

Foreman - Bug #29407

Provisioning a host when the OS hostname is altered through DHCP splits host into 2 separate hosts

03/24/2020 09:39 PM - Damon Maria

Status: New	
Priority: Normal	
Assignee:	
Category: Host creation	
Target version:	
Difficulty:	Fixed in Releases:
Triaged: No	Found in Releases: 1.24.2
Bugzilla link:	Red Hat JIRA:
Pull request:	
Description	
<p>During provisioning a host with DHCP, if the OS hostname is altered by the response from the DHCP server (I've observed this with Ubuntu 18.04) the facts host record lookup fails to find the host and therefore creates a new one. Subsequent Puppet reports and facts will go to the new host, not the original one created by the user.</p> <p>The root cause is this code in Host::Base.import_host finding the host to apply the first facts from Puppet:</p> <pre>host = Host.find_by_certname(certname) if certname.present? host = Host.find_by_name(hostname) host = new(:name => hostname) # if no host was found, build a new one</pre> <p>The first query finds nothing because the host record in the DB does not have a certname yet. The 2nd finds nothing because the hostname in facts has been altered by the DHCP server. So a new host is created and the certname will be applied to that. Thus, that new host record will match any future calls to Host::Base.import_host.</p>	
Original description	
<p>I'm using bootdisk plugin to provision Ubuntu 18.04 hosts behind DHCP servers not managed by Foreman. I create the host in Foreman with its name and install from a generic bootdisk ISO. This correctly pulls the correct information from Puppet, installs, and completes the Foreman build process.</p> <p>But when Puppet calls in the hostname of the machine has changed from what Foreman set through preseed because it has been updated with the domain and hostname from the local DHCP server. We don't control the network this is deployed in, and Foreman doesn't setup netplan in preseed_networking_setup template. Even tho the host already exists in Foreman, and matches the certname sent by Puppet, Foreman adds a new host under the hostname fact set by the DHCP server, and the facts and Puppet report go there.</p> <p>So I end up with 2 hosts. A managed one I setup, and an unmanaged one generated by Puppet.</p> <p>I presume this is a bug? I would have thought if the certname matches an existing host then that should be used?</p> <p>I've found previous reports questioning this behaviour:</p> <ul style="list-style-type: none">• https://community.theforeman.org/t/foreman-1-6-0-certname-cn-and-hostname-fqdn/3035• https://community.theforeman.org/t/new-hosts-showing-up-with-fqdn-instead-of-certname/1403 <p>Some of those also mention the security implications which I think are fairly serious and easily exploitable in this situation.</p>	

History

#1 - 03/25/2020 03:52 AM - Damon Maria

Found following in the docs too:

create_new_host_when_facts_are_uploaded

When facts are received from Puppet or other configuration management systems, a corresponding host will be created in Foreman if the certname or hostname is unknown. When false, this behavior is disabled and facts will be discarded from unknown hosts. Default: true See also:

create_new_host_when_report_is_uploaded

create_new_host_when_report_is_uploaded

If a report is received from Puppet or other configuration management systems, a corresponding host will be created in Foreman if the hostname is unknown. When false, this behavior is disabled and reports will be discarded from unknown hosts. Default: true See also:

create_new_host_when_facts_are_uploaded

The `create_new_host_when_facts_are_uploaded` setting if not being followed. But `create_new_host_when_report_is_uploaded` does not refer to certname. Strange they are different.

#2 - 03/27/2020 08:59 AM - Lukas Zapletal

- Category set to PuppetCA

Hello, I believe you need to change templates and workflow to follow what Foreman expects. Puppet is not the only configuration management or fact source Foreman can handle, therefore hostname is used as the key when deciding what kind of host checks in. In Puppet context, client cert is used only for authorization. I guess you need to change your workflow and make sure the hostname does not get changed.

#3 - 03/27/2020 09:07 AM - Lukas Zapletal

For the record, quickly looking into the codebase we search by both clientcert and hostname:

```
host = Host.find_by_certname(certname) if certname.present?
host ||= Host.find_by_name(hostname)
host ||= new(:name => hostname) # if no host was found, build a new one
```

Are you sure your certname hasn't changed? Can you check it, run "foreman-rake console" and "Host.find("hostname").certname" and compare certname in your X509 certificate (CN).

#4 - 03/27/2020 09:46 AM - Ewoud Kohl van Wijngaarden

Can you share your puppet.conf? I'd like to know if certname is set there. My suspicion is that it isn't and a new cert is created with the new hostname.

#5 - 03/28/2020 02:19 AM - Damon Maria

For below "display2.whanganui.tasman.lan" is the hostname I setup in Foreman (name: display2, domain: whanganui.tasman.lan). However, after doing the Foreman bootdisk install I ended up with a new host "grade-display.home" that Puppet runs (facts, reports) are applied to. "grade-display" is because the DHCP server remembers an old name that MAC address had and "home" because that's the router I'm behind while working from home during lockdown.

@Lukas

Unfortunately I can't get that console command to work. No matter what I try for "hostname" I get:

```
$ sudo foreman-rake console
Loading production environment (Rails 5.2.1)
irb(main):001:0> Host.find("display2.whanganui.tasman.lan").certname
Traceback (most recent call last):
  3: from lib/tasks/console.rake:5:in `block in <top (required)>'
  2: from (irb):1
  1: from app/models/host.rb:15:in `method_missing'
ActiveRecord::RecordNotFound (Couldn't find Host::Managed with 'id'=display2.whanganui.tasman.lan [WHERE "hosts"."type" IN ('Host::Managed')])
irb(main):002:0> Host.find("grade-display.home").certname
Traceback (most recent call last):
  3: from lib/tasks/console.rake:5:in `block in <top (required)>'
  2: from (irb):2
  1: from app/models/host.rb:15:in `method_missing'
ActiveRecord::RecordNotFound (Couldn't find Host::Managed with 'id'=grade-display.home [WHERE "hosts"."type" IN ('Host::Managed')])
```

For hostname I've tried the FQDN, and just hostname without domain (didn't expect that to be it). The FQDN matches what's in the URL when viewing a host in the web UI or what's in the search when I view a host's facts. I've tried both the names above and the names of other hosts in Foreman that are working fine, same result.

@Ewoud

Here's the puppet.conf on that machine:

```
# cat /etc/puppetlabs/puppet/puppet.conf

[main]
vardir = /opt/puppetlabs/puppet/cache
logdir = /var/log/puppetlabs/puppet
```

```
rundir = /var/run/puppetlabs
ssldir = /etc/puppetlabs/puppet/ssl
```

```
[agent]
ca_server      = XXXX
certname       = display2.whanganui.tasman.lan
environment    = tannery_production
server         = XXXX
```

It's what the puppet.conf provisioning template in Foreman produced. Note: the only modification I have from standard Foreman templates is the puppet.conf template because a PR I submitted that has been merged isn't available in Foreman 1.24.2 (<https://github.com/foreman/community-templates/pull/659>).

#6 - 03/28/2020 02:24 AM - Damon Maria

Further:

```
puppetserver ca list --all
```

Lists the expected cert "display2.whanganui.tasman.lan", and not the 'imposter' one ("grade-display.home").

#7 - 03/31/2020 08:59 PM - Damon Maria

Lukas Zapletal wrote:

Are you sure your certname hasn't changed? Can you check it, run "foreman-rake console" and "Host.find("hostname").certname" and compare certname in your X509 certificate (CN).

OK. I did a bit of searching and found an alternate way of querying the host in foreman-rake console which works:

```
irb(main):002:0> Host.find_by_name("display2.whanganui.tasman.lan").certname
=> "display2.whanganui.tasman.lan"
irb(main):003:0> Host.find_by_name("grade-display.home").certname
=> "display2.whanganui.tasman.lan"
irb(main):004:0> Host.find_by_certname("display2.whanganui.tasman.lan")
=> #<Host::Managed id: 38, name: "grade-display.home", last_compile: nil, last_report: "2020-03-31 04:15:03",
updated_at: "2020-03-31 04:15:44", created_at: "2020-03-24 06:06:00", root_pass: nil, architecture_id: 1, operat
atingsystem_id: 1, environment_id: 36, ptable_id: nil, medium_id: nil, build: false, comment: "", disk: nil, i
nstalled_at: nil, model_id: 4, hostgroup_id: nil, owner_id: 4, owner_type: "User", enabled: true, puppet_ca_pr
oxy_id: 1, managed: false, use_image: nil, image_file: nil, uuid: nil, compute_resource_id: nil, puppet_proxy_
id: 1, certname: "display2.whanganui.tasman.lan", image_id: nil, organization_id: 1, location_id: 2, type: "Ho
st::Managed", otp: nil, realm_id: nil, compute_profile_id: nil, provision_method: nil, grub_pass: "", global_s
tatus: 0, lookup_value_matcher: "fqdn=grade-display.home", pxe_loader: nil, initiated_at: nil, build_errors: n
il>
irb(main):005:0> Host.find_by_name("display2.whanganui.tasman.lan")
=> #<Host::Managed id: 35, name: "display2.whanganui.tasman.lan", last_compile: nil, last_report: nil, updated
_at: "2020-03-24 06:06:13", created_at: "2020-03-24 00:59:46", root_pass: "XXXX", architecture_id: 1, operatin
gssystem_id: 1, environment_id: 14, ptable_id: 110, medium_id: 7, build: false, comment: "", disk: "", installe
d_at: "2020-03-24 06:06:13", model_id: nil, hostgroup_id: nil, owner_id: 4, owner_type: "User", enabled: true,
puppet_ca_proxy_id: 1, managed: true, use_image: nil, image_file: nil, uuid: nil, compute_resource_id: nil, pu
ppet_proxy_id: 1, certname: nil, image_id: nil, organization_id: 3, location_id: 2, type: "Host::Managed", ot
p: nil, realm_id: nil, compute_profile_id: nil, provision_method: "build", grub_pass: "XXXX", global_status: 0
, lookup_value_matcher: "fqdn=display2.whanganui.tasman.lan", pxe_loader: "iPXE Chain BIOS", initiated_at: "20
20-03-24 05:03:57", build_errors: nil>
```

So you can see the certname matches the hostname on the host I created (display2.whanganui.tasman.lan), and the same certname is put against the host created by Foreman from Puppet (grade-display.home). Note, as per above, Host.find_by_certname("display2.whanganui.tasman.lan") finds the one created by Foreman/Puppet, not the original one I created.

Is there anything else I could run to help debug this?

No, the certname was never changed. This all comes from provisioning from a bootdisk and no changes after that.

I have re-run this a couple of times with the same name (after deleting hosts in Foreman and puppetserver ca clear ...). But might try that again with a different name.

#8 - 04/01/2020 09:36 AM - Lukas Zapletal

I don't believe bootdisk has anything to do with this, you mentioned it several times but keep in mind that in bootdisk workflows you create host entry in Foreman first (giving it hostname + subnet etc) and then bootdisk is generated (or generic bootdisk is used) and it kicks off the installation.

Anyway, two hosts with the same cert name is definitely not what we want to see - in the code we do Host.find_by_certname therefore I should

probably create a unique index on that.

Can you return to the console and find `created_at` flag for both hosts, then go to production.log and try to find requests which caused these hosts to be created. Just to confirm when these were created.

#9 - 04/01/2020 06:25 PM - Damon Maria

Here's the relevant logs.

Here's the original creation of display2.whanganui.tasman.lan by me in Foreman:

```
2020-03-24T00:59:46 [I|app|9cb87aac] Started POST "/hosts" for 101.98.66.45 at 2020-03-24 00:59:46 +0000
2020-03-24T00:59:46 [I|app|9cb87aac] Processing by HostsController#create as */*
2020-03-24T00:59:46 [I|app|9cb87aac] Parameters: {"utf8"=>"", "authenticity_token"=>"MBd+st/TMuZt2XVy2WXam7
NHuyTNXfrjrv/Q65ecwqAwr4FRcD90d7NvDH5nQIEaG12vnXiU9h9r4n7ou44H9A==", "host"=>{"name"=>"display2", "organizatio
n_id"=>"3", "location_id"=>"2", "hostgroup_id"=>"", "compute_resource_id"=>"", "environment_id"=>"14", "puppet
proxy_id"=>"1", "puppet_ca_proxy_id"=>"1", "puppetclass_ids"=>[""], "managed"=>"true", "progress_report_id"=>
"[FILTERED]", "type"=>"Host::Managed", "interfaces_attributes"=>{"0"=>{"_destroy"=>"0", "type"=>"Nic::Managed"
, "mac"=>"00:90:27:e4:85:1e", "identifier"=>"", "name"=>"display2", "domain_id"=>"7", "ip"=>"", "ip6"=>"", "ma
naged"=>"1", "primary"=>"1", "provision"=>"1", "virtual"=>"0", "tag"=>"", "attached_to"=>""}}, "architecture_i
d"=>"1", "operatingsystem_id"=>"1", "provision_method"=>"build", "build"=>"1", "medium_id"=>"7", "ptable_id"=>
"110", "pxe_loader"=>"iPXE Chain BIOS", "disk"=>"", "root_pass"=>"[FILTERED]", "is_owned_by"=>"4-Users", "enab
led"=>"1", "model_id"=>"", "comment"=>"", "overwrite"=>"false"}}
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on mac 00:90:27:e4:85:1e
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on ip
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on type Nic::Managed
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on name display2.whanganui.tasman.lan
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on host_id 35
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on subnet_id
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on domain_id 7
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on attrs {}
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on provider
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on username
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on password [redacted]
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on virtual false
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on link true
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on identifier
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on tag
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on attached_to
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on managed true
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on mode balance-rr
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on attached_devices
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on bond_options
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on primary true
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on provision true
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on compute_attributes {}
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on ip6
2020-03-24T00:59:46 [I|aud|9cb87aac] Nic::Managed (69) create event on subnet6_id
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on name display2.whanganui.tasman.lan
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on root_pass $5$nrp2EzNEhzx5U6E7$VsIS17EkN.5
ajxDnYytFVtNxUEGavYsOHBrtVCAYf97
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on architecture_id 1
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on operatingsystem_id 1
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on environment_id 14
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on ptable_id 110
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on medium_id 7
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on build true
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on comment
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on disk
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on installed_at
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on model_id
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on hostgroup_id
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on owner_id 4
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on owner_type User
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on enabled true
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on puppet_ca_proxy_id 1
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on managed true
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on use_image
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on image_file
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on uuid
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on compute_resource_id
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on puppet_proxy_id 1
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on certname
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on image_id
```

```

2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on organization_id 3
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on location_id 2
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on otp
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on realm_id
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on compute_profile_id
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on provision_method build
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on grub_pass $6$Y4VYyItLUHUiWQAY$gLoKnzVGDSH
Y9/Eucu0T3ZrmlPloOHD12eh5rzinEjPtmPNmSdPFZCmhDZw8kUGxCulqOPrd04bUdjPINhnwY1
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on pxe_loader iPXE Chain BIOS
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on initiated_at
2020-03-24T00:59:46 [I|aud|9cb87aac] Host::Base (35) create event on build_errors
2020-03-24T00:59:46 [I|app|9cb87aac] Remove puppet certificate for display2.whanganui.tasman.lan
2020-03-24T00:59:46 [I|app|9cb87aac] Adding autosign entry for display2.whanganui.tasman.lan
2020-03-24T00:59:47 [I|app|9cb87aac] Processed 2 tasks from queue 'Host::Managed Post', completed 2/2
2020-03-24T00:59:47 [I|app|9cb87aac] Redirected to https://foreman.mindhive.cloud/hosts/display2.whanganui.tas
man.lan
2020-03-24T00:59:47 [I|app|9cb87aac] Completed 302 Found in 634ms (ActiveRecord: 102.8ms)

```

But gathering the create of grade-display.home got messy, It seems I had it left-over from a previous run as I went through this process multiple times trying to solve this problem. So to make things simpler I deleted grade-display.home in Foreman. Just to make sure it was setup right I tested it in the console again:

```

$ sudo -i foreman-rake console
Loading production environment (Rails 5.2.1)
irb(main):001:0> Host.find_by_certname("display2.whanganui.tasman.lan")
=> nil
irb(main):002:0> Host.find_by_name("display2.whanganui.tasman.lan").certname
=> "display2.whanganui.tasman.lan"

```

find_by_certname fails yet the Host record has a certname!

OK, so that would obviously cause this bug. Is this an index issue or something since I ended up with 2 hosts with the same certname?

Just to prove it out I then ran "puppet agent -t" on the machine to watch what happens:

```

# puppet agent -t
Notice: Local environment: 'tannery_production' doesn't match server specified node environment 'tannery_swarm', switching agent to 'tannery_swarm'.
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Retrieving locales
Info: Loading facts
Notice: Local environment: 'tannery_swarm' doesn't match server specified environment 'tannery_production', re starting agent run with environment 'tannery_production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Retrieving locales
Info: Loading facts
Info: Caching catalog for display2.whanganui.tasman.lan
Info: Applying configuration version '94ba5ef6f4ad2ac5c3b38860f084c66f0871b947'
...
Notice: Applied catalog in 20.80 seconds

```

I'm currently testing a feature branch in R10K and so while the puppet.conf on the machine specifies an environment of tannery_production (as was setup by Foreman during provisioning) in Foreman now display2.whanganui.tasman.lan is set to the environment tannery_swarm. I'm used to seeing the notice in Puppet of "switching agent" but I've never seen "restarting agent run with environment". So it appears at first Foreman found the correct host (how else did it get the new environment of tannery_swarm), but then Foreman created a new host which meant Foreman no longer wanted to override the Puppet provided environment and so Puppet restarted.

Here's the production.log for the same time:

```

2020-04-01T17:46:39 [I|app|c3689514] Started GET "/node/display2.whanganui.tasman.lan?format=yml" for 172.31.84.205 at 2020-04-01 17:46:39 +0000
2020-04-01T17:46:39 [I|app|c3689514] Processing by HostsController#externalNodes as YAML
2020-04-01T17:46:39 [I|app|c3689514] Parameters: {"name"=>"display2.whanganui.tasman.lan"}
2020-04-01T17:46:39 [I|app|c3689514] Rendering text template
2020-04-01T17:46:39 [I|app|c3689514] Rendered text template (0.0ms)
2020-04-01T17:46:39 [I|app|c3689514] Completed 200 OK in 163ms (Views: 0.4ms | ActiveRecord: 54.5ms)
2020-04-01T17:46:54 [I|app|c5f33e37] Started POST "/api/hosts/facts" for 172.31.84.205 at 2020-04-01 17:46:54 +0000
2020-04-01T17:46:54 [I|app|c5f33e37] Processing by Api::V2::HostsController#facts as JSON
2020-04-01T17:46:54 [I|app|c5f33e37] Parameters: {"facts"=>"[FILTERED]", "name"=>"grade-display.home", "cert

```

```

name"=>"display2.whanganui.tasman.lan", "apiv"=>"v2", "host"=>{"certname"=>"display2.whanganui.tasman.lan", "name"=>"grade-display.home"}}
2020-04-01T17:46:54 [I|app|c5f33e37] Import facts for 'grade-display.home' completed. Added: 462, Updated: 0, Deleted 0 facts
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on mac
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on ip
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on type Nic::Managed
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on name grade-display.home
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on host_id 39
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on subnet_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on domain_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on attrs {}
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on provider
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on username
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on password [redacted]
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on virtual false
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on link true
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on identifier
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on tag
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on attached_to
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on managed true
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on mode balance-rr
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on attached_devices
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on bond_options
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on primary true
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on provision true
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on compute_attributes {}
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on ip6
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) create event on subnet6_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on name grade-display.home
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on root_pass
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on architecture_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on operatingsystem_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on environment_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on ptable_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on medium_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on build false
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on comment
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on disk
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on installed_at
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on model_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on hostgroup_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on owner_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on owner_type
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on enabled true
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on puppet_ca_proxy_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on managed false
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on use_image
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on image_file
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on uuid
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on compute_resource_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on puppet_proxy_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on certname display2.whanganui.tasman.lan
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on image_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on organization_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on location_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on otp
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on realm_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on compute_profile_id
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on provision_method
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on grub_pass
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on pxe_loader
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on initiated_at
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on build_errors
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) update event on mac , 00:90:27:e4:85:1e
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) update event on domain_id , 34
2020-04-01T17:46:57 [I|aud|c5f33e37] Nic::Managed (76) update event on identifier , enp2s0
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) update event on architecture_id , 1
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) update event on operatingsystem_id , 1
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) update event on environment_id , 14
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) update event on model_id , 4
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) update event on puppet_ca_proxy_id , 1
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) update event on puppet_proxy_id , 1
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) update event on organization_id , 1
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) update event on location_id , 2

```

```

2020-04-01T17:46:57 [I|app|c5f33e37] Completed 201 Created in 3095ms (Views: 1.3ms | ActiveRecord: 1951.6ms)
2020-04-01T17:46:57 [I|app|65575b35] Started GET "/node/display2.whanganui.tasman.lan?format=yml" for 172.31.84.205 at 2020-04-01 17:46:57 +0000
2020-04-01T17:46:57 [I|app|65575b35] Processing by HostsController#externalNodes as YAML
2020-04-01T17:46:57 [I|app|65575b35] Parameters: {"name"=>"display2.whanganui.tasman.lan"}
2020-04-01T17:46:57 [I|app|65575b35] Rendering text template
2020-04-01T17:46:57 [I|app|65575b35] Rendered text template (0.0ms)
2020-04-01T17:46:57 [I|app|65575b35] Completed 200 OK in 109ms (Views: 0.4ms | ActiveRecord: 37.5ms)
2020-04-01T17:47:12 [I|app|b163ed98] Started POST "/api/hosts/facts" for 172.31.84.205 at 2020-04-01 17:47:12 +0000
2020-04-01T17:47:12 [I|app|b163ed98] Processing by Api::V2::HostsController#facts as JSON
2020-04-01T17:47:12 [I|app|b163ed98] Parameters: {"facts"=>"[FILTERED]", "name"=>"grade-display.home", "certname"=>"display2.whanganui.tasman.lan", "apiv"=>"v2", "host"=>{"certname"=>"display2.whanganui.tasman.lan", "name"=>"grade-display.home"}}
2020-04-01T17:47:13 [I|app|b163ed98] Import facts for 'grade-display.home' completed. Added: 0, Updated: 12, Deleted 0 facts
2020-04-01T17:47:13 [I|app|b163ed98] Completed 201 Created in 934ms (Views: 1.2ms | ActiveRecord: 536.6ms)
2020-04-01T17:47:13 [I|app|34ac6311] Started GET "/node/display2.whanganui.tasman.lan?format=yml" for 172.31.84.205 at 2020-04-01 17:47:13 +0000
2020-04-01T17:47:13 [I|app|34ac6311] Processing by HostsController#externalNodes as YAML
2020-04-01T17:47:13 [I|app|34ac6311] Parameters: {"name"=>"display2.whanganui.tasman.lan"}
2020-04-01T17:47:13 [I|app|34ac6311] Rendering text template
2020-04-01T17:47:13 [I|app|34ac6311] Rendered text template (0.0ms)
2020-04-01T17:47:13 [I|app|34ac6311] Completed 200 OK in 110ms (Views: 0.4ms | ActiveRecord: 39.1ms)

```

And so the grade-display.home host is created again.

#10 - 04/03/2020 11:54 AM - Lukas Zapletal

I know this could look really weird:

```

irb(main):001:0> Host.find_by_certname("display2.whanganui.tasman.lan")
=> nil
irb(main):002:0> Host.find_by_name("display2.whanganui.tasman.lan").certname
=> "display2.whanganui.tasman.lan"

```

But this can be taxonomy scope, can you try with `Host.unscoped.find_by_certname("display2.whanganui.tasman.lan")` ?

#11 - 04/04/2020 12:14 AM - Damon Maria

That host has since checked in again through Puppet and so been recreated. As such I get:

```

irb(main):002:0> Host.unscoped.find_by_certname("display2.whanganui.tasman.lan").hostname
=> "grade-display.home"

```

If I delete grade-display.home, leaving just the host I created, and try again:

```

irb(main):004:0> Host.unscoped.find_by_certname("display2.whanganui.tasman.lan")
=> nil
irb(main):005:0> Host.find_by_name("display2.whanganui.tasman.lan").certname
=> "display2.whanganui.tasman.lan"

```

So it still can't find it with "unscoped".

#12 - 04/06/2020 01:46 PM - Lukas Zapletal

Can you please do this:

```
Host.unscoped.where(certname: "hostname").all
```

I am not Rails expert, someone help me here.

#13 - 04/06/2020 09:43 PM - Damon Maria

```

irb(main):002:0> Host.unscoped.where(certname: "display2.whanganui.tasman.lan").all
=> #<ActiveRecord::Relation [#<Host::Managed id: 42, name: "grade-display.home", last_compile: nil, last_report: "2020-04-06 09:26:45", updated_at: "2020-04-06 09:27:16", created_at: "2020-04-05 06:02:38", root_pass: nil, architecture_id: 1, operatingsystem_id: 1, environment_id: 14, ptable_id: nil, medium_id: nil, build: false, comment: nil, disk: nil, installed_at: nil, model_id: 4, hostgroup_id: nil, owner_id: nil, owner_type: nil, enabled: true, puppet_ca_proxy_id: 1, managed: false, use_image: nil, image_file: nil, uuid: nil, compute_resource_id: nil, puppet_proxy_id: 1, certname: "display2.whanganui.tasman.lan", image_id: nil, organization_id: 1,

```

```
location_id: 2, type: "Host::Managed", otp: nil, realm_id: nil, compute_profile_id: nil, provision_method: nil, grub_pass: "", global_status: 0, lookup_value_matcher: "fqdn=grade-display.home", pxe_loader: nil, initiate_d_at: nil, build_errors: nil]>
irb(main):004:0> Host.unscoped.find_by_name("display2.whanganui.tasman.lan").certname
=> "display2.whanganui.tasman.lan"
```

#14 - 04/08/2020 11:18 AM - Lukas Zapletal

Sorry I meant to do this similarly as you did with the above:

```
> Host.unscoped.find_by_certname("display2.whanganui.tasman.lan")
> Host.find_by_name("display2.whanganui.tasman.lan").certname
```

Therefore:

```
> Host.unscoped.where(certname: "display2.whanganui.tasman.lan").all
> Host.find_by_name("display2.whanganui.tasman.lan").certname
```

#15 - 04/08/2020 12:50 PM - Damon Maria

Same result:

```
irb(main):003:0> Host.unscoped.where(certname: "display2.whanganui.tasman.lan").all
=> #<ActiveRecord::Relation [#<Host::Managed id: 42, name: "grade-display.home", last_compile: nil, last_report: "2020-04-07 08:11:47", updated_at: "2020-04-07 08:12:18", created_at: "2020-04-05 06:02:38", root_pass: nil, architecture_id: 1, operatingsystem_id: 1, environment_id: 14, ptable_id: nil, medium_id: nil, build: false, comment: nil, disk: nil, installed_at: nil, model_id: 4, hostgroup_id: nil, owner_id: nil, owner_type: nil, enabled: true, puppet_ca_proxy_id: 1, managed: false, use_image: nil, image_file: nil, uuid: nil, compute_resource_id: nil, puppet_proxy_id: 1, certname: "display2.whanganui.tasman.lan", image_id: nil, organization_id: 1, location_id: 2, type: "Host::Managed", otp: nil, realm_id: nil, compute_profile_id: nil, provision_method: nil, grub_pass: "", global_status: 0, lookup_value_matcher: "fqdn=grade-display.home", pxe_loader: nil, initiate_d_at: nil, build_errors: nil]>
irb(main):004:0> Host.find_by_name("display2.whanganui.tasman.lan").certname
=> "display2.whanganui.tasman.lan"
```

But Maybe you mean delete the 'Puppet generated' host (grade-display.home) as before. If I do that and try again:

```
irb(main):005:0> Host.unscoped.where(certname: "display2.whanganui.tasman.lan").all
=> #<ActiveRecord::Relation []>
irb(main):006:0> Host.find_by_name("display2.whanganui.tasman.lan").certname
=> "display2.whanganui.tasman.lan"
```

#16 - 04/17/2020 09:47 PM - Damon Maria

Hi Lukas Zapletal.

I will have this machine behind the DHCP server that triggers this problem until around this coming Thursday or Friday. If there are anymore tests you want me to perform to get to the bottom of it then please let me know. I'm happy to work through it with you and the Foreman team.

#17 - 04/24/2020 01:30 PM - Lukas Zapletal

Hello, I am out of ideas honestly, puppet is not my knowledge domain but I was interested because this really looks weird. Let me start a thread on our community site about this.

#18 - 04/27/2020 01:08 PM - Lukas Zapletal

Ok Tomer had a good point in <https://community.theforeman.org/t/activerecord-not-finding-a-record/18401>

Please do this:

```
Host.find_by_certname("display2.whanganui.tasman.lan")
Host.find_by_name("display2.whanganui.tasman.lan")
Host.find_by_name("display2.whanganui.tasman.lan")[:certname]
Host.find_by_name("display2.whanganui.tasman.lan")[:name]
```

It looks like certname is not set at all, we have a fallback to use "name" instead. This is confusing.

#19 - 04/27/2020 10:43 PM - Damon Maria

That is exactly the reason:

```
irb(main):003:0> Host.find_by_name("display2.whanganui.tasman.lan")[:certname]
```



```
=> nil
irb(main):004:0> Host.find_by_name("display2.whanganui.tasman.lan")[:name]
=> "display2.whanganui.tasman.lan"
```

So, back to the base problem. This is a breakdown of the Foreman log (above in this issue) when Foreman erroneously creates the new host during a puppet run.

First there is what I assume is the ENC request for Puppet to determine the environment:

```
2020-04-01T17:46:39 [I|app|c3689514] Started GET "/node/display2.whanganui.tasman.lan?format=yml" for 172.31.84.205 at 2020-04-01 17:46:39 +0000
2020-04-01T17:46:39 [I|app|c3689514] Processing by HostsController#externalNodes as YAML
2020-04-01T17:46:39 [I|app|c3689514] Parameters: {"name"=>"display2.whanganui.tasman.lan"}
2020-04-01T17:46:39 [I|app|c3689514] Rendering text template
2020-04-01T17:46:39 [I|app|c3689514] Rendered text template (0.0ms)
2020-04-01T17:46:39 [I|app|c3689514] Completed 200 OK in 163ms (Views: 0.4ms | ActiveRecord: 54.5ms)
```

Foreman must find the correct host here because Puppet reports "'tannery_production' doesn't match server specified node environment 'tannery_swarm', switching agent to 'tannery_swarm'". The new environment (tannery_swarm) has come from the setting on the correct host in Foreman.

Next comes the facts which creates the new host, even tho the passed certname matches the name of the existing host:

```
2020-04-01T17:46:54 [I|app|c5f33e37] Started POST "/api/hosts/facts" for 172.31.84.205 at 2020-04-01 17:46:54 +0000
2020-04-01T17:46:54 [I|app|c5f33e37] Processing by Api::V2::HostsController#facts as JSON
2020-04-01T17:46:54 [I|app|c5f33e37] Parameters: {"facts"=>"[FILTERED]", "name"=>"grade-display.home", "certname"=>"display2.whanganui.tasman.lan", "apiv"=>"v2", "host"=>{"certname"=>"display2.whanganui.tasman.lan", "name"=>"grade-display.home"}}
2020-04-01T17:46:54 [I|app|c5f33e37] Import facts for 'grade-display.home' completed. Added: 462, Updated: 0, Deleted 0 facts
...
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on name grade-display.home
...
2020-04-01T17:46:57 [I|aud|c5f33e37] Host::Base (39) create event on certname display2.whanganui.tasman.lan
...
2020-04-01T17:46:57 [I|app|c5f33e37] Completed 201 Created in 3095ms (Views: 1.3ms | ActiveRecord: 1951.6ms)
```

Next comes another ENC request, which Foreman must match to the new host it just created:

```
2020-04-01T17:46:57 [I|app|65575b35] Started GET "/node/display2.whanganui.tasman.lan?format=yml" for 172.31.84.205 at 2020-04-01 17:46:57 +0000
2020-04-01T17:46:57 [I|app|65575b35] Processing by HostsController#externalNodes as YAML
2020-04-01T17:46:57 [I|app|65575b35] Parameters: {"name"=>"display2.whanganui.tasman.lan"}
2020-04-01T17:46:57 [I|app|65575b35] Rendering text template
2020-04-01T17:46:57 [I|app|65575b35] Rendered text template (0.0ms)
2020-04-01T17:46:57 [I|app|65575b35] Completed 200 OK in 109ms (Views: 0.4ms | ActiveRecord: 37.5ms)
```

So the cause has to be Foreman not finding the existing host when the first facts are sent by Puppet. Foreman logs in that request:

```
"name"=>"grade-display.home", "certname"=>"display2.whanganui.tasman.lan"
```

So it's given the correct certname, wrong hostname. The queries at the top of this comment tell us the host it should find has the name of "display2.whanganui.tasman.lan", but a nil certname (makes sense since this is while we're building the host).

Going through the code I end up in Host::Base.import_host which searches as so:

```
host = Host.find_by_certname(certname) if certname.present?
host ||= Host.find_by_name(hostname)
host ||= new(:name => hostname) # if no host was found, build a new one
```

So given this logic it would fail to find the existing host as only the passed certname matches the host name. Shouldn't it also search for hosts where host name = certname, possibly with the extra requirement that the host does not have a certname? IMHO this would come as the 2nd check (before Host.find_by_name) as certname can't be altered / faked at the agent end and is more secure.

Just to re-cap how to trigger this: provisioning a host with DHCP when the OS hostname is altered by the DHCP server will result in this situation.

#20 - 04/28/2020 07:24 AM - Lukas Zapletal

Nice analysis.

Shouldn't it also search for hosts where host name = certname, possibly with the extra requirement that the host does not have a certname?

Can you provide some (pseudo) code? If you mean to search also for a host which has certname set to nil and its name matches the certname (which was verified by X509) then I think we could do that. However if you mean to search for anything based on name (arbitrary input, not part of X509 chain) then that would be a security problem.

Ewoud what you think?

#21 - 04/28/2020 11:16 AM - Damon Maria

Nice analysis.

The advantages of open source :)

Shouldn't it also search for hosts where host name = certname, possibly with the extra requirement that the host does not have a certname?

Can you provide some (pseudo) code? If you mean to search also for a host which has certname set to nil and its name matches the certname (which was verified by X509) then I think we could do that.

Yes, exactly that. Although I'm not sure also requiring a nil certname is required, I was just being cautious.

I've never used ActiveRecord so don't know how it should look. But something like:

```
host = Host.find_by_certname(certname) if certname.present?  
host ||= Host.find_by_name(certname) if certname.present? # <- possibly also requiring record's certnam  
e is nil? Otherwise it will overwrite the certname when updating from facts?  
host ||= Host.find_by_name(hostname) # <- but does the same logic apply here? record's certname should  
be nil? And/or this call should be guarded with "unless certname.present?"  
host ||= new(:name => hostname)
```

However if you mean to search for anything based on name (arbitrary input, not part of X509 chain) then that would be a security problem.

Totally agree. I would prefer if certname was supplied then only that was used. But understand that would be a breaking change.

#22 - 04/28/2020 11:33 AM - Damon Maria

I haven't seen the logic used when a host record is looked up during the ENC API call but this lookup for fact updating needs to be consistent with that. Whichever host record the ENC call finds, the facts needs to find the same one. At the moment it doesn't. Just something to consider.

#23 - 04/28/2020 10:13 PM - Damon Maria

Apologies for the stream of thoughts.

Why is certname not set on the host record when it is first created (if a Puppet CA is specified)? The certname is known beforehand. And it would avoid these issues.

Or is it that certname being nil represents a state? Like that the host hasn't been signed by the CA yet or something?

#24 - 05/30/2020 12:16 PM - Damon Maria

- Subject changed from Provisioning a host with DHCP half-applies to a generated host from DHCP provided name, not built host to Provisioning a host when the OS hostname is altered through DHCP splits host into 2 separate hosts

- Description updated

- Category changed from PuppetCA to Host creation

Lukas Zapletal wrote:

Ewoud what you think?

Just giving this a bump, as the root cause has been found, and I gather it definitely is a bug. Who should be assigned?

I've updated the description with the root cause found.

#25 - 06/02/2020 07:33 AM - Lukas Zapletal

Just go ahead and do the patch, test it on your instance and send a PR, we will surely review it. It must pass all tests and it must work.

#26 - 06/14/2020 12:39 AM - Damon Maria

Lukas Zapletal wrote:

Just go ahead and do the patch, test it on your instance and send a PR, we will surely review it. It must pass all tests and it must work.

I actually think the 'cleanest' approach would be to set the certname on the host (maybe when it's put into build mode). It seems strange that certname is currently filled in from Puppet facts when the most secure way to look up the host is by certname. Otherwise issues like this can arise.

But this is the kind of change that could have implications far beyond what I can think of.