Pulp - Task #8704

Task # 8732 (CLOSED - COMPLETE): [EPIC] As a user, I can rest easy with all sensitive credentials in the database encrypted at rest

Installer: create a key for pulp to use when encrypting sensitive db fields

05/05/2021 07:47 PM - daviddavis

Status:	CLOSED - CURRENTRELEASE	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	mdepaulo@redhat.com	**% Done:**	100%
Category:	Installer - Moved to GitHub issues	**Estimated time:**	0:00 hour
Sprint/Milestone:	3.14.0		
Platform Release:		**Tags:**	
Groomed:	No	**Sprint:**	Sprint 98
Sprint Candidate:	No	**Quarter:**	

Description

#8192 encrypts fields in our database using a private key. We need to have the installer generate this key. Pulp will read in this key and use it to encrypt/decrypt sensitive fields in our database.

From #8192:

> The private key will need to be generated at install time. We need to determine where to keep these by default securely. They need to be readable by code without a human involved.

Associated revisions

Revision f196208b - 06/07/2021 11:17 PM - Mike DePaulo

Create or import a key for pulp-api to use when

encrypting sensitive db fields.

Introduces new variables pulp_db_fields_key & pulp_db_fields_key_remote.

fixes: #8704 Create a key for pulp to use when encrypting sensitive db fields https://pulp.plan.io/issues/8704

Revision f196208b - 06/07/2021 11:17 PM - Mike DePaulo

Create or import a key for pulp-api to use when

encrypting sensitive db fields.

Introduces new variables pulp_db_fields_key & pulp_db_fields_key_remote.

fixes: #8704 Create a key for pulp to use when encrypting sensitive db fields https://pulp.plan.io/issues/8704

Revision 9a7291f9 - 06/11/2021 09:02 PM - daviddavis

Use openssl to generate db key

ref #8704

Revision 9a7291f9 - 06/11/2021 09:02 PM - daviddavis

Use openssl to generate db key

ref #8704

Revision b45ade85 - 06/30/2021 11:30 AM - William Bradford Clark

Use url-safe base64 encoding for Fernet key

Fernet.generate_key() (from Python's cryptography.fernet module) generates 32 pseudorandom bytes in url-safe base64-encoded form, i.e. using the url-safe base64 alphabet described in https://datatracker.ietf.org/doc/html/rfc4648#section-5

This commit converts the output from the openssl command used to generate the Fernet key to the same url-safe base64 alphabet. This is technically not required as Python's urlsafe_b64decode function will translate to the url-safe alphabet when loading the key; however we might as well store the key using the same base64 alphabet which is used internally by cryptography.frenet

refs: #8704

Revision b45ade85 - 06/30/2021 11:30 AM - William Bradford Clark

Use url-safe base64 encoding for Fernet key

Fernet.generate_key() (from Python's cryptography.fernet module) generates 32 pseudorandom bytes in url-safe base64-encoded form, i.e. using the url-safe base64 alphabet described in https://datatracker.ietf.org/doc/html/rfc4648#section-5

This commit converts the output from the openssl command used to generate the Fernet key to the same url-safe base64 alphabet. This is technically not required as Python's urlsafe_b64decode function will translate to the url-safe alphabet when loading the key; however we might as well store the key using the same base64 alphabet which is used internally by cryptography.frenet

refs: #8704

Revision e61d7fdc - 06/30/2021 11:34 AM - William Bradford Clark

Fix typo in pulp_db_fields_key documentation

refs: #8704

Revision e61d7fdc - 06/30/2021 11:34 AM - William Bradford Clark

Fix typo in pulp_db_fields_key documentation

refs: #8704

Revision b6e7a069 - 06/30/2021 11:43 AM - William Bradford Clark

Use 0640 filemode for Fernet keyfile

refs: #8704

Revision b6e7a069 - 06/30/2021 11:43 AM - William Bradford Clark

Use 0640 filemode for Fernet keyfile

refs: #8704

History

#1 - 05/05/2021 07:49 PM - daviddavis

- Blocks Story #8192: Add code to pulpcore that uses the db key to encrypt fields added

#2 - 05/10/2021 04:27 PM - daviddavis

Here's how to generate the key:

```
dd if=/dev/urandom bs=32 count=1 2>/dev/null | openssl base64
```

#3 - 05/11/2021 09:25 PM - mdepaulo@redhat.com

- Assignee set to mdepaulo@redhat.com

#4 - 05/11/2021 09:25 PM - daviddavis

- Blocks deleted (Story #8192: Add code to pulpcore that uses the db key to encrypt fields)

#5 - 05/11/2021 09:25 PM - daviddavis

- Parent task set to #8192

#6 - 05/11/2021 09:27 PM - mdepaulo@redhat.com

Needs to be done by the end of sprint 97. (per daviddavis)

#7 - 05/14/2021 05:34 PM - rchan

- Sprint changed from Sprint 96 to Sprint 97

#8 - 05/24/2021 09:32 PM - daviddavis

- Status changed from NEW to ASSIGNED

#9 - 06/02/2021 06:03 PM - rchan

- Sprint changed from Sprint 97 to Sprint 98

#10 - 06/07/2021 08:40 PM - pulpbot

- Status changed from ASSIGNED to POST

PR: https://github.com/pulp/pulp_installer/pull/645

#11 - 06/08/2021 08:46 PM - daviddavis

- Subject changed from Create a key for pulp to use when encrypting sensitive db fields to Installer: create a key for pulp to use when encrypting sensitive db fields

#12 - 06/10/2021 04:21 PM - Anonymous

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset ansible-pulp|f196208b282b702fcebc00d84d048a6ea59126ae.

#13 - 06/11/2021 09:24 PM - pulpbot

PR: https://github.com/pulp/pulp_installer/pull/652

#14 - 06/15/2021 04:14 PM - bmbouter

- Sprint/Milestone set to 3.14.0

#15 - 07/01/2021 05:52 PM - bmbouter

- Status changed from MODIFIED to CLOSED - CURRENTRELEASE

#16 - 08/11/2021 07:38 PM - daviddavis

- Parent task changed from #8192 to #8732