RPM Support - Issue #9206

Repodata signing is broken if sqlite is enabled

08/04/2021 02:09 AM - rmcgover

Status:	NEW	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0:00 hour
Category:			
Sprint/Milestone:			
Severity:	2. Medium	**Groomed:**	No
Version:	2.21.1	**Sprint Candidate:**	No
Platform Release:		**Tags:**	Pulp 2
OS:		**Sprint:**	Sprint 107
Triaged:	Yes	**Quarter:**	

Description

In Pulp2, if a repo has repodata signing enabled via gpg_sign_metadata: true, and also has sqlite enabled via generate_sqlite: true, then the published signatures are invalid.

Steps to reproduce

- Enable GPG signing of repodata for a repo, with valid setup, per https://docs.pulpproject.org/en/2.21/plugins/pulp_rpm/tech-reference/yum-plugins.html#gpg-signing-of-repository-metadata
- Enable sqlite generation for a repo by setting generate_sqlite: true.
- Publish repo.
- Download repomd.xml, repomd.xml.asc and attempt to verify the signature.

Actual behavior

Signature verification fails.

Expected behavior

Signature verification succeeds.

Additional info

It's broken because the signing occurs on an intermediate version of repomd.xml rather than the final form.

It can be easily observed by inspection of the publish steps in BaseYumRepoPublisher:
https://github.com/pulp/pulp_rpm/blob/5c5a7dcc058b29d89b3a913d29cfcab41db96686/plugins/pulp_rpm/plugins/distributors/yum/publish.py#L46

Here's the last few steps of that publisher, with added comments:

```
        self.add_child(PublishModulesStep())
        self.add_child(PublishCompsStep())
        self.add_child(PublishMetadataStep())
        self.add_child(CloseRepoMetadataStep())  # finalizes repomd.xml and creates repomd.xml.asc
        self.add_child(GenerateSqliteForRepoStep(self.get_working_dir()))  # rewrites repomd.xml t
o add sqlite, invalidating signature
        self.add_child(RemoveOldRepodataStep())
```

Though CloseRepoMetadataStep treats repomd.xml as "final" and ready for signing, if generate_sqlite is enabled then the very next step will overwrite repomd.xml with different content (generated by sqliterepo_c command) and will not redo the signing, meaning the signature will never be correct.

History

#1 - 08/05/2021 05:36 PM - dalley

- Triaged changed from No to Yes

- Sprint set to Sprint 102

#2 - 08/12/2021 05:23 PM - rchan

- Sprint changed from Sprint 102 to Sprint 103

#3 - 08/27/2021 05:08 PM - rchan

- Sprint changed from Sprint 103 to Sprint 104

#4 - 09/10/2021 12:28 AM - rchan

- Sprint changed from Sprint 104 to Sprint 105

#5 - 09/23/2021 11:54 PM - rchan

- Sprint changed from Sprint 105 to Sprint 106

#6 - 10/08/2021 03:16 PM - rchan

- Sprint changed from Sprint 106 to Sprint 107