

Pulp - Story #8246

Task # 7960 (CLOSED - COMPLETE): FIPS and support for ALLOWED_CONTENT_CHECKSUMS

As a user, I do not have md5 and sha1 in ALLOWED_CONTENT_CHECKSUMS by default

02/11/2021 10:13 PM - bmbouter

Status:	CLOSED - CURRENTRELEASE	Start date:	
Priority:	Normal	Due date:	
Assignee:	bmbouter	% Done:	100%
Category:		Estimated time:	0:00 hour
Sprint/Milestone:	3.11.0	Tags:	
Platform Release:		Sprint:	Sprint 90
Groomed:	No	Quarter:	
Sprint Candidate:	No		

Description

Current State

Currently the [ALLOWED_CONTENT_CHECKSUMS](#) contains ["md5", "sha1", "sha224", "sha256", "sha384", "sha512"] in [the settings file](#).

Also the [CI adjusts this default to remove MD5](#) from this list, and there are tests which expect that MD5 to be disincluded.

Removing MD5 and SHA1

We want to make Pulp secure by default. MD5 is known to be insecure, and therefore it is unsafe for Pulp to allow its use for calculating package integrity by default. SHA-1 is widely believed to be insecure, or will be soon, and should not be allowed by default for the same reason.

Future State

- MD5 and SHA1 will no longer be in ALLOWED_CONTENT_CHECKSUMS by default.
- The CI will no longer set this setting as it is not required.

Associated revisions

Revision e5346955 - 02/12/2021 09:10 PM - bmbouter

Removes md5 and sha1 from checksum defaults

The md5 and sha1 checksums are not considered secure and therefore should not be included as available hashers for Pulp to perform Artifact integrity checks with.

This PR:

- Removes them from the default in settings
- Updates the ALLOWED_CONTENT_CHECKSUMS settings documentation.
- Re-applies the plugin_templat to no longer modify the set of allowed checksums in the CI environment.

closes #8246

History

#1 - 02/11/2021 10:14 PM - bmbouter

- Status changed from NEW to ASSIGNED
- Assignee set to bmbouter

#2 - 02/11/2021 10:14 PM - bmbouter

- Description updated

#3 - 02/11/2021 11:23 PM - pulpbot

- Status changed from ASSIGNED to POST

PR: <https://github.com/pulp/pulpcore/pull/1123>

#4 - 02/12/2021 09:11 PM - bmbouter

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset [pulpcore|e5346955562b7786efea251a4a37356c47f6e256](#).

#5 - 02/22/2021 04:22 PM - daviddavis

- Sprint set to Sprint 90

#6 - 03/15/2021 01:37 PM - ipanova@redhat.com

- Sprint/Milestone set to 3.11.0

#7 - 03/16/2021 07:55 PM - ipanova@redhat.com

- Status changed from MODIFIED to CLOSED - CURRENTRELEASE