CertGuard - Story #4009

Story # 3968 (CLOSED - CURRENTRELEASE): As a Pulp user, I can protect content I have stored in Pulp

Make CertGuard capabilities in Pulp3

09/13/2018 11:33 PM - bmbouter

Status:	CLOSED - CURRENTRELEASE	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	jortel@redhat.com	**% Done:**	100%
Category:		**Estimated time:**	0:00 hour
Sprint/Milestone:	1.0.0 Release		
Platform Release:		**Tags:**	
Groomed:	Yes	**Sprint:**	Sprint 47
Sprint Candidate:	No	**Quarter:**	

Description

In RPM for Pulp2, there is a WSGIAccessScript that uses the client script to verify the client's right to access a specific URL. This should be a RPM-specific guard that is provided by the RPM plugin.

In Pulp2 here are some links that are related:

https://github.com/pulp/pulp/tree/2-master/repoauth/pulp/repoauth <--- the actual checking code itself
https://github.com/pulp/pulp_rpm/blob/2-master/plugins/etc/httpd/conf.d/pulp_rpm.conf#L48 <---- the httpd WSGIAccessScript

We need to get some test data posted on here that can be used for development.

For crypto the Red Hat security team has recommended: https://pypi.org/project/cryptography/ as a portable crypto library for Python.

This should inherit from ContentGuard and be discoverable by core as an available ContentGuard.

Here are some field names:

class OidContentGuard(ContentGuard):

- name 32 Charfield
- CA certificate - TextFile (not a path) <------ note this is uploaded by the user

Related issues:

Blocked by Pulp - Story #4074: As a user, the content guard logic needs to be...	**CLOSED - CURRENTRELEASE**
Copied to CertGuard - Test #4363: Test the RHSMCertGuard	**CLOSED - DUPLICATE**

Associated revisions

Revision 53986229 - 01/16/2019 12:45 AM - jortel@redhat.com

Add content guard. closes #4009

History

#1 - 09/13/2018 11:37 PM - bmbouter

- Parent task set to #3968

#2 - 09/14/2018 04:45 PM - bmbouter

- Tracker changed from Issue to Story

- % Done set to 0

Converted to story at triage

#3 - 09/14/2018 06:25 PM - bmbouter

- Description updated

#4 - 09/14/2018 06:34 PM - bmbouter

- Description updated

#5 - 09/14/2018 06:40 PM - daviddavis

- Groomed changed from No to Yes

- Sprint set to Sprint 43

#6 - 10/18/2018 09:13 PM - amacdona@redhat.com

- Sprint changed from Sprint 43 to Sprint 44

#7 - 10/18/2018 10:24 PM - jortel@redhat.com

- Blocked by Story #4074: As a user, the content guard logic needs to be loaded and used by the content app. added

#8 - 11/06/2018 07:38 PM - daviddavis

- Sprint changed from Sprint 44 to Sprint 45

#9 - 11/26/2018 05:50 PM - jortel@redhat.com

Is this really specific to RPM content only? If not, perhaps this content-guard should be contributed by a separate plugin?

#10 - 11/26/2018 06:38 PM - bmbouter

I think it's more broadly useful to other plugins. I also think that until another plugin actually wants to use it, shipping it along with RPM is a very easy thing to do now. The packaging, release bumping, release note-ing, travis overhead can be a lot to do.

When we do go to make it, it's own package and repo, I highly recommend using cookiecutter which is how I generated the generic package for the pulp_streamer.

#11 - 11/26/2018 06:48 PM - bmbouter

I had some questions about where the cert will be checked, and if we are sure that Pulp needs to provide custom code to do that type of checking?

In terms of where the checking is happening, I've been wondering lately about if Pulp should be doing cert validation in its WSGI process or outside of it. In Pulp2 the WSGIAccessScript was code Pulp provided but it was run "outside" of the Pulp WSGI process. Or are we validating the cert "inside" the Pulp WSGI process in Pulp's Django view code?

Also does Pulp have to provide code on how to check an OidCertificateGuard or can Apache validate an OidCertificateGuard like a nomral cert without Pulp providing a custom WSGIAccessScript?
I have the same quesiton for nginx as well.

#12 - 11/26/2018 09:51 PM - jortel@redhat.com

It's been my understanding that the primary motivation behind pulp3 *ContentGuards* was to provide content protection in a way that was independent of the web server. Mainly, that complicated apache/nginx configurations and access scripts would not be necessary. To fully achieve this, it seems that an SSL based ContentGuard should have the capability to validate the certificate in addition to the specialized things such as OID matching. I would expect the certificate validation to be enabled/disabled through the guard attributes. When content protection starts to require mod-ssl configurations and/or access scripts, I no longer see the value of *ContentGuards*.

#13 - 11/27/2018 06:06 PM - jortel@redhat.com

- Status changed from NEW to ASSIGNED

- Assignee set to jortel@redhat.com

#14 - 11/27/2018 09:43 PM - bmbouter

jortel@redhat.com wrote:

> It's been my understanding that the primary motivation behind pulp3 *ContentGuards* was to provide content protection in a way that was independent of the web server. Mainly, that complicated apache/nginx configurations and access scripts would not be necessary. To fully achieve this, it seems that an SSL based ContentGuard should have the capability to validate the certificate in addition to the specialized things such as OID matching. I would expect the certificate validation to be enabled/disabled through the guard attributes. When content protection starts to require mod-ssl configurations and/or access scripts, I no longer see the value of *ContentGuards*.

I totally agree with this reasoning. So this means authorization for content guards are checked "inside" Pulp's Content app.

Is the plan to only use the cryptography Python library mentioned in the ticket? That is a Python dependency so that I think would work well.

#15 - 11/28/2018 12:02 AM - jortel@redhat.com

Looking into the cryptography package, it does not seem to support certificate validation.

[1] https://github.com/pyca/cryptography/issues/2381

#16 - 11/28/2018 04:06 PM - daviddavis

- Tags Pulp 3 RC Blocker added

#17 - 11/29/2018 03:31 PM - rchan

- Sprint changed from Sprint 45 to Sprint 46

#18 - 11/29/2018 04:15 PM - bmbouter

In discussing making this its own python package that ships separately from RPM, here are some questions we came up with:

1. What will the PyPI package name be? e.g. for the streamer it's pulp_streamer
2. What will the python package path be? e.g. for the streamer it's pulpcore.streamer
3. What will the repo name be? I recommend the same as (1)
4. Which github team will have write perms to that repo?
5. Where will issues for it be filed?

#19 - 11/29/2018 07:46 PM - jortel@redhat.com

bmbouter wrote:

> In discussing making this its own python package that ships separately from RPM, here are some questions we came up with:
>
> 1. What will the PyPI package name be? e.g. for the streamer it's pulp_streamer

pulp_oidguard

> 2. What will the python package path be? e.g. for the streamer it's pulpcore.streamer

pulp_oidguard

> 3. What will the repo name be? I recommend the same as (1)

pulp_oidguard

> 4. Which github team will have write perms to that repo?

I recommend we have a new team of 2-3.

> 5. Where will issues for it be filed?

My first thought is a new project in pulp.plan.io but wondering if we should consider just using github issues.

#20 - 11/30/2018 03:29 PM - bmbouter

@jortel, all those answers look great, ty.

+1 to using Redmine as a tracker for consistency. Let me know if you need any help setting that up, there are a few strange configuration points.

#21 - 12/03/2018 08:34 PM - jortel@redhat.com

Let's consider an attribute (setting) on the guard to enable/disable OID/path matching. This supports the guard also being useful to users only needing the client certificate validation part. Given this, I wonder if the name should be more focused on SSL/certificate (more broadly) and less on the OID/path matching. Perhaps: *pulp_sslguard* would be more appropriate.

Thoughts?

#22 - 12/03/2018 08:59 PM - bmbouter

jortel@redhat.com wrote:

> Let's consider an attribute (setting) on the guard to enable/disable OID/path matching. This supports the guard also being useful to users only needing the client certificate validation part. Given this, I wonder if the name should be more focused on SSL/certificate (more broadly) and less on the OID/path matching. Perhaps: *pulp_sslguard* would be more appropriate.

> Thoughts?

+1 to a setting to disable the OID/path matching. I think it should by default do the checking so that could turn it off.

Renaming I think makes sense. I really like the "certificate" or "cert" in the name over SSL because strictly speaking we're not doing SSL. Maybe *pulp-certguard* or *pulp-cert-guard* which would be either *pulp_certguard* or *pulp_cert_guard* respectively as package names?

What do you think?

#23 - 12/03/2018 09:03 PM - jortel@redhat.com

The name pulp-certguard (or pulp_certguard) works for me.

#24 - 12/03/2018 09:04 PM - bmbouter

That works for me also.

#26 - 12/12/2018 03:54 PM - jortel@redhat.com

- Project changed from RPM Support to CertGuard

#27 - 01/04/2019 10:06 PM - rchan

- Sprint changed from Sprint 46 to Sprint 47

#28 - 01/18/2019 03:30 PM - jortel@redhat.com

- Status changed from ASSIGNED to MODIFIED

- % Done changed from 0 to 100

Applied in changeset 53986229dbac8fc653382b66266bce3a3a2936d8.

#29 - 01/22/2019 11:02 PM - jortel@redhat.com

- Tags Pulp 3 added

#30 - 01/30/2019 03:46 PM - bherring

- Copied to Test #4363: Test the RHSMCertGuard added

#31 - 04/10/2019 10:39 PM - bmbouter

- Subject changed from Make a OidCertificateGuard that is ported from Pulp2 to Make CertGuard capabilities in Pulp3

retitling this because another issue actually providing the OID Certificate functionality so I want to retitle this for clarity.

#32 - 04/10/2019 10:41 PM - bmbouter

- Sprint/Milestone set to 1.0.0 Release

#33 - 04/26/2019 10:34 PM - bmbouter

- Tags deleted (Pulp 3)

#34 - 07/21/2020 10:16 PM - bmbouter

- Status changed from MODIFIED to CLOSED - CURRENTRELEASE