Foreman - Feature #1069

Unattended install behind firewall and built status

07/26/2011 10:31 AM - NoName NoSurname

Status:	Closed		
Priority:	Normal		
Assignee:	Greg Sutcliffe		
Category:	Unattended installations		
Target version:	1.1		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Hello,

It would be nice if we can build machines behind firewall. The problem is that, today, the Kickstart will send, at the end, a wget "built" information to foreman server. But if the machine is behind a firewall, foreman will not know from who this request come as he only see the FW IPs.

Is that possible ?

Thanks

Related issues:

Related to Smart Proxy - Feature #969: Direct Client->Foreman communication s...	**Closed**	**06/09/2011**
Has duplicate Foreman - Bug #1059: Post Centos install build information to f...	**Duplicate**	**07/21/2011**

Associated revisions

Revision 81159d4b - 10/04/2012 11:14 AM - Greg Sutcliffe

Use tokens for discovery of host identity during installation

- fixes #1069
- fixes #1720
- refs #969

History

#1 - 08/02/2011 06:31 PM - Corey Osman

I dont' know much about the provisioning aspect of foreman but it seems the following URL works great when foreman is on the same network.

http://foreman:3000/unattended/built (IP is inspected to verify build was successful)

However, in situations where NAT is used I think we should be relying on a url scheme rather than inspected IP packets.
This method would allow for any system in any network to send the built ack to foreman with worrying about NAT.

http://foreman:3000/unattended/fqdn/built

#2 - 08/03/2011 02:21 AM - Ohad Levy

Corey Osman wrote:

> However, in situations where NAT is used I think we should be relying on a url scheme rather than inspected IP packets.
> This method would allow for any system in any network to send the built ack to foreman with worrying about NAT.

My main concern here is security... since this is a non authenticated call.

I'm more then open for suggestion of how to identify the requesting machine...

#3 - 08/03/2011 08:48 AM - Marcello de Sousa

Following the same line as suggested in #969 - Direct Client->Foreman communication shouldn't be needed (and moved to the Proxy)

We would have to figure out exactly how, but the client server should never really need to contact Foreman directly (I want to have my Foreman firewalled) and IMHO this "Built acknoledgement" should also be moved to the proxy .

#4 - 10/20/2011 03:53 PM - Corey Osman

well i would do something like this: wget -q -O /dev/null --no-check-certificate https://foreman/unattended/built/$UUID
where $UUID is a random string shared with the client at the time the provision file is generated. So in the provision file the wget -q -O /dev/null --no-check-certificate https://foreman/unattended/built/$UUID line would be unique each time.

This would help with not relying on a specific IP to be present and instead a hard coded Mac address and UUID.

#5 - 07/03/2012 09:03 AM - Ohad Levy

we can simply use a unique secure uuid to identify the system, very similar to how puppet certnames work.

#6 - 10/04/2012 11:15 AM - Ohad Levy

- Category set to Unattended installations

- Assignee set to Greg Sutcliffe

- Target version set to 1.1

#7 - 10/04/2012 01:25 PM - Anonymous

- Status changed from New to Closed

- % Done changed from 0 to 100

Applied in changeset 81159d4bf8355ab2fac1813127fccf60baf75fbc.