Pulp - Story #5974

As a user, I can restrict file:/// to one or more specific paths

01/13/2020 04:59 PM - bmbouter

Status:	CLOSED - CURRENTRELEASE	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	bmbouter	**% Done:**	100%
Category:		**Estimated time:**	0:00 hour
Sprint/Milestone:	3.1.0		
Platform Release:		**Tags:**	
Groomed:	No	**Sprint:**	Sprint 65
Sprint Candidate:	No	**Quarter:**	

Description

At the system level, default to denying file import from file:/// unless a subpath of one or more declared approved paths. The list of approved paths will live in settings as it's a system-wide thing.

Example whitelisting importing from /mnt/ and /anotherdir/

ALLOWED_IMPORT_PATHS = ['/mnt/', '/anotherdir/']

Then any file:/// sync that starts with '/mnt/' or '/anotherdir/', e.g. file:///mnt/foo/ or file:///anotherdir/bar/PULP_MANIFEST would sync.

Each path listed in ALLOWED_IMPORT_PATHS must be absolute

Default

For safety reasons, this would be disabled by default and administrators need to opt-in to its use.

ALLOWED_IMPORT_PATHS = []

Validation checking at Remote save-time and runtime

The Remote serializer needs to validate at save time. Also that validation needs to be performed at runtime. It's this second check that will handle any existing Remote's with invalid paths already saved in the DB in a reasonable way.

Associated revisions

Revision b7db663a - 01/29/2020 11:30 PM - bmbouter

Adds ALLOWED_IMPORT_PATHS for file:// urls

Remote.url now validate to only allow file:// paths that are a subpath of a configured ALLOWED_IMPORT_PATHS setting. This setting comes with docs. URLs starting with other protocol handlers, e.g. http:// or https:// are unaffected.

https://pulp.plan.io/issues/5974 closes #5974

History

#1 - 01/13/2020 05:00 PM - bmbouter

- Description updated

#2 - 01/13/2020 05:08 PM - bmbouter

- Description updated

Question 1: symlinks

How/where should we prevent the file:/// import processes from following symlinks. If we follow symlinks users could perhaps break out of the constraint this feature creates. Should that be its own piece of work separate from this?

Question 2: disallowing ..

Also what about disallowing .. from file:/// urls at all through validation? Should we make that part of this story also?

#3 - 01/14/2020 06:57 PM - bmbouter

- Sprint/Milestone set to 3.1.0

#4 - 01/15/2020 05:44 PM - gmbnomis

I think restricting the allowed paths by configuration is a good idea (if it is ok for the use cases that this feature should support). And disabling it by default is the safest option.

bmbouter wrote:

> ## Question 1: symlinks
>
> How/where should we prevent the file:/// import processes from following symlinks. If we follow symlinks users could perhaps break out of the constraint this feature creates. Should that be its own piece of work separate from this?

I would like to have it part of this piece of work, as the protection offered without is basically none. Please see https://pulp.plan.io/issues/3841#note-11 **and** the problem mentioned in https://pulp.plan.io/issues/3841#note-12 for an implementation that could help here (using realpath to resolve symlinks). Normalizing via realpath() would probably need to happen for both the file URI to check as well as the configured allowed paths.

> ## Question 2: disallowing ..
>
> Also what about disallowing .. from file:/// urls at all through validation? Should we make that part of this story also?

We could do, but using realpath() will normalize .. away anyway.

#5 - 01/27/2020 08:48 PM - bmbouter

- Status changed from NEW to ASSIGNED

- Assignee set to bmbouter

- Sprint set to Sprint 65

Adding 3.1 story to sprint since I have capacity to complete it.

#6 - 01/27/2020 10:32 PM - bmbouter

- Status changed from ASSIGNED to POST

PR available at: https://github.com/pulp/pulpcore/pull/520

#7 - 01/30/2020 12:11 AM - bmbouter

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset pulpcore|b7db663aa87bbd0e74069c501d4f1b9b317b8779.

#8 - 01/31/2020 12:25 PM - bmbouter

- Status changed from MODIFIED to CLOSED - CURRENTRELEASE