RPM Support - Issue #2642

--auth-ca parameter on repo creation not working

03/17/2017 09:58 AM - lenny

Status:	CLOSED - WONTFIX	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0:00 hour
Category:			
Sprint/Milestone:			
Severity:	2. Medium	**Groomed:**	No
Version:	2.12.1	**Sprint Candidate:**	No
Platform Release:		**Tags:**	Pulp 2
OS:	CentOS 7	**Sprint:**	
Triaged:	Yes	**Quarter:**	

Description

Hi,

the --auth-ca parameter creates the local certificate files under /etc/pki/pulp/content, but client requests still verified with the host ca.

You can find the setup on the mailing list: https://www.redhat.com/archives/pulp-list/2017-March/msg00004.html

Regards,

Rene

History

#2 - 03/21/2017 03:28 PM - bizhang

Hi Lenny,

Can you try setting the auth_cert option:
http://docs.pulpproject.org/plugins/pulp_rpm/tech-reference/yum-plugins.html#optional-configuration-parameters

If that doesn't work can you send me the full rest API call you're using to to create (pass the -vv command via pulp-admin and it will show you the rest API call) and I can take a look.

#3 - 03/21/2017 04:15 PM - lenny

- File dump added

Hi,

thanks for your effort.

> The file must contain both the certificate itself and its private key.

I´ve combined the client cert and key file with cat to one file.

> pulp-admin -vv rpm repo update --repo-id centos-x86_64-7.3.1611-base --relative-url testing/centos/7.3.1611/os/x86_64/ --feed http://ftp.tu-chemnitz.de/pub/linux/centos/7.3.1611/os/x86_64/ --auth-cert=client.cert --auth-ca=Pulp_CA.cert

You can find the output in the attachments.

> pulp-admin repo list --detail

Shows me the certs and protected true state. Die Repository is still unprotected.

> enabled: true

Set repo_auth.conf and restart httpd. All repositories are now protected.

> /etc/pki/pulp/content/

Cert etc. are created by pulp in content path.

> curl -v --cert ./certs/Pulp_client.cert --key ./certs/Pulp_client.key
> https://my.server.name/pulp/repos/testing/centos/7.3.1611/os/x86_64/repodata/repomd.xml

curl: (56) Peer does not recognize and trust the CA that issued your certificate

The client certificate get verified by the host ca file (Comodo CA).

#4 - 03/24/2017 03:56 PM - bizhang

- Triaged changed from No to Yes

#5 - 03/24/2017 04:00 PM - bizhang

I was able to get this working by setting the SSLVerifyClient to optional_no_ca in the pulp_content.conf [0]
Since the pulp_content was validating the client cert being passed with the PulpCA instead of the repo CA.

We should also make a new blog post or update the old one with the correct steps [1]

Steps I took to make protected repos work:

```
vi /etc/pulp/repo_auth.conf
# Set enabled to true

vi /etc/httpd/conf.d/pulp_content.conf
# set SSLVerifyClient to optional_no_ca
# this is necessary because otherwise the client cert is rejected since it wasn't signed with the pulp CA

# restart apache

pulp-admin rpm repo create --repo-id=bar --relative-url=bar \
--feed=http://repos.fedorapeople.org/repos/pulp/pulp/demo_repos/zoo/ --auth-ca=/home/vagrant/certs/caPulp.crt

pulp-admin rpm repo publish run --repo-id=bar

[vagrant@dev ~]$ curl --user admin:admin https://dev.example.com/pulp/repos/bar/repodata/repomd.xml -i
HTTP/1.1 403 Forbidden
Date: Thu, 23 Mar 2017 19:43:57 GMT
Server: Apache/2.4.25 (Fedora) OpenSSL/1.0.2k-fips mod_wsgi/4.4.23 Python/2.7.13
Content-Length: 0
Content-Type: text/html; charset=utf-8

[vagrant@dev ~]$ curl https://dev.example.com/pulp/repos/bar/repodata/repomd.xml --cert /home/vagrant/certs/cl
ient.crt --key /home/vagrant/certs/client.key
<?xml version="1.0" encoding="UTF-8"?>
<repomd xmlns="http://linux.duke.edu/metadata/repo" xmlns:rpm="http://linux.duke.edu/metadata/rpm"><revision>1
490218171</revision>
<data type="filelists"><location href="repodata/3c5a3d87d0e93a6a3f0aceb78095c84df594a4b68d1fda1dae3117ad5b6eac
3d-filelists.xml.gz" /><timestamp>1490218171</timestamp><size>145</size><checksum type="sha256">3c5a3d87d0e93a
6a3f0aceb78095c84df594a4b68d1fda1dae3117ad5b6eac3d</checksum><open-size>124</open-size><open-checksum type="sh
a256">e2b3c5cc76abd55189dbe9be272ecb9b3cdbce84d32c2a03aa080d0ed6f8e511</open-checksum></data>
<data type="other"><location href="repodata/8a52c39f87df76e9b57185dacdec14654a001f4e0f23a6d2cbdf642c7a157e34-o
ther.xml.gz" /><timestamp>1490218171</timestamp><size>140</size><checksum type="sha256">8a52c39f87df76e9b57185
dacdec14654a001f4e0f23a6d2cbdf642c7a157e34</checksum><open-size>120</open-size><open-checksum type="sha256">b1
715ac8e6eaca8d4194d6b3add82d483d6ef3e7e6a214d46e0ed22f30a006d4</open-checksum></data>
<data type="primary"><location href="repodata/8dc7807b1f58effa31df6df5da80ea87731ecf600c2becf47166115d91f93787
-primary.xml.gz" /><timestamp>1490218171</timestamp><size>151</size><checksum type="sha256">8dc7807b1f58effa31
df6df5da80ea87731ecf600c2becf47166115d91f93787</checksum><open-size>166</open-size><open-checksum type="sha256
">9e9d5d6658e9c9221c3ee6116268f7445207f5c40b02d36f2a0991ac64889ee9</open-checksum></data>
<data type="updateinfo"><location href="repodata/36f5de7bdf0db8ae637f641dc862535811a9c616d2470ba69baf0ede72228
3e5-updateinfo.xml.gz" /><timestamp>1490218171</timestamp><size>92</size><checksum type="sha256">36f5de7bdf0db
8ae637f641dc862535811a9c616d2470ba69baf0ede722283e5</checksum><open-size>51</open-size><open-checksum type="sh
a256">f5922ee6f9f76089a8135e281dbd0e88ae4765166a8b9c66659de709cc556f08</open-checksum></data>
<data type="group"><location href="repodata/a27718cc28ec6d71432e0ef3e6da544b7f9d93f6bb7d0a55aacd592d03144b70-c
omps.xml" /><timestamp>1490218171</timestamp><size>124</size><checksum type="sha256">a27718cc28ec6d71432e0ef3e
6da544b7f9d93f6bb7d0a55aacd592d03144b70</checksum></data>
</repomd>
[vagrant@dev ~]$
```

[0] https://github.com/pulp/pulp/blob/master/server/etc/httpd/conf.d/pulp_content.conf#L16
[1] http://pulpproject.org/2011/05/18/pulp-protected-repositories/

#6 - 03/24/2017 04:05 PM - bmbouter

+1 to updating the old blog post. It would be a PR against this file:
https://github.com/pulp/pulpproject.org/blob/gh-pages/_posts/2011-05-18-pulp-protected-repositories.md

#8 - 03/24/2017 09:28 PM - bizhang

I just tested this with a client cert signed by a different CA, and it looks like this feature is broken. I would expect the request to fail because client.crt has been signed with a different CA.crt, but instead it succeeds

```
[vagrant@dev ~]$ curl https://dev.example.com/pulp/repos/bar/repodata/repomd.xml --cert /home/vagrant/certs2/c
lient.crt --key /home/vagrant/certs2/client.key
<?xml version="1.0" encoding="UTF-8"?>
<repomd xmlns="http://linux.duke.edu/metadata/repo" xmlns:rpm="http://linux.duke.edu/metadata/rpm"><revision>1
490218171</revision>
<data type="filelists"><location href="repodata/3c5a3d87d0e93a6a3f0aceb78095c84df594a4b68d1fda1dae3117ad5b6eac
3d-filelists.xml.gz" /><timestamp>1490218171</timestamp><size>145</size><checksum type="sha256">3c5a3d87d0e93a
6a3f0aceb78095c84df594a4b68d1fda1dae3117ad5b6eac3d</checksum><open-size>124</open-size><open-checksum type="sh
a256">e2b3c5cc76abd55189dbe9be272ecb9b3cdbce84d32c2a03aa080d0ed6f8e511</open-checksum></data>
<data type="other"><location href="repodata/8a52c39f87df76e9b57185dacdec14654a001f4e0f23a6d2cbdf642c7a157e34-o
ther.xml.gz" /><timestamp>1490218171</timestamp><size>140</size><checksum type="sha256">8a52c39f87df76e9b57185
dacdec14654a001f4e0f23a6d2cbdf642c7a157e34</checksum><open-size>120</open-size><open-checksum type="sha256">b1
715ac8e6eaca8d4194d6b3add82d483d6ef3e7e6a214d46e0ed22f30a006d4</open-checksum></data>
<data type="primary"><location href="repodata/8dc7807b1f58effa31df6df5da80ea87731ecf600c2becf47166115d91f93787
-primary.xml.gz" /><timestamp>1490218171</timestamp><size>151</size><checksum type="sha256">8dc7807b1f58effa31
df6df5da80ea87731ecf600c2becf47166115d91f93787</checksum><open-size>166</open-size><open-checksum type="sha256
">9e9d5d6658e9c9221c3ee6116268f7445207f5c40b02d36f2a0991ac64889ee9</open-checksum></data>
<data type="updateinfo"><location href="repodata/36f5de7bdf0db8ae637f641dc862535811a9c616d2470ba69baf0ede72228
3e5-updateinfo.xml.gz" /><timestamp>1490218171</timestamp><size>92</size><checksum type="sha256">36f5de7bdf0db
8ae637f641dc862535811a9c616d2470ba69baf0ede722283e5</checksum><open-size>51</open-size><open-checksum type="sh
a256">f5922ee6f9f76089a8135e281dbd0e88ae4765166a8b9c66659de709cc556f08</open-checksum></data>
<data type="group"><location href="repodata/a27718cc28ec6d71432e0ef3e6da544b7f9d93f6bb7d0a55aacd592d03144b70-c
omps.xml" /><timestamp>1490218171</timestamp><size>124</size><checksum type="sha256">a27718cc28ec6d71432e0ef3e
6da544b7f9d93f6bb7d0a55aacd592d03144b70</checksum></data>
</repomd>
```

#9 - 01/08/2018 05:31 PM - balonik

I spent several hours trying to setup protected repos using 2.14.3 and I must say that its not working at all.
The referenced blog post from 2011 is using incorect OID value.
1.3.6.1.4.1.2312.9.2.0000.1.6=ASN1:UTF8:repos/myRepo/
should be only
1.3.6.1.4.1.2312.9.2.0000.1.6=ASN1:UTF8:myRepo/
because Pulp strips the pulp/repos/ from the request as I found in bug report from 2012 - https://bugzilla.redhat.com/show_bug.cgi?id=790157

You cannot have unprotected repos when switching 'enabled: true' in /etc/pulp/repo_auth.conf. All repos require client cert with the extension from that point on (I must look why this works on RHUI3).

I don't trust the options --host-ca, --auth-ca and --auth-cert at all.
--auth-cert - I have used different certifcate than provided in the repo create command, with configured OIDs and it worked
--host-ca - I don't understand how this can be of importance to client verification
--auth-ca - this is ignored as well, I have used different CA cert in the repo create command, but the client cert is always checked against the cacert value in server.conf

#10 - 04/12/2019 10:18 PM - bmbouter

- Status changed from NEW to CLOSED - WONTFIX

Pulp 2 is approaching maintenance mode, and this Pulp 2 ticket is not being actively worked on. As such, it is being closed as WONTFIX. Pulp 2 is still accepting contributions though, so if you want to contribute a fix for this ticket, please reopen or comment on it. If you don't have permissions to reopen this ticket, or you want to discuss an issue, please reach out via the developer mailing list.

#11 - 04/15/2019 10:20 PM - bmbouter

- Tags Pulp 2 added

Files

dump	14.5 KB	03/21/2017	lenny