Packaging - Issue #1905

Streamer SSL cert not added to Pulp's trust store on RHEL 6

05/10/2016 10:26 PM - Ichimonji10

Status:	CLOSED - CURRENTRELEASE	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	elyezer	**Estimated time:**	0:00 hour
Category:			
Sprint/Milestone:			
Severity:	1. Low	**Groomed:**	No
Version - Packaging:	master	**Sprint Candidate:**	No
Platform Release:		**Tags:**	Pulp 2
Target Release - Packaging:		**Sprint:**	
OS:	RHEL 6	**Quarter:**	
Triaged:	Yes		

Description

The Pulp streamer has three components:

- Apache reverse proxy
- Squid proxy
- content streamer

All clients talk to Apache, whether that client be an end user or Pulp itself. One of Apache's duties is to provide SSL-encrypted communications. (Another is to forward requests to Squid as appropriate.) For this to work, the client must trust the SSL certificates presented by Apache.

When Pulp packaging is used to install Pulp and the Pulp streamer on a host, Pulp packaging updates the host's system trust store so that the client trusts the streamer. Unfortunately, this doesn't happen when the target host runs RHEL 6.

You can prove this to yourself by using Pulp packaging to install Pulp and the Pulp streamer on a RHEL 6 host, and then running the Pulp Smash test case pulp_smash.tests.rpm.api_v2.test_download_policies.BackgroundTestCase . This test case does the following:

1. Reset Pulp, including the Squid cache.
2. Create a repository with the “background” download policy.
3. Sync and publish the repository.
4. Download an RPM from the repository.

This test case will fail with two errors:

- test_request_history should show that the client was not redirected. However, the client is redirected. This indicates that Pulp doesn't have a requested file and is redirecting the client to the streamer.
- test_repo_local_units shows that not all files have been downloaded to Pulp itself.

These failures indicate that Pulp is failing to download some or all files from the Pulp streamer. Examining the logs on the Pulp server reinforces this suspicion. The following entries appear in the logs of a system for which everything is OK:

```
May 10 13:48:28 mgmt12.rhq.lab.eng.bos.redhat.com pulp[10091]: requests.packages.urllib3.connectio
npool:INFO: Starting new HTTPS connection (1): mgmt12.rhq.lab.eng.bos.redhat.com
May 10 13:48:28 pulp-streamer.example.com pulp[10091]: requests.packages.urllib3.connectionpool:IN
FO: Starting new HTTPS connection (2): pulp-streamer.example.com
May 10 13:48:28 pulp-streamer.example.com pulp[10091]: requests.packages.urllib3.connectionpool:IN
FO: Starting new HTTPS connection (3): pulp-streamer.example.com
May 10 13:48:28 pulp-streamer.example.com pulp[10091]: requests.packages.urllib3.connectionpool:IN
FO: Starting new HTTPS connection (4): pulp-streamer.example.com
May 10 13:48:28 pulp-streamer.example.com pulp[10091]: requests.packages.urllib3.connectionpool:IN
FO: Starting new HTTPS connection (5): pulp-streamer.example.com
May 10 13:48:29 pulp-streamer.example.com pulp_streamer[6548]: requests.packages.urllib3.connectio
npool:INFO: Starting new HTTPS connection (1): repos.fedorapeople.org
```

```
May 10 13:48:29 pulp-streamer.example.com pulp_streamer[6548]: requests.packages.urllib3.connectio
npool:INFO: Starting new HTTPS connection (2): repos.fedorapeople.org
May 10 13:48:29 pulp-streamer.example.com pulp_streamer[6548]: requests.packages.urllib3.connectio
npool:INFO: Starting new HTTPS connection (3): repos.fedorapeople.org
May 10 13:48:29 pulp-streamer.example.com pulp_streamer[6548]: requests.packages.urllib3.connectio
npool:INFO: Starting new HTTPS connection (4): repos.fedorapeople.org
May 10 13:48:29 pulp-streamer.example.com pulp_streamer[6548]: requests.packages.urllib3.connectio
npool:INFO: Starting new HTTPS connection (5): repos.fedorapeople.org
```

These log items show Pulp making requests to the Pulp streamer, which then makes requests to the source repository. On RHEL 6, the following log entries appear:

```
May 10 13:49:48 pulp-streamer pulp: requests.packages.urllib3.connectionpool:INFO: Starting new HT
TPS connection (1): pulp-streamer.example.com
May 10 13:49:48 pulp-streamer pulp: requests.packages.urllib3.connectionpool:INFO: Starting new HT
TPS connection (2): pulp-streamer.example.com
May 10 13:49:48 pulp-streamer pulp: requests.packages.urllib3.connectionpool:INFO: Starting new HT
TPS connection (3): pulp-streamer.example.com
May 10 13:49:48 pulp-streamer pulp: requests.packages.urllib3.connectionpool:INFO: Starting new HT
TPS connection (4): pulp-streamer.example.com
May 10 13:49:48 pulp-streamer pulp: requests.packages.urllib3.connectionpool:INFO: Starting new HT
TPS connection (5): pulp-streamer.example.com
May 10 13:49:48 pulp-streamer pulp: nectar.downloaders.threaded:WARNING: Skipping requests to pulp
-streamer.example.com due to repeated connection failures: [Errno 1] _ssl.c:492: error:14090086:SS
L routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
May 10 13:49:48 pulp-streamer pulp: nectar.downloaders.threaded:WARNING: Skipping requests to pulp
-streamer.example.com due to repeated connection failures: [Errno 1] _ssl.c:492: error:14090086:SS
L routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
May 10 13:49:48 pulp-streamer pulp: nectar.downloaders.threaded:WARNING: Skipping requests to pulp
-streamer.example.com due to repeated connection failures: [Errno 1] _ssl.c:492: error:14090086:SS
L routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
May 10 13:49:48 pulp-streamer pulp: nectar.downloaders.threaded:WARNING: Skipping requests to pulp
-streamer.example.com due to repeated connection failures: [Errno 1] _ssl.c:492: error:14090086:SS
L routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
May 10 13:49:48 pulp-streamer pulp: nectar.downloaders.threaded:WARNING: Skipping requests to pulp
-streamer.example.com due to repeated connection failures: [Errno 1] _ssl.c:492: error:14090086:SS
L routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

So - why is Pulp failing to fetch files from the streamer? Which component is broken? The broken component appears to be the system trust store. On a functioning system:

```
$ openssl s_client -connect $(hostname --long):443
[…]
    Verify return code: 0 (ok)
[…]
```

On RHEL 6:

```
$ openssl s_client -connect $(hostname --long):443
[…]
    Verify return code: 21 (unable to verify the first certificate)
[…]
```

Let's fix Pulp packaging so that it correctly updates the system trust store. This will allow Pulp to communicate with the Pulp streamer.

History

#1 - 05/13/2016 05:14 PM - dkliban@redhat.com

- Priority changed from Normal to High

- Severity changed from 2. Medium to 1. Low

- Triaged changed from No to Yes

#2 - 05/19/2016 03:19 PM - jcline@redhat.com

Ran across this for other reasons: https://access.redhat.com/solutions/1174393

Looks like there's an extra step or two on el6 to update the trust store.

#3 - 05/25/2016 02:07 AM - elyezer

I have submitted the PR [1] to fix the certificate trust on RHEL6 based systems. Also the PR adds a check to make sure the certificate is trusted by running openssl s_client.

[1] https://github.com/pulp/pulp_packaging/pull/168

#4 - 05/25/2016 02:07 PM - bmbouter

Is there also a code change needed in a repo other than pulp_packaging?

#5 - 05/25/2016 04:49 PM - jcline@redhat.com

bmbouter wrote:

> Is there also a code change needed in a repo other than pulp_packaging?

No, this should be everything.

#6 - 05/25/2016 07:27 PM - bmbouter

- Status changed from NEW to CLOSED - CURRENTRELEASE

- Assignee set to elyezer

The only fix needed is already merged so I'm moving to MODIFIED. We aren't referencing the commit as usual because the commit is in the pulp_packaging repo so we can't reference it. Also, it's not in any code going into any specific release so it doesn't actually have a Target Platform Release set.

#7 - 05/26/2016 04:22 PM - lchimonji10

I can verify that this bug is fixed as of last night's Jenkins test runs. The relevant tests which were blocked by this test ran. (They passed, too. :-)

#8 - 04/15/2019 10:30 PM - bmbouter

- Tags Pulp 2 added