Foreman - Bug #1938

Foreman shouldn't use the FQDN fact to identify the node when facts are uploaded

11/14/2012 04:47 AM - Nacho Barrientos

Status:	Closed		
Priority:	Normal		
Assignee:	Amos Benari		
Category:	Facts		
Target version:	1.2.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Hi,

When new facts are uploaded to Foreman, at some point models/host.rb:importHostAndFacts is executed. That function relies on certname and fqdn facts as keys to fetch the host from Foreman's database. This is dangerous because a malicious user with root privileges on a puppet managed machine could do as follows:

- Modify puppet.conf to remove certname directive
- Tweak facter to return a different value for the FQDN fact (target's machine for instance)

in order to change the facts of a different machine.

Example:

Chuck has root access on machine ibsltestw0.example.org and wants to replace fact "uptime_seconds" on Foreman for machine ibsltestm0.example.org (owned by Alice), so Chuck follows the procedure above (he fakes FQDN and uptime_seconds facts) and runs Puppet agent. Crafted facts are uploaded to the Puppet master:

```
puppetmaster /var/lib/puppet/yaml/facts # grep fqdn ibsltest*
ibsltestm0.example.org.yaml:    fqdn: ibsltestm0.example.org
ibsltestw0.example.org.yaml:    fqdn: ibsltestm0.example.org <-- this is not good for Foreman

puppetmaster /var/lib/puppet/yaml/facts  # grep uptime_seconds ibsltest*
ibsltestm0.example.org.yaml:    uptime_seconds: "9965187"
ibsltestw0.example.org.yaml:    uptime_seconds: "666"
```

Before the catalog is compiled, the master executes Foreman's ENC to upload ibsltestw0's new set of facts to Foreman and also to get the node's classification data. There is no certname fact, so Foreman uses the FQDN fact (which value is ibsltestm0.example.org) as a key to get a host instance.

```
      when Puppet::Node::Facts
        certname = facts.values["certname"]
        name     = facts.values["fqdn"]
        values   = facts.values
      when Hash
        certname = facts["certname"]
        name     = facts["fqdn"]
        values   = facts
[...]
    if name == certname or certname.nil?
      h = Host.find_by_name name
    else
```

so ibsltestm0's facts are replaced:

```
$ curl -s -k -L --cookie ssocookie-foreman.txt https://foreman.example.org/hosts/ibsltestm0.exampl
e.org/facts -H "Content-Type:application/json" -H "Accept:application/json" | grep -q '"uptime_sec
```

```
onds":"666"' && echo "facts injection proven"
facts injection proven
```

Proposed fix:

The serialization of the object type Puppet::Node::Facts looks like this:

```
--- !ruby/object:Puppet::Node::Facts
  expiration: 2012-11-12 15:58:08.153312 +01:00
  name: ibsltestm0.example.org
  values:
    [more facts here]
    fqdn: ibsltestm0.example.org
    [more facts here]
```

AFAIK, the top level key 'name' is set by the Puppet master based on the common name of the certificate associated with the node. That's data that can't be tampered agent-side and a good candidate to safely identify the node trying to replace the facts.

If an object with Hash type is received (second case) I can't think of any way to be sure what is the hostname of the node being modified. Maybe in that case we should delegate to Foreman's administrator via a config option the decision of allowing facts replacements based on the FQDN fact.

Related issues:

Related to Foreman - Feature #1843: Accept a simple hash of facts to work wit...	**Closed**	**08/30/2012**

Associated revisions

Revision baeb54f1 - 06/10/2013 05:56 AM - Amos Benari

fixes #1938 Foreman shouldn't use the FQDN fact to identify the node when facts are uploaded

Revision 1cb4a2a4 - 06/11/2013 10:27 AM - Amos Benari

fixes #1938 Foreman shouldn't use the FQDN fact to identify the node when facts are uploaded
(cherry picked from commit baeb54f19a67ef8e5fbce513548cda1653341e17)

History

#1 - 04/11/2013 02:08 PM - Dominic Cleal

- Category set to Facts

- Target version set to 1.2.0

#2 - 05/13/2013 11:44 AM - Mikael Fridh

Confirmed; on puppet 2.6.12 etc the following is true about the Puppet::Node::Facts object (Meaning, the following is true in the cases I observed):

- 'certname' fact is never set (even if certname = foo.bar.baz in puppet.conf)
- There is a 'clientcert' fact

But that's irrelevant anyway, should use the top-level facts.name key instead as suggested here.

I had to patch my Foreman 1.1 to do exactly this today since I have explicitly configured (clientcert<=>fqdn mismatching) certname = in most of my puppet agents.

#3 - 05/13/2013 11:53 AM - Mikael Fridh

clientcert facts gets set from the certname setting in Puppet 2.6.x to 3.1.x. 0.24.x doesn't seem to have any such facts:
https://github.com/puppetlabs/puppet/blob/master/lib/puppet/node/facts.rb#L29

Why are we pulling the certname fact again?

#4 - 06/06/2013 06:42 AM - Amos Benari

- Status changed from New to Assigned

- Assignee set to Amos Benari

#5 - 06/10/2013 06:17 AM - Amos Benari

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

Applied in changeset baeb54f19a67ef8e5fbce513548cda1653341e17.