Foreman - Bug #16853

SSH Host Keys Not Uploaded When Joining IPA Realm

10/10/2016 02:56 PM - Jason Nance

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Realm		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

When provisioning a new host that is to be joined to a FreeIPA realm the host's SSH public keys are not uploaded to IPA.

History

#1 - 10/10/2016 03:02 PM - Jason Nance

This may be an issue with the process that TFM is using to join the hosts to the realm. My understanding is that TFM adds a host entry in order to get a 1-time registration password and that password is then passed to ipa-client-install when the host is provisioned (in the IPA kickstart snippet). I believe that the installation client only submits the keys if a host entry doesn't exist.

Possibly related:

https://fedorahosted.org/freeipa/ticket/2655

#2 - 10/11/2016 02:56 AM - Dominic Cleal

- Category set to Realm

#3 - 11/28/2016 06:21 PM - Jason Nance

With help from the mailing list this has been tracked down to:

https://access.redhat.com/solutions/1320523

I resolved this by creating a kickstart snipped "generate_ssh_host_keys" with the following content:

```
<%#
kind: snippet
name: generate_ssh_host_keys
%>
# Call this during post to force creation of SSH host keys so that IPA registration uploads them
# https://access.redhat.com/solutions/1320523
<% if @host.operatingsystem.major.to_i < 7 -%>
/usr/bin/ssh-keygen -q -t rsa -f /etc/ssh/ssh_host_rsa_key -C '' -N ''
chmod 600 /etc/ssh/ssh_host_rsa_key
chmod 644 /etc/ssh/ssh_host_rsa_key.pub
/sbin/restorecon /etc/ssh/ssh_host_rsa_key.pub

/usr/bin/ssh-keygen -q -t ecdsa -f /etc/ssh/ssh_host_ecdsa_key -C '' -N ''
chmod 600 /etc/ssh/ssh_host_ecdsa_key
chmod 644 /etc/ssh/ssh_host_ecdsa_key.pub
/sbin/restorecon /etc/ssh/ssh_host_ecdsa_key.pub
<% else -%>
# By default this creates RSA, ECDSA, and ED25519 keys
/usr/sbin/sshd-keygen
<% end -%>
```

I then updated my copy of "Kickstart Default" and changed:

```
<% if @host.info['parameters']['realm'] && @host.realm && @host.realm.realm_type == 'FreeIPA' -%>
<%= snippet "freeipa_register" %>
<% end -%>
```

To:

```
<% if @host.info['parameters']['realm'] && @host.realm && @host.realm.realm_type == 'FreeIPA' -%>
<%= snippet "generate_ssh_host_keys" %>
<%= snippet "freeipa_register" %>
<% end -%>
```

I understand if you don't consider this a Foreman bug and close it. It would be nice if the changes outlined above were included in the default snippets/kickstart (it may need a bit of tweaking to support Fedora).

Note that my version of the host key generation for EL 6 and lower only creates RSA and ECDSA keys. I believe the default is to create RSA, RSA1, and DSA (at least according to the KB article referenced).