \$fqdn and an unqualified "puppet" string.. so if your puppetmaster's hostname was something like server1.mydomain.com and you had a DNS cname puppet.mydomain.com pointing at it, clients would need to reference it by an unqualified 'puppet' or it's actual hostname.

IE: 'server1.mydomain.com' and 'puppet' would work, but 'puppet.mydomain.com' would not.

It sounds like (from Dominic's comment) this isn't still the default behavior when creating the puppetmaster's cert, but it was definitely the behavior for many versions of puppet.

Ohad definitely implemented this for a reason (to resolve certain users' issues), so we should be careful to change this behavior without providing people a quick way to go into "legacy mode" that doesn't require generating new puppetmaster certs. (As much as I really want this change to go through, I think we do need to support a setting.)

#11 - 06/10/2013 05:13 AM - Dominic Cleal

- Status changed from Need more information to New

- Target version changed from Bug scrub to 1.3.0

Agreed, let's support both modes via a setting. I'd prefer for the default to be no change in the hostname (to match recent Puppet defaults), then changing the setting causes the domain to be stripped.

#12 - 06/10/2013 05:30 AM - Romain Vrignaud

I agree also that should be supported with a setting.

#13 - 08/17/2013 07:29 PM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Jeremy Kitchen

#14 - 08/18/2013 01:25 AM - Jeremy Kitchen

ok, so the code change was pretty trivial. I have it done, however I have 2 questions:

1) how do I make this setting available to an existing install? The code checking for the setting was being used properly, but going to the settings page it didn't show up. It only started showing up after I deleted the database and started from scratch with a rake db:migrate

2) how should we handle upgrades vs fresh installs? Dominic says the default should be no change in the hostname, and I would agree with that, but that's a change in the default behavior and a pretty quiet one which could be really frustrating at 2am :)

Thanks, and I should be able to have a PR after this is taken care of!

#15 - 08/19/2013 07:35 AM - Dominic Cleal

Jeremy Kitchen wrote:

ok, so the code change was pretty trivial. I have it done, however I have 2 questions:

1) how do I make this setting available to an existing install? The code checking for the setting was being used properly, but going to the settings page it didn't show up. It only started showing up after I deleted the database and started from scratch with a rake db:migrate

Adding a new entry to app/models/setting/*.rb will caused it to be added if the setting doesn't already exist when the application starts up. It won't need a reinstallation/migration.

2) how should we handle upgrades vs fresh installs? Dominic says the default should be no change in the hostname, and I would agree with that, but that's a change in the default behavior and a pretty quiet one which could be really frustrating at 2am :)

I'm in favour of changing the default behaviour, and ensuring it's in the upgrade notes for 1.3, though appreciate your point.

The only other idea I have is to change the default value of the setting based on whether there are any smart proxies currently registered, but since setting default values are re-evaluated and changed on each Foreman startup, this would affect new installs as well as old ones, so that's a no-go.

Thanks, and I should be able to have a PR after this is taken care of!

Thanks!

#16 - 08/19/2013 05:35 PM - Jeremy Kitchen

[PR #852](#)

#17 - 08/19/2013 05:51 PM - Dominic Cleal

- Status changed from Assigned to Ready For Testing

#18 - 09/02/2013 09:31 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset [f5d4e70a90babbb6e87cd7fd9babd88754965e26](#).