Installer - Bug #27568

changing ssl certificates only for web access

08/09/2019 07:34 AM - Alex Losa

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Foreman modules		
Target version:			
Difficulty:	medium	**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

I'd like to change the ssl certificate to access to the website of my Foreman/Katello and use a wildcard of my organization

How could I do it?

Only for https access to the website

Related issues:

Has duplicate Katello - Bug #27753: About Support #27568	**Duplicate**

History

#1 - 08/13/2019 07:52 PM - Chris Roberts

- Tracker changed from Bug to Support

- Category set to Installer

- Assignee set to Chris Roberts

- Target version set to Katello Recycle Bin

- Triaged changed from No to Yes

Hi Alex,

Please see this article:

https://theforeman.org/plugins/katello/3.12/advanced/certificates.html

Let me know if this does not answer your question.

#2 - 08/13/2019 07:52 PM - Chris Roberts

- Status changed from New to Resolved

#3 - 08/14/2019 06:04 AM - Alex Losa

I saw that website and I did all there is said.

I checked my certs:

[root@foreman-ssl ~]# katello-certs-check -c certs/wildcard_ieca.junta-andalucia.es.crt -k certs/wildcard_ieca.junta-andalucia.es.key -b certs/AC_FNMT_Foreman.crt
Checking server certificate encoding:
[OK]

date: fecha inválida «ago 14 06:03:00 2019»
Checking expiration of certificate:
[OK]

Checking expiration of CA bundle:
[OK]

Checking if server certificate has CA:TRUE flag
[OK]

Checking to see if the private key matches the certificate:
[OK]

Checking CA bundle against the certificate file:
[OK]

Checking Subject Alt Name on certificate
[OK]

Checking Key Usage extension on certificate for Key Encipherment
[OK]

Validation succeeded

```
To use them inside a NEW $FOREMAN_PROXY, run this command:

foreman-proxy-certs-generate --foreman-proxy-fqdn "$FOREMAN_PROXY" \
                                    --certs-tar  "~/$FOREMAN_PROXY-certs.tar" \
                                    --server-cert "/root/certs/wildcard_ieca.junta-andalucia.es.crt" \
                                    --server-key "/root/certs/wildcard_ieca.junta-andalucia.es.key" \
                                    --server-ca-cert "/root/certs/AC_FNMT_Foreman.crt" \

To use them inside an EXISTING $FOREMAN_PROXY, run this command INSTEAD:

foreman-proxy-certs-generate --foreman-proxy-fqdn "$FOREMAN_PROXY" \
                                    --certs-tar  "~/$FOREMAN_PROXY-certs.tar" \
                                    --server-cert "/root/certs/wildcard_ieca.junta-andalucia.es.crt" \
                                    --server-key "/root/certs/wildcard_ieca.junta-andalucia.es.key" \
                                    --server-ca-cert "/root/certs/AC_FNMT_Foreman.crt" \
                                    --certs-update-server
```

I tried to install Foreman/Katello with this command:

foreman-installer --scenario katello --certs-server-cert certs/wildcard_ieca.junta-andalucia.es.crt --certs-server-cert-req certs/wildcard_ieca.junta-andalucia.es.req --certs-server-key certs/wildcard_ieca.junta-andalucia.es.key --certs-server-ca-cert certs/AC_FNMT_Foreman.crt

I received this error and stopped the installation:

Parameter certs-server-ca-cert invalid: certs/AC_FNMT_Foreman.crt is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]?[^\\/]+))/ or regexes matchinError during configuration, exiting

And this is the log information of the problem with certs:

ESC[0m
ESC[mNotice: Compiled catalog for foreman-ssl.ieca.junta-andalucia.es in environment production in 0.68 secondsESC[0m
ESC[mNotice: Applied catalog in 0.07 secondsESC[0m

[INFO 2019-08-13T13:57:25 main] ... finished
[INFO 2019-08-13T13:57:25 main] Executing hooks in group pre_values
[INFO 2019-08-13T13:57:25 main] All hooks in group pre_values finished
[INFO 2019-08-13T13:57:25 main] Running installer with args [["--scenario", "katello", "--certs-server-cert", "certs/wildcard_ieca.junta-andalucia.es.crt", "--certs-server-cert-req", "certs/wildcard_ieca.junta-andalucia.es.req", "--certs-server-key", "certs/wildcard_ieca.junta-andalucia.es.key", "--certs-server-ca-cert", "certs/AC_FNMT_Foreman.crt"]]
[INFO 2019-08-13T13:57:25 main] Executing hooks in group pre_validations
[DEBUG 2019-08-13T13:57:25 main] Hook /usr/share/foreman-installer/katello/hooks/pre_validations/10-check_foreman_proxy_pulp.rb returned nil
[DEBUG 2019-08-13T13:57:25 main] Hook /usr/share/foreman-installer/katello/hooks/pre_validations/12-check_capsule_tar.rb returned nil
[DEBUG 2019-08-13T13:57:25 main] Hook /usr/share/foreman-installer/katello/hooks/pre_validations/30-mongo_storage_engine.rb returned nil
[DEBUG 2019-08-13T13:57:25 main] Hook /usr/share/foreman-installer/katello/hooks/pre_validations/31-upgrade-puppet.rb returned nil
[INFO 2019-08-13T13:57:25 main] All hooks in group pre_validations finished
[INFO 2019-08-13T13:57:25 main] Running validation checks
[ERROR 2019-08-13T13:57:25 main] Parameter certs-server-cert invalid: certs/wildcard_ieca.junta-andalucia.es.crt is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]?[^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
[ERROR 2019-08-13T13:57:25 main] Parameter certs-server-key invalid: certs/wildcard_ieca.junta-andalucia.es.key is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]?[^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
[ERROR 2019-08-13T13:57:25 main] Parameter certs-server-cert-req invalid: certs/wildcard_ieca.junta-andalucia.es.req is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]?[^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
[ERROR 2019-08-13T13:57:25 main] Parameter certs-server-ca-cert invalid: certs/AC_FNMT_Foreman.crt is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]?[^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
[DEBUG 2019-08-13T13:57:25 main] Exit with status code: 21 (signal was invalid_values)
[ERROR 2019-08-13T13:57:25 main] Errors encountered during run:
[ERROR 2019-08-13T13:57:25 main] Parameter certs-server-cert invalid: certs/wildcard_ieca.junta-andalucia.es.crt is not one of regexes matching

/^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]\?[\\/][^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
[ERROR 2019-08-13T13:57:25 main] Parameter certs-server-key invalid: certs/wildcard_ieca.junta-andalucia.es.key is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]\?[\\/][^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
[ERROR 2019-08-13T13:57:25 main] Parameter certs-server-cert-req invalid: certs/wildcard_ieca.junta-andalucia.es.req is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]\?[\\/][^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
[ERROR 2019-08-13T13:57:25 main] Parameter certs-server-ca-cert invalid: certs/AC_FNMT_Foreman.crt is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]\?[\\/][^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
[DEBUG 2019-08-13T13:57:25 main] Cleaning /tmp/kafo_puppet20190813-2065-b6t1p7.conf
[DEBUG 2019-08-13T13:57:25 main] Cleaning /tmp/default_values.yaml
[INFO 2019-08-13T13:57:25 main] Installer finished in 5.154968775 seconds

#4 - 08/14/2019 01:14 PM - Chris Roberts

Thanks for the update Alex.

I will test this today with a wildcard cert and see why this is happening. Do you have any specific things set in the CSR or odd with the domain?

Was this wildcard cert created from a public CA or an internal CA?

#5 - 08/14/2019 01:14 PM - Chris Roberts

- Status changed from Resolved to Assigned

#6 - 08/14/2019 01:14 PM - Chris Roberts

- Target version changed from Katello Recycle Bin to Katello 3.14.0

#7 - 08/21/2019 05:05 PM - Chris Roberts

- Status changed from Assigned to Closed

- Target version changed from Katello 3.14.0 to Katello Recycle Bin

#8 - 09/11/2019 05:43 PM - John Mitsch

- Tracker changed from Support to Bug

- Status changed from Closed to Assigned

- Target version changed from Katello Recycle Bin to Katello Backlog

I'm going to reopen this bug so we can continue the conversation here and address your issue and I'll close out
https://projects.theforeman.org/issues/27753

The response in 27753 was:
[Thanks for the update Alex.
I will test this today with a wildcard cert and see why this is happening. Do you have any specific things set in the CSR or odd with the domain?
Was this wildcard cert created from a public CA or an internal CA?]

My cert is a normal wildcard created from a public CA. FNMT from Spain.

#9 - 09/11/2019 05:44 PM - John Mitsch

- Has duplicate Bug #27753: About Support #27568 added

#10 - 09/16/2019 03:36 PM - Chris Roberts

- Status changed from Assigned to Need more information

Hi Alex,

I tested this with a wildcard and I am getting:

```bash
[ERROR 2019-09-16T15:35:07 verbose]  /Stage[main]/Certs::Apache/Cert[toledossl.satellite.lab.eng.rdu2.redhat.com-apache]/ensure: change from 'absent' to 'present' failed: Execution of '/usr/bin/katello-ssl-tool --gen-server --set-hostname toledossl.satellite.lab.eng.rdu2.redhat.com --server-cert toledossl.satellite.lab.eng.rdu2.redhat.com-apache.crt --server-cert-req toledossl.satellite.lab.eng.rdu2.redhat.com-apache.crt.req --server-key toledossl.satellite.lab.eng.rdu2.redhat.com-apache.key --server-rpm toledossl.satellite.lab.eng.rdu2.redhat.com-apache --rpm-only' returned 33:
...working...
[ERROR 2019-09-16T15:35:07 verbose]
[ERROR 2019-09-16T15:35:07 verbose]  can't find a file that should have been created during an earlier step:
[ERROR 2019-09-16T15:35:07 verbose]        ./ssl-build/KATELLO-TRUSTED-SSL-CERT

```

We have a fix for the above error, but since you are getting:

```
certs/wildcard_ieca.junta-andalucia.es.crt is not one of regexes matching /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]\?[\\/][^\\/]+))/ or regexes matching /^\/([^\/\0]+\/*)*$/
```

Can I have you paste the output of the following command:

1. openssl x5909 -in certs/wildcard_ieca.junta-andalucia.es.crt -noout -text

#11 - 09/18/2019 09:23 AM - Alex Losa

[root@foreman certs]# openssl x509 -in wildcard_ieca.junta-andalucia.es.crt -noout -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
13:78:58:13:e2:ac:eb:d5:5a:d9:c7:f3:7b:1f:79:90
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=ES, O=FNMT-RCM, OU=AC Componentes Inform\xC3\xA1ticos
Validity
Not Before: Apr 20 10:58:59 2018 GMT
Not After : Apr 20 10:58:58 2020 GMT
Subject: C=ES, L=SEVILLA, O=INSTITUTO DE ESTAD\xC3\x8DSTICA Y CARTOGRAF\xC3\x8DA DE ANDALUC\xC3\x8DA, OU=INSTITUTO DE ESTAD\xC3\x8DSTICA Y CARTOGRAF\xC3\x8DA DE ANDALUC\xC3\x8DA/serialNumber=Q9150014J/2.5.4.97=VATES-Q9150014J, CN=*.ieca.junta-andalucia.es
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:80:15:da:c0:39:4e:4c:66:a3:43:0e:08:2e:84:
27:da:a1:09:15:a3:eb:82:1f:27:ea:6f:28:68:78:
f8:7e:35:f4:2b:ed:5d:4f:fe:f7:57:86:aa:9f:5c:
65:e5:89:da:eb:a9:c8:05:3f:ef:91:1a:23:8c:d8:
c4:73:f7:ed:7a:66:cf:3f:42:a1:60:b6:08:d5:91:
73:0c:84:19:a7:f9:81:13:05:bb:f3:d1:84:0d:55:
96:77:20:64:d5:69:24:c6:32:59:a9:83:8a:d3:c8:
3d:de:20:49:62:85:8c:a1:fc:b9:3b:35:ca:5c:56:
3f:ef:3a:02:24:bf:67:6a:05:27:0f:df:0e:cc:59:
a4:32:11:d8:26:8b:c1:0a:9b:63:5f:a7:ce:4d:62:
63:67:f9:62:15:d2:e1:f7:d8:3c:03:31:49:43:51:
9a:ec:5c:91:a2:b1:c0:2b:02:80:bc:f2:c9:5f:1c:
06:ed:3c:2c:dd:5e:12:f0:2f:5e:df:33:4c:5c:da:
52:98:52:d4:b4:33:b6:1f:c1:a9:24:6f:39:ad:77:
b3:92:a4:f4:c2:89:87:57:d4:1b:94:84:48:73:3f:
05:5c:4e:99:e5:f9:49:77:4c:36:90:06:45:2d:56:
08:62:f3:49:a4:ae:d8:c3:f7:d7:17:2d:24:71:2d:
8c:2f
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
Authority Information Access:
OCSP - URI:http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder
CA Issuers - URI:http://www.cert.fnmt.es/certs/ACCOMP.crt

```
X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.5734.3.9.17
                  CPS: http://www.cert.fnmt.es/dpcs/
                  User Notice:
                    Explicit Text: Certificado wildcard de autenticación de sitio web según reglamento europeo
 eIDAS. Sujeto a condiciones de uso según DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-Espa
ña)
                Policy: 0.4.0.2042.1.7

X509v3 Subject Alternative Name:
                DNS:*.ieca.junta-andalucia.es
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Subject Key Identifier:
                33:B8:9D:94:BD:32:EB:78:92:19:37:26:F2:A3:0A:0D:69:93:92:4E
            qcStatements:
                0..0......F.....0......F..0......F...0r.....F..0h02.,
https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf..es02.,https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf..en
```

```
            X509v3 Authority Key Identifier:
                keyid:19:F8:58:2F:14:D6:A6:CC:9B:04:98:08:0D:4C:D7:AB:00:A7:83:65

X509v3 CRL Distribution Points:

Full Name:
                  URI:ldap://ldapcomp.cert.fnmt.es/CN=CRL1,OU=AC%20Componentes%20Informaticos,O=FNMT-RCM,C=ES?
certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
                  URI:http://www.cert.fnmt.es/crlscomp/CRL1.crl

Signature Algorithm: sha256WithRSAEncryption
         28:1d:cb:c6:1e:98:4f:d4:24:04:c4:06:ea:08:04:9c:e7:f4:
         ab:d6:2d:d1:7d:d1:5f:6a:e0:c4:25:0f:11:40:d5:2e:db:eb:
         0e:67:d4:54:52:57:0c:e6:e4:ed:2d:22:46:ba:4d:7e:b3:d1:
         27:70:ed:df:2a:c6:b1:c5:c8:79:36:b8:89:83:95:5e:b1:fa:
         6c:6e:8e:11:6e:82:16:47:9e:ad:98:75:41:73:f8:96:a8:56:
         4f:8e:22:4e:65:e9:17:f2:29:56:94:32:43:a6:50:ce:68:0a:
         39:a7:b8:45:82:a3:1e:5d:6d:0e:b9:fb:c5:98:11:65:4c:ad:
         fc:5c:9e:5b:b8:49:4d:8d:96:91:d9:30:8e:9d:00:a4:7f:db:
         51:cd:b5:26:a0:6f:11:81:15:23:8a:c9:7b:08:ed:25:1c:2a:
         da:b6:c2:73:ec:10:38:fc:b7:a7:81:25:c6:88:6b:ed:fe:f5:
         5f:ca:b6:d4:e3:d1:99:f8:64:47:da:9b:84:2a:0e:73:c5:3d:
         55:69:7f:a5:a4:c2:11:27:3a:60:d2:18:71:12:ae:f7:22:1c:
         37:84:d0:5b:ed:94:b8:e1:ce:65:07:a4:99:c6:d0:22:dc:f3:
         4c:ce:6f:4e:b9:c2:9d:16:b5:36:66:56:1e:49:87:f1:71:7b:
         a7:95:23:79
[root@foreman certs]#
```

#12 - 09/18/2019 01:55 PM - Chris Roberts

- Target version changed from Katello Backlog to Katello 3.14.0

- Difficulty set to medium

Alex,

Looking at your cert I see the following in the subject line:

Subject: C=ES, L=SEVILLA, O=INSTITUTO DE ESTAD\xC3\x8DSTICA Y CARTOGRAF\xC3\x8DA DE ANDALUC\xC3\x8DA, OU=INSTITUTO DE ESTAD\xC3\x8DSTICA Y CARTOGRAF\xC3\x8DA DE ANDALUC\xC3\x8DA/serialNumber=Q9150014J/2.5.4.97=VATES-Q9150014J, CN=*.ieca.junta-andalucia.es

Here is mine:

Subject: C=US, ST=North Carolina, L=Raleigh, O=Red Hat, CN=satellite1.latest-el7.satellite.lab.eng.rdu2.redhat.com

I am thinking the \ are causing the issue coming from this error /^(([a-zA-Z]:[\\/])|([\\/][\\/][^\\/]+[\\/][^\\/]+)|([\\/][\\/]\?[\\/][^\\/]+))/ o

Let me look into this more, thank you for the output you provided.

#13 - 09/19/2019 11:38 AM - Alex Losa

Ok, I'll keep waiting for your response.

Thanks.

#14 - 09/24/2019 02:52 PM - Chris Roberts

- Status changed from Need more information to Assigned

#15 - 12/11/2019 07:11 PM - Jonathon Turel

- Target version deleted (Katello 3.14.0)

- Triaged changed from Yes to No

#16 - 12/18/2019 06:37 PM - Ian Ballou

- Target version set to Katello 3.15.0

- Triaged changed from No to Yes

#17 - 02/10/2020 01:57 PM - Jonathon Turel

- Target version deleted (Katello 3.15.0)

- Triaged changed from Yes to No

#18 - 02/25/2020 02:07 PM - Chris Roberts

- Project changed from Katello to Installer

- Category changed from Installer to Foreman modules

- Assignee deleted (Chris Roberts)

- Priority changed from High to Normal

Hi Alex,

I tried a few things and am unable to get the parser to read the cert correctly. I am making this a valid issue and moving it to the foreman-installer component so it can get triaged and set to a release etc.

Sorry for the delays.

#19 - 02/25/2020 02:08 PM - Chris Roberts

- Status changed from Assigned to New