FreeNAS - Feature #25521

Generate SHA256 checksum for manual update file

08/09/2017 02:12 PM - T F

Status:	Resolved	**Estimated time:**	0.00 hour
Priority:	No priority		
Assignee:	Kris Moore		
Category:	OS		
Target version:	11.1-BETA1		
Severity:	New	**Needs Merging:**	Yes
Reason for Closing:		**Needs Automation:**	No
Reason for Blocked:		**Support Suite Ticket:**	n/a
Needs QA:	No	**Hardware Configuration:**	
Needs Doc:	Yes		

Description

I am only able to verify the full release ISO files and not the manual update tar file. Could someone with direct access to the master file please get me a sha256 sum for https://download.freenas.org/11/11.0-U2/FreeNAS-11.0-U2-manual-update.tar and also talk to the powers that be about adding this as part of the standard release process similar to the iso file?

Associated revisions

Revision 788a6303 - 09/06/2017 12:07 PM - Kris Moore

Update freenas-release.py to create a .sha256 of the manual update file after signing it. Also include some previous work which Sean hadn't checked in yet.

Ticket: #25521

History

#1 - 08/09/2017 03:59 PM - Dru Lavigne

- Assignee changed from Release Council to Kris Moore

#2 - 08/15/2017 06:43 AM - Kris Moore

- Assignee changed from Kris Moore to Vaibhav Chauhan

Vb - Does this file get created automatically and we just forgot to copy it?

#3 - 08/15/2017 05:27 PM - Vaibhav Chauhan

- Status changed from Unscreened to 15

- Assignee changed from Vaibhav Chauhan to Sean Fagan

kris we have to manually create this file, and I did create the tarfile but I don't remember that any .sha256 checksum file is generate as part of the process, I will had this over to sef as he had created this utility and he maybe able to tell me if I have missed something.

#4 - 08/15/2017 05:37 PM - Sean Fagan

- Assignee changed from Sean Fagan to Vaibhav Chauhan

No SHA is generated, however, there's no reason that couldn't be done as part of the process. (That is to say, whatever puts the file up on a server can generate a SHA256 checksum easily enough.)

I don't know what the process or script used to generate the file is, so i'm a bit hampered.

#5 - 09/05/2017 10:38 AM - Dru Lavigne

Kris: what are your thoughts?

#6 - 09/05/2017 10:44 AM - Sean Fagan

Note that the manifest file for the manual update file is signed, and if the signature is invalid, it won't be applied.

#7 - 09/05/2017 11:06 AM - Dru Lavigne

- Assignee changed from Vaibhav Chauhan to Kris Moore

#8 - 09/05/2017 11:59 AM - Kris Moore

- Category changed from Forums/Websites to 1

- Status changed from 15 to Unscreened

- Assignee changed from Kris Moore to Sean Fagan

Sean,

The line is right here:

https://github.com/freenas/build/blob/master/build/tools/create-upgrade-distribution.py#L82

Can you add another command there to run sha256 -q on the resulting manual-update file so we at least have it locally to push out?

#9 - 09/05/2017 12:12 PM - Sean Fagan

- Assignee changed from Sean Fagan to Kris Moore

That's not it: that is **not** the manual update file on the download servers. (That file contains an unsigned manifest, while the one on the servers does. I sent this to VB 3 weeks ago because I don't know what process he uses to create it, so I can't say how it should be changed.)

#10 - 09/05/2017 12:55 PM - Sean Fagan

This creates a hash file during the build, but I have not created a pull request for it, because, again, it will *not* solve the problem.

```
diff --git a/build/tools/create-upgrade-distribution.py b/build/tools/create-upgrade-distribution.py
index d82e34f..9e720b9 100755
--- a/build/tools/create-upgrade-distribution.py
+++ b/build/tools/create-upgrade-distribution.py
@@ -80,7 +80,9 @@ def create_upgradefile():
                                os.path.join(temp_dir, entry))
     sh("chmod 755 {0}".format(temp_dir))
     sh("tar -C {0} -cf {1} .".format(temp_dir, e("${BE_ROOT}/release/${PRODUCT}-${VERSION}-manual-update-unsi
gned.tar")))
+    sh("sha256 -q {0} > {0}.sha256".format(e("${BE_ROOT}/release/${PRODUCT}-${VERSION}-manual-update-unsigned
.tar")))
     info("tar-file path: ${{BE_ROOT}}/release/${{PRODUCT}}-${{VERSION}}-manual-update-unsigned.tar")
+    info("tar-file checksum path:  ${{BE_ROOT}}/release/${{PRODUCT}}-${{VERSION}}-manual-update-unsigned.tar.
sha256")
     shutil.rmtree(temp_dir)
```

```
if __name__ == '__main__':
```

#11 - 09/05/2017 12:57 PM - Kris Moore

- Assignee changed from Kris Moore to Vaibhav Chauhan

Understood. Vb, how do you sign this particular fire before uploading? Some manual command / process? That will allow us to determine where to insert the sha256 command.

#12 - 09/06/2017 06:36 AM - Kris Moore

- Status changed from Unscreened to Resolved

- Assignee changed from Vaibhav Chauhan to Kris Moore

- Target version set to 11.1

This should be fixed now, added the following to the freenas-release python. Vb, let me know if anything looks odd next time you run it.

```
--- /usr/local/bin/freenas-release.good.20170907        2017-09-06 06:31:53.000000000 -0700
+++ /usr/local/bin/freenas-release      2017-09-06 06:32:01.000000000 -0700
@@ -3549,6 +3549,8 @@
sys.exit(1)
shutil.rmtree(dest, ignore_errors=True)
print(temp_dest)
print("Creating sha256 checksum")
+       os.popen("/sbin/sha256 -q {0} > {0}.sha256".format(temp_dest) )
else:
print(dest)
```

#13 - 09/06/2017 11:10 AM - Sean Fagan

The intent of "print(temp_dest)" is so that a script can use that to automatically get the pathname of the extracted tar file, so I'd remove the "Creating sha256 checksum" line, *or* print it to stderr, and then print out the path of the checksum file.

#14 - 09/06/2017 11:15 AM - Kris Moore

Removed that extra print, since I wasn't aware this was being used to feed other scripts.

Sean - I gather you are the original author of this freenas-release code? If so it probably makes sense to send these type of things over to you in the future.

#15 - 09/06/2017 11:21 AM - Sean Fagan

My question has always been how VB created it. That is, what process he uses. I'm hesitant to suggest any code changes until he answers that question.

(For example: if he uses a script to extract the tarball and copy that over, there's no need to change freenas-release, since whatever is extracting and copying can just as easily call sha256 itself. If he's instead running the extraction by hand, then it makes more sense to change the tool.)

#16 - 09/06/2017 11:44 AM - Vaibhav Chauhan

so I use this command to manually-sign the update file on update.freenas.org

sudo freenas-release --archive /tank/www/FreeNAS --database /home/sef/FreeNAS-updates.db --project FreeNAS --key /home/sef/Keys/ix-freenas-key.key extract --dest /tmp/FreeNAS-<VERSION_NUMBER>-manual-update.tar --tar FreeNAS-11-STABLE/LATEST

during the process I am asked PEM passphrase.

then I copy this update.tar file over to download.freenas.org

#17 - 09/06/2017 11:46 AM - Sean Fagan

Okay, given that, then (with the modification I suggested) Kris' change is the right thing to do. You'll then want to copy /tmp/FreeNAS-<VERSION_NUMBER>-manual-update.tar* over.

#18 - 09/06/2017 11:48 AM - Kris Moore

Excellent. I made that suggested change, you should end up with the .tar file and a .tar.sha256 next time, be sure to copy both over.

#19 - 09/06/2017 11:52 AM - Sean Fagan

Did you check the change in? :)

#20 - 09/06/2017 12:08 PM - Kris Moore

Yep, all merged in now.

#21 - 09/09/2017 11:07 AM - Dru Lavigne

- Subject changed from Manual update tar file lacks sha256 sum for download verification to Generate SHA256 checksum for manual update file

#22 - 09/26/2017 03:59 PM - Dru Lavigne

- Target version changed from 11.1 to 11.1-BETA1

#24 - 10/26/2017 10:50 AM - Bonnie Follweiler

- Needs QA changed from Yes to No

- QA Status Test Passes FreeNAS added

- QA Status deleted (Not Tested)