

## Installer - Bug #26978

### Error occurred: Neither PUB key nor PRIV key: nested asn1 error (openscap)

06/06/2019 02:22 PM - Sven Vogel

<b>Status:</b> New	
<b>Priority:</b> Normal	
<b>Assignee:</b>	
<b>Category:</b>	
<b>Target version:</b>	
<b>Difficulty:</b>	<b>Fixed in Releases:</b>
<b>Triaged:</b> Yes	<b>Found in Releases:</b> 1.21.3
<b>Bugzilla link:</b>	<b>Red Hat JIRA:</b>
<b>Pull request:</b>	
<b>Description</b>	
<p>Problem: we try to use openscap with Foreman/Katello and the installation looks good but we got the following error.</p> <p>maybe there is a problem with the certificates. the system is registered with subscription-manager without any problem. i found this article <a href="https://access.redhat.com/solutions/2175231">https://access.redhat.com/solutions/2175231</a> 1 but its old and i think not more relevant. you can see my config files below.</p> <p>maybe i need to change or reset something happen with the certificates.</p> <p>any ideas or help?</p> <p>Error occurred: Neither PUB key nor PRIV key: nested asn1 error</p> <p>Expected outcome: No Error :slight_smile:</p> <p>Foreman and Proxy versions: Foreman: 1.21.3 Katello: 3.11 OpenScap: 0.7.1</p> <p>Foreman and Proxy plugin versions: Proxy: 1.21.3</p> <p>Other relevant data: /etc/foreman_scap_client/config.yaml</p> <pre># Client private key # It could be Puppet agent private key (e.g., '/var/lib/puppet/ssl/private_keys/myhost.example.com .pem') # Or (recommended for client reporting to Katello) consumer private key (e.g., '/etc/pki/consumer/ key.pem') :host_private_key: '/etc/pki/consumer/key.pem'  # policy (key is id as in Foreman)  3: :profile: 'xccdf_org.ssgproject.content_profile_stig-rhel7-disa' :content_path: '/var/lib/openscap/content/3e1654fd14a5352d65294db555710bfda5cad1a942209e2d787ea7 940035616e.xml' # Download path # A path to download SCAP content from proxy :download_path: '/compliance/policies/3/content/3e1654fd14a5352d65294db555710bfda5cad1a942209e2d 787ea7940035616e' :tailoring_path: '' :tailoring_download_path: ''</pre>	

```

4:
:profile: 'xccdf_org.ssgproject.content_profile_hipaa'
:content_path: '/var/lib/openscap/content/3e1654fd14a5352d65294db555710bfda5cad1a942209e2d787ea7
940035616e.xml'
# Download path
# A path to download SCAP content from proxy
:download_path: '/compliance/policies/4/content/3e1654fd14a5352d65294db555710bfda5cad1a942209e2d
787ea7940035616e'
:tailoring_path: ''
:tailoring_download_path: ''

---
:enabled: https

# Log file for the forwarding script.
:openscap_send_log_file: /var/log/foreman-proxy/openscap-send.log

# Directory where OpenSCAP audits are stored
# if they failed to post to Foreman. smart_proxy_openscap_send will
# try to re-send them.
:spooldir: /var/spool/foreman-proxy/openscap

# Directory where OpenSCAP content XML are stored
# So we will not request the XML from Foreman each time
:contentdir: /var/lib/foreman-proxy/openscap/content

# Directory where OpenSCAP report XML are stored
# So Foreman can request arf xml reports
:reportsdir: /var/lib/foreman-proxy/openscap/reports

# Directory where OpenSCAP report XML are stored
# In case sending to Foreman succeeded, yet failed to save to reportsdir
:failed_dir: /var/lib/foreman-proxy/openscap/failed

# Directory where corrupted OpenSCAP report XML are stored
# when proxy cannot parse the report sent by client
:corrupted_dir: /var/lib/foreman-proxy/openscap/corrupted

# Proxy name to send to Foreman with parsed report
# Foreman matches it against names of registered proxies to find the report source
:registered_proxy_name: katello01.example.com

# Proxy url to send to Foreman with parsed report
# Foreman matches it against urls of registered proxies to find the report source
:registered_proxy_url: https://katello01.example.com:9090

# Timeout to send ARF reports to Foreman, in seconds
:timeout: 60

s_client is working

openssl s_client -connect katello01.example.com:9090 -CAfile /etc/rhsm/ca/katello-server-ca.pem -c
ert /etc/pki/consumer/cert.pem -key /etc/pki/consumer/key.pem

```

## History

### #1 - 06/06/2019 02:26 PM - Sven Vogel

i will get the message from the /var/log/foreman-proxy/proxy.log

```

2019-06-06T16:23:16 3ba56e3e [I] Started GET /policies/3/content/3e1654fd14a5352d65294db555710bfda5cad1a942209
e2d787ea7940035616e
2019-06-06T16:23:16 3ba56e3e [I] Creating directory to store SCAP file: /var/lib/foreman-proxy/openscap/conten
t/3
2019-06-06T16:23:16 3ba56e3e [E] Error occurred: Neither PUB key nor PRIV key: nested asn1 error
2019-06-06T16:23:16 3ba56e3e [D] Error occurred: Neither PUB key nor PRIV key: nested asn1 error
2019-06-06T16:23:16 3ba56e3e [I] Finished GET /policies/3/content/3e1654fd14a5352d65294db555710bfda5cad1a94220
9e2d787ea7940035616e with 500 (2.33 ms)

```

## #2 - 06/06/2019 02:27 PM - Sven Vogel

- Found in Releases foreman\_openscap 0.7.10, puppet-foreman\_scap\_client 0.3.19 added

## #3 - 06/06/2019 08:26 PM - Sven Vogel

- Triage changed from No to Yes

after some investigation i found the Solution. the error indicates that the problem seems to be something to do with the foreman/katello proxy private key.

**We have different installations and it seems after a new install or reset of the certificates the installer dont set them correctly.**

if you use katello with foreman the following should be set correctly in the file.

/etc/foreman-proxy/settings.yml

```
# SSL Setup

# if enabled, all communication would be verified via SSL
# NOTE that both certificates need to be signed by the same CA in order for this to work
# see http://theforeman.org/projects/smart-proxy/wiki/SSL for more information
:ssl_ca_file: /etc/foreman-proxy/ssl_ca.pem
:ssl_certificate: /etc/foreman-proxy/ssl_cert.pem
:ssl_private_key: /etc/foreman-proxy/ssl_key.pem

# Use this option only if you need to disable certain cipher suites.
# Note: we use the OpenSSL suite name, such as "RC4-MD5".
# The complete list of cipher suite names can be found at:
# https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-SUITE-NAMES
#:ssl_disabled_ciphers: [CIPHER-SUITE-1, CIPHER-SUITE-2]

# Use this option only if you need to strictly specify TLS versions to be
# disabled. SSLv3 and TLS v1.0 are always disabled and cannot be configured.
# Specify versions like: '1.1', or '1.2'
#:tls_disabled_versions: []

# the hosts which the proxy accepts connections from
# commenting the following lines would mean every verified SSL connection allowed
:trusted_hosts:
  - katello01.example.com

# Endpoint for reverse communication
:foreman_url: https://katello01.example.com

# SSL settings for client authentication against Foreman. If undefined, the values
# from general SSL options are used instead. Mainly useful when Foreman uses
# different certificates for its web UI and for smart-proxy requests.
:foreman_ssl_ca: /etc/foreman-proxy/foreman_ssl_ca.pem
:foreman_ssl_cert: /etc/foreman-proxy/foreman_ssl_cert.pem
:foreman_ssl_key: /etc/foreman-proxy/foreman_ssl_cert.pem
```

you will see the error here! cert and key are the same file.

```
:foreman_ssl_cert: /etc/foreman-proxy/foreman_ssl_cert.pem
:foreman_ssl_key: /etc/foreman-proxy/foreman_ssl_cert.pem
```

should be cert and key.

```
:foreman_ssl_cert: /etc/foreman-proxy/foreman_ssl_cert.pem
:foreman_ssl_key: /etc/foreman-proxy/foreman_ssl_key.pem
```

the strange problem is and its reproducible if you check the foreman-installer --full-help you will see its a base problem. you cant reset it to the correct value. normally it should.

```
--foreman-proxy-foreman-ssl-key Corresponding key to a foreman_ssl_cert certificate
                                When not specified, the ssl_key is used instead. (current: "/etc/foreman-pro
xy/foreman_ssl_cert.pem")
--reset-foreman-proxy-foreman-ssl-key Reset foreman_ssl_key to the default value (UNDEF) <----- its und
ef???
```

```
foreman-installer --foreman-proxy-foreman-ssl-key="/etc/foreman-proxy/foreman_ssl_key.pem" -v
```

maybe anybody can classify a other category for this ticket and reproduce this.

**#4 - 06/11/2019 10:16 AM - Ondřej Pražák**

- *Project changed from OpenSCAP to Installer*
- *Triaged changed from Yes to No*
- *Found in Releases 1.21.3 added*
- *Found in Releases deleted (foreman\_openscap 0.7.10, puppet-foreman\_scap\_client 0.3.19)*

Thank you for a detailed bug report, moving to installer as it seems the default cert paths are not correctly set.

**#5 - 05/14/2020 01:50 PM - Zach Huntington-Meath**

- *Triaged changed from No to Yes*