

FreeNAS - Bug #23197

Try to validate certificate before importing it

04/07/2017 04:23 PM - Cyber Jock

Status:	Resolved	
Priority:	Nice to have	
Assignee:	Vladimir Vinogradenko	
Category:	Middleware	
Target version:	11.1	
Seen in:	TrueNAS-9.10.2-U1	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

A TrueNAS customer running 9.10.2-U1 was adding their signed cert from digicert to their TrueNAS for the purposes of WebGUI encryption. Digicert offers several options. When choosing "nginx" for the best format it defaults to a cert format that does not work on TrueNAS.

When setting up a certificate the TrueNAS customer created a CSR on the TrueNAS, then uploaded it to digicert. On their website you can choose the format type (customer was choosing nginx, which gives a pem file with multiple certs in it). They would import the .pem file contents into TrueNAS which would happily accept it. However, once you tried to enable https and use the cert, the dropdown for the cert to choose would have no options aside from -----.

Upon further investigation we determined that by choosing 'nginx' on the digicert website results in a format that isn't compatible with the TrueNAS. Through the process of testing, we determined that you must choose "OTHER" and then select from a dropdown that has multiple options. The 3 that are important is:

1. A single .pem file containing all the certs.
2. A single .pem file containing only the end entity certificate.
3. A single .pem file containing all the certs except for the root.

If you choose anything except option 2, your .pem file will contain more than one cert. If you then take the entire contents of the .pem file and use it, it will not work. It was not initially obvious that the .pem file contained more than 1 cert because all of the text was a single long line.

To avoid this kind of confusion we should find a way to make it obvious that the input we're providing (the .pem with more than 1 cert) is not acceptable and reject it or accept it and determine which one of the certs we want to use and discard the remainder. The latter seems hard if not impossible to do.

I was able to manually choose the proper settings that allowed him to use the certificate for https.

Not sure what category this should fall in, so marking it as TrueNAS. Attached screenshots are for explaining what the customer saw when trying to create his cert.

Associated revisions

Revision 5a16e970 - 11/12/2017 04:49 AM - Vladimir Vinogradenko

fix(gui): Proper common clean_certificate with validation for all certificate-related forms

Ticket: #23197

Revision 8aa9eada - 11/12/2017 06:00 AM - Vladimir Vinogradenko

fix(gui): Proper common clean_certificate with validation for all certificate-related forms

Ticket: #23197

Revision fd774c9b - 12/04/2017 12:36 PM - Vladimir Vinogradenko

fix(gui): Proper common clean_certificate with validation for all certificate-related forms

Ticket: #23197

Revision 7b70c9b8 - 12/04/2017 12:37 PM - Vladimir Vinogradenko

fix(gui): Proper common clean_certificate with validation for all certificate-related forms

Ticket: #23197

History

#1 - 04/08/2017 10:43 AM - Kris Moore

- Assignee set to Marcelo Araujo
- Target version set to 400

#2 - 04/09/2017 07:44 PM - Marcelo Araujo

- Status changed from Unscreened to Screened

#3 - 04/19/2017 08:10 AM - Kris Moore

- Target version changed from 400 to TrueNAS 11.1-U1

#4 - 06/13/2017 11:58 AM - Kris Moore

- Assignee changed from Marcelo Araujo to Suraj Ravichandran

#5 - 08/22/2017 07:45 AM - Dru Lavigne

- Assignee changed from Suraj Ravichandran to William Grzybowski

William: please load balance between Vladimir and Nikola.

#6 - 08/23/2017 04:43 AM - William Grzybowski

- Project changed from TrueNAS to FreeNAS
- Category changed from Middleware to Middleware
- Status changed from Screened to Unscreened
- Assignee changed from William Grzybowski to Nikola Gigic
- Target version changed from TrueNAS 11.1-U1 to 11.1

Nikola, is this something you think you can tackle?

Thanks!

#7 - 09/26/2017 09:05 AM - Nikola Gigic

- Status changed from Unscreened to Screened

#8 - 10/25/2017 11:16 AM - Kris Moore

- Target version changed from 11.1 to 11.1-U1

#9 - 10/31/2017 09:19 AM - Dru Lavigne

- Assignee changed from Nikola Gigic to Vladimir Vinogradenko

#10 - 11/12/2017 04:49 AM - Vladimir Vinogradenko

- Status changed from Screened to 15

This ticket is very old, so we'll need to retest this because some work has been done on related parts of code since then.

They would import the .pem file contents into TrueNAS which would happily accept it. However, once you tried to enable https and use the cert, the dropdown for the cert to choose would have no options aside from -----.

The only certificates hidden from that list are CERT_TYPE_CSR. The code that promotes CERT_TYPE_CSR to CERT_TYPE_EXISTING was there for many years. I wonder how did the bug you're describing have happened. Are you able to repeat this now? What are exact steps?

If you choose anything except option 2, your .pem file will contain more than one cert. If you then take the entire contents of the .pem file and use it, it will not work. It was not initially obvious that the .pem file contained more than 1 cert because all of the text was a single long line.

FreeNAS supports certificate chains and parses appropriate pem files correctly.

What may be the issue here is opening pem files with Unix-style line-endings in Windows notepad: then line breaks would be eaten and certificate would be invalid.

We may solve this issue by providing file upload field along with textarea.

To avoid this kind of confusion we should find a way to make it obvious that the input we're providing (the .pem with more than 1 cert) is not acceptable

Certificate validation was also already present in FreeNAS CertificateAuthorityImportForm. I've also added it to CertificateCSREditForm and CertificateImportForm as part of the work on this ticket.

#11 - 11/14/2017 11:29 AM - Dru Lavigne

- Status changed from 15 to 47
- Assignee changed from Vladimir Vinogradenko to Bonnie Follweiler

Bonnie: is this a scenario that QA can test?

#13 - 12/04/2017 11:52 AM - Dru Lavigne

- Status changed from 47 to 42
- Assignee changed from Bonnie Follweiler to Vladimir Vinogradenko
- Target version changed from 11.1-U1 to 11.1

Vlad: please merge to stable so this can go into 11.1.

#14 - 12/04/2017 11:55 AM - Dru Lavigne

- TrueNAS
- Subject changed from 2 certs being added to WebGUI is accepted, but doesn't work. to Try to validate certificate before importing it

#15 - 12/06/2017 02:32 PM - Nick Wolff

- Needs QA changed from Yes to No
- QA Status Test Passes FreeNAS added
- QA Status deleted (Not Tested)

Test Passes

#16 - 12/07/2017 08:22 AM - Dru Lavigne

- Status changed from 42 to Ready For Release

#17 - 12/13/2017 04:10 PM - Dru Lavigne

- Status changed from Ready For Release to Resolved

Files

2017-04-07_14h47_01.jpg	781 KB	04/07/2017	Cyber Jock
2017-04-07_14h47_18.jpg	735 KB	04/07/2017	Cyber Jock
2017-04-07_14h47_25.jpg	737 KB	04/07/2017	Cyber Jock
2017-04-07_14h47_29.jpg	732 KB	04/07/2017	Cyber Jock