FreeNAS - Bug #8773

SSH keys regenerated on first reboot after enabling SSH

03/20/2015 04:25 PM - Peter C

Status:	Resolved		
Priority:	Nice to have		
Assignee:	Xin Li		
Category:	OS		
Target version:	N/A		
Seen in:	9.3-RELEASE	**Needs Merging:**	Yes
Severity:	New	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	Yes	**ChangeLog Required:**	No
Needs Doc:	Yes		

Description

When first enabling SSH, host keys are generated, and the generation is shown in /var/log/messages (but not on console).

However, upon the subsequent reboot, SSH host keys are again generated, which gets logged on the console only (but not in /var/log/messages). From then on, this second set of keys persists across reboots.

At any given point in time, the current SSH host keys can be checked either by connecting via SSH or by "ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub" (for the RSA key). Prior to reboot, it shows the first set of keys. After reboot, it shows the second.

If you happen to be unfortunate enough to confirm your host keys on your admin clients before that first reboot, you'll be very surprised when you next try to SSH and are warned that the host keys have changed, with no mention of the change in the server's log files...

To reproduce:
1) Install
2) Enable SSH
3) Check the SSH keys (/var/log/messages, ssh-keygen or ssh)
4) Reboot and watch the console after ntpd is started, you'll briefly see the keys being regenerated
5) Confirm the new SSH keys (ssh-keygen or ssh)
6) Reboot, no SSH keys are generate when starting sshd.
7) Confirm the new SSH keys have persisted

Associated revisions

Revision 72271093 - 03/25/2015 01:48 PM - Xin Li

Save SSH host keys after starting SSH.

Ticket: #8773

Revision 07716062 - 03/25/2015 01:49 PM - Xin Li

Save SSH host keys after starting SSH.

Ticket: #8773
(cherry picked from commit 722710931b11dca0bd8922eebdb6457e47ddaa22)

Revision af57701b - 03/25/2015 01:49 PM - Xin Li

Save SSH host keys after starting SSH.

Ticket: #8773
(cherry picked from commit 722710931b11dca0bd8922eebdb6457e47ddaa22)

History

#1 - 03/21/2015 01:15 PM - Jordan Hubbard

- Category set to 81

- Assignee set to Xin Li

- Target version set to Unspecified

#2 - 03/25/2015 01:49 PM - Xin Li

- Status changed from Unscreened to Ready For Release

#3 - 03/27/2015 06:25 PM - Jordan Hubbard

- Status changed from Ready For Release to Resolved

#4 - 08/26/2016 01:45 PM - Kris Moore

- Target version changed from Unspecified to N/A