FreeNAS - Bug #25645

Fix sshd config generation

08/22/2017 10:51 AM - Vladimir Vinogradenko

Status:	Resolved		
Priority:	Nice to have		
Assignee:	Vladimir Vinogradenko		
Category:	Middleware		
Target version:	11.1-BETA1		
Seen in:	11.0-U2	**Needs Merging:**	Yes
Severity:	New	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	No	**ChangeLog Required:**	No
Needs Doc:	Yes		

Description

If user does not specify «Extra options:» in SSH service configuration, he gets:

```
Protocol 2
UseDNS no
ChallengeResponseAuthentication no
ClientAliveCountMax 3
ClientAliveInterval 15
NoneEnabled yes
VersionAddendum none
...
```

But if he adds something as simple as

```
# Comment
```

in there, he gets:

```
Protocol 2
UseDNS no
ChallengeResponseAuthentication no
ClientAliveCountMax 3
ClientAliveInterval 15
NoneEnabled yes
Ciphers +aes128-cbc
...
```

Note that VersionAddendum none is gone, but Ciphers +aes128-cbc appeared.

This occurs because of code duplication in https://github.com/freenas/freenas/blob/master/src/freenas/etc/ix.rc.d/ix-sshd#L40. It can lead to various errors during fixes. E.g. commit https://github.com/freenas/freenas/commit/d0eab1441ac79deba5406ddb91b3faa9f7389382 changes only branch 1 while commit https://github.com/freenas/freenas/commit/d092075f96 changes only branch 2. For service as important as sshd this may someday lead to vulnerability.

Related issues:

Related to FreeNAS - Bug #20044: SFTP backup from CUCM 10.5.2.12900-14 fails ...	**Resolved**	**01/05/2017**

History

#1 - 08/23/2017 04:11 AM - William Grzybowski

- Status changed from 15 to Unscreened

This was definitely an overlook during some rewrite of that script a long while ago.

Please ago ahead and fix the inconsistency adding VersionAddendum and Ciphers +aes128-cbc to both cases. I dont think adding aes128-cbc is a big deal, since it just allows that cipher be used if the client really wants to. We even allow No cipher at all, because of replication without encryption, for speed.

#2 - 08/23/2017 05:00 AM - Vladimir Vinogradenko

- Status changed from Unscreened to Needs Developer Review

#3 - 08/23/2017 05:33 AM - William Grzybowski

- Status changed from Needs Developer Review to Reviewed by Developer

#4 - 08/23/2017 05:34 AM - Dru Lavigne

Vladimir or William: what is the target version?

#5 - 08/23/2017 05:35 AM - Vladimir Vinogradenko

- Status changed from Reviewed by Developer to Ready For Release

#6 - 08/23/2017 05:49 AM - William Grzybowski

- Target version changed from N/A to 11.1

- Seen in changed from N/A to 11.0-U2

#7 - 08/23/2017 05:49 AM - William Grzybowski

- Priority changed from No priority to Nice to have

#8 - 09/01/2017 07:40 AM - Dru Lavigne

- Subject changed from Inconsistent sshd config generation to Fix sshd config generation

#9 - 09/20/2017 06:35 AM - William Grzybowski

- Related to Bug #20044: SFTP backup from CUCM 10.5.2.12900-14 fails with FreeNAS-9.10.2 (a476f16) added

#10 - 09/27/2017 07:34 AM - Dru Lavigne

- Target version changed from 11.1 to 11.1-BETA1

#11 - 10/24/2017 04:48 AM - Dru Lavigne

- Status changed from Ready For Release to Resolved

#12 - 11/06/2017 12:46 PM - Nick Wolff

- QA Status Test Passes FreeNAS added

- QA Status deleted (Not Tested)

#13 - 11/09/2017 08:37 AM - Joe Maloney

- Needs QA changed from Yes to No