CL'SO

Ceph-CSI Support for AES-GCM: Challenges and Opportunities

David Mohren | DevOps Engineer
November, 2025

What to Expect?

- Talk is about making **data at rest more secure** in Ceph-CSI
- Concepts also applicable to other parts of Ceph
- Beginners welcome
  - Give intro in
    - Cryptographic Basics
    - Ceph-CSI
- Important to note throughout this presentation I will talk about integrity
  - This refers to cryptographic integrity
  - Not protecting data against bit flips but malicious modifications

CL'SO

Content

Context: Information Security

- Confidentiality
  - Only authorized may understand
- **(Cryptographic)** Integrity
  - Only authorized may modify
- Availability
  - Information has to be accessible in a timely manner manner

CIA-Triad

What is AES-GCM?

- AES-GCM
  - Protects Data Confidentiality
  - Protects Data Integrity
- Other cipher typically only establish confidentiality
- This type of cipher is called “Authenticated Encryption with Associated Data” (AEAD)

- But there are other means of achieving this…

Motivation: Useful for Ceph?

- Customer wants to create a highly secure in-house cloud system
  - They want to be BSI compliant

- BSI TR-02102-1 Guidelines
  - "The use of a volume encryption alone is only recommended if it includes effective ***cryptographic protection against data manipulation*** [...]"
  - "[It], is generally recommended to provide [...] mechanisms for data authentication in the overall system."

Motivation: Useful for Ceph?

- EU's Digital Operational Resilience Act (DORA)
  - Became effective 17th of January 2025
  - "Ensures that banks, insurance companies, investment firms and other financial entities can **withstand, respond to, and recover** from [...] **cyberattacks or system failures**"

- Article 5 (2) (b) "[The management body shall] put in place policies that aim to ensure the maintenance of high standards of availability, **authenticity, integrity** and confidentiality, of data;"

How to establish Data Confidentiality & Integrity?

CLYSO

AES-GCM Limits…

1. AES-GCM can only encrypt a limited amount of data per key

1. So what can we do with?

1. What else should we use to encrypt storage data?

You can also read about this in TR-02102

Google

aes gcm limits

All Images Videos News Short videos Forums Web More Tools

AI Overview

AES-GCM's primary limit is that **it can only encrypt 64 GiB of data per key** before security guarantees degrade, and that a unique **nonce must be used for every encryption with the same key** to prevent attacks. This nonce uniqueness requirement makes key lifetime critical, with recommendations to limit a key's usage to roughly 2^32 messages for robust security, though this can vary depending on message size and nonce construction.

Data Size Limit

- **64 GiB Maximum:** For any given key and nonce, AES-GCM is limited to encrypting a maximum of 64 GiB (2^39 - 256 bits) of plaintext.
- **Lifetime Limit:** Over the lifetime of a key, the total number of blocks of plaintext and associated data should be limited, with a common upper bound being 2^64 blocks.

Nonce Uniqueness

- **Critical Requirement:** Using the same nonce (initialization vector) with the same key for different messages is catastrophic and completely breaks the security of the GCM scheme.

distributed systems, some applications use alternatives like AES-GCM-SIV, which is specifically designed to be resistant to nonce misuse, according to the Cryptology ePrint Archive.

Authentication Tag Length

- **Security Parameter:** The length of the authentication tag (t) is a security parameter, with recommended values of 128, 120, 112, 104, or 96 bits.
- **Shorter Tags Discouraged:** Using shorter authentication tags significantly weakens the authentication strength of AES-GCM.

Key Lifetime Considerations

- **Deterministic vs. Random Nonces:** The maximum number of messages per key depends on the nonce construction:
  - **Random Construction:** A random nonce requires at least 12 bytes of entropy, with a maximum of roughly 2^32 messages per key.
  - **Deterministic Construction:** A deterministic (counter-based) construction can allow for more messages but introduces its own limits based on counter size, with 2^32 or 2^S (where S is the counter bit length), whichever is smaller, being the maximum.

Galois/Counter Mode - Wikipedia
GCM is proven secure in the concrete security model. It is secure when it is used with a block...
Wikipedia

How long is Key lifetime of AES-GCM key?
22 Jan 2019 — If two computers use the AES-GCM to encrypt exchange messages, then what is the key's lifetime of AES-...
Information Security Stack Exchan...

AES-GCM-SIV: Specification and Analysis
This addition allows for encrypting up to 250 messages with the same key, compared to the significant limitation of only...
Cryptology ePrint Archive

Show all

Alternatives to AES-GCM

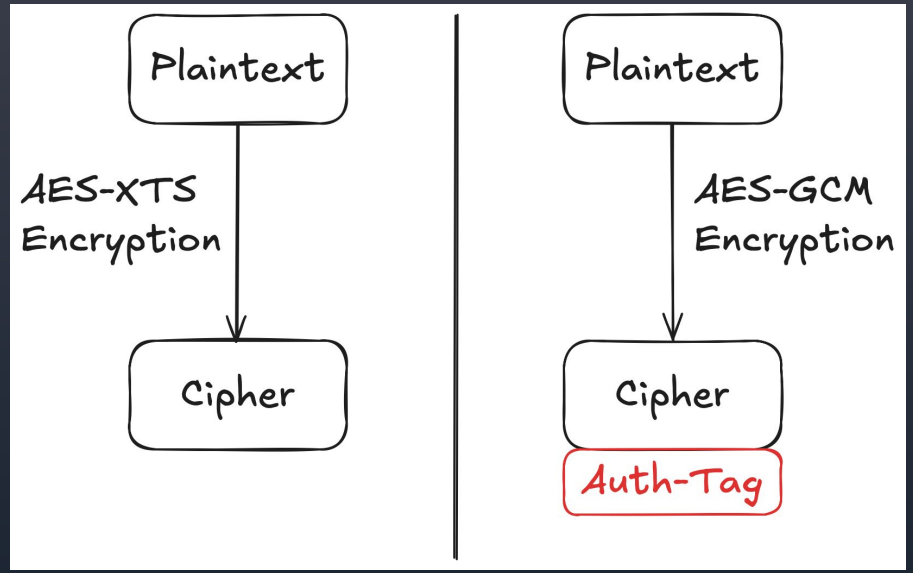
- Compound methods
  - Use traditional cipher like AES-XTS
  - Combine it with an HMAC

- Usage of AEAD ciphers
  - “Combine” Encryption with Tagging computation
  - Typically faster than performing Tagging and Encryption separate
  - For example: AES-GCM-SIV, XChaCha20-Poly1305

Tagging Problems…

- Methods to protect Integrity results in a ciphertext expansion
  - Extra length comes from authentication tag

- Major challenge behind Integrity protection



Example AES-XTS Encryption vs. AES-GCM

How to Integrate such Approaches into Ceph-CSI?

Kubernetes & Ceph-Rook: Basics

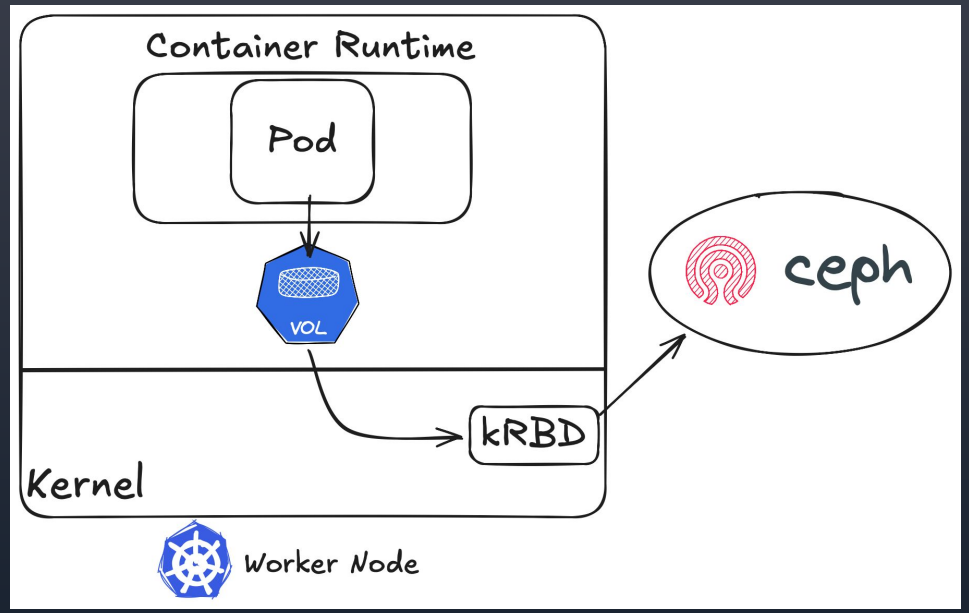
- Kubernetes
  - Deployment, scaling, and management of containerized applications
- Ceph-Rook
  - Deploys and manages Ceph inside a Kubernetes Cluster
- Ceph-Container Storage Interface (CSI)
  - Makes Ceph storage “usable” for Kubernetes resources

- CSI is about volumes
  - “Consumption of both block and mountable volumes.”

Ceph-CSI Basics

- Pod performs IO to volume
- Volume is a kernel rbd mount
- Krbd sents IO to Ceph

- Mounts/Demounts Volumes

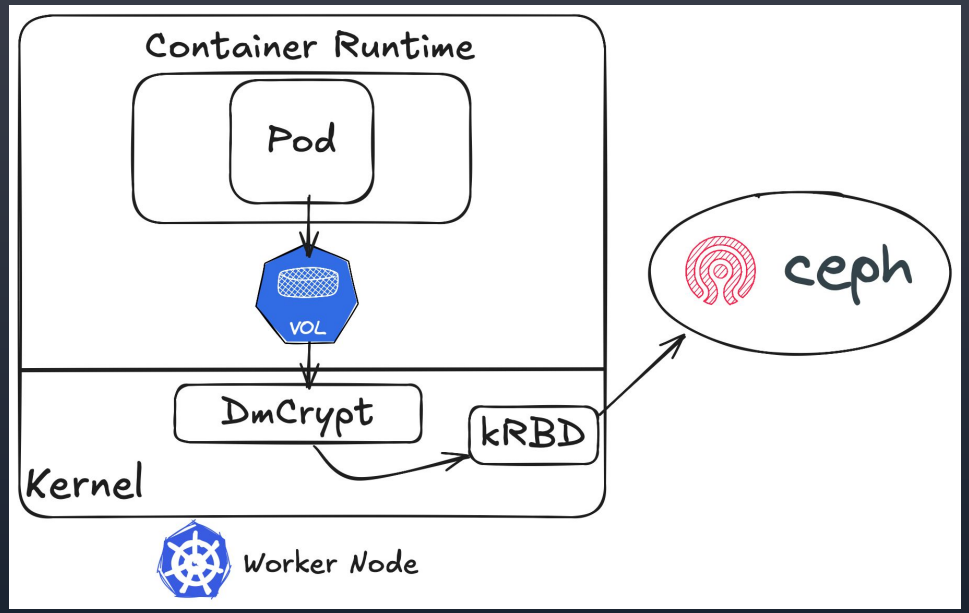


Example RBD Kernel Mount IO Path without Encryption

Encryption in Ceph-CSI

- Filesystem Volume Encryption
  - With fscrypt
- Block Volume Encryption
  - With dmcrypt or fscrypt

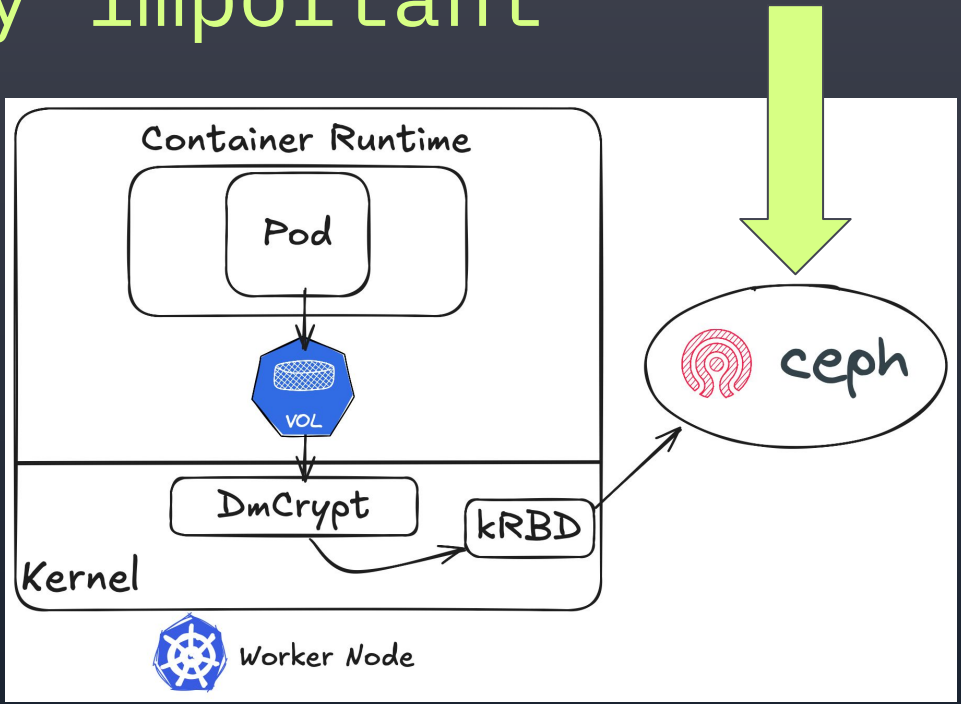
- Idea leverage linux kernel encryption capabilities
  - No user-space encryption



Example RBD Kernel Mount IO Path with Encryption

Why is Integrity important

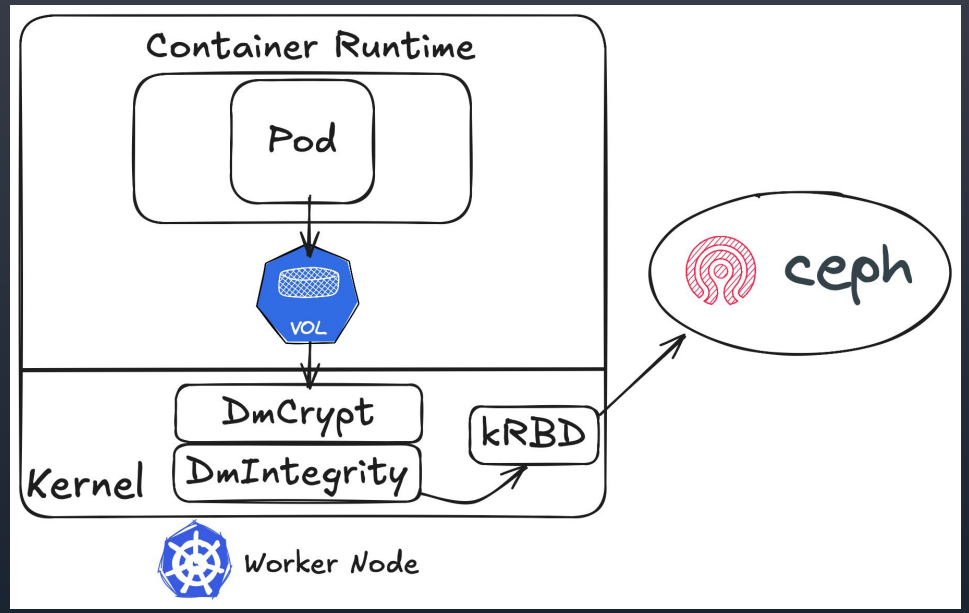
- What happens when data gets manipulated in Ceph?
- How can maintainers notice manipulation?
- Why is dmcrypt not solving this?



Example RBD Kernel Mount IO Path with Encryption

Ceph-CSI: Adding Integrity

- Usage of kernel module dmIntegrity
- Dm-crypt encrypt/decrypts data
  - AEAD ciphers induce a ciphertext expansion
- Dm-Integrity accommodates ciphertext expansion on storage medium

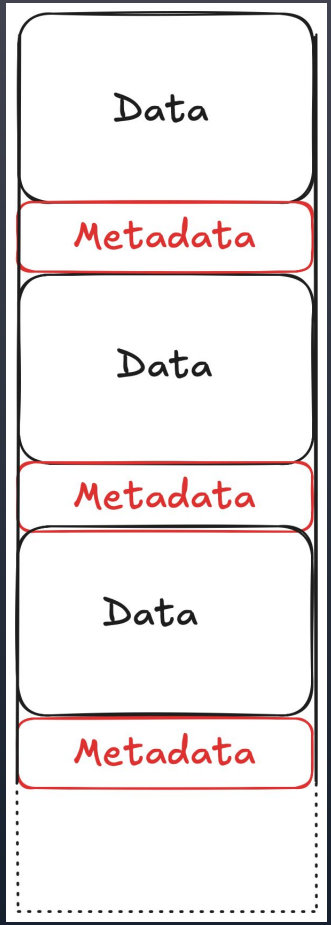


Example RBD Kernel Mount IO Path with Encryption + Integrity Protection

DmIntegrity Limits…

- Whole volume has to be formatted
  - No thin provisioning of RBD images
- Implements a Journaling
  - Write of data and authentication tags must be atomic
- AEAD support Experimental

- Alternatives to using Dmintegrity is to re-implement it in user-space



Dm-Integrity Disk Data Layout

Recommended Configuration

- Use Compound Configuration
  - Like an AES-XTS with HMAC
  - Recovery by ignoring integrity checks in case of failure
  - AEAD support is experimental

How can what you learned by applied throughout Ceph?

Data Security is Evolving

- Stakes are get higher
  - Larger amounts of data get stored
  - More sensitive data gets stored

- More stringent compliance requirements
  - DORA
  - FIPS compliance
  - More to come…

Integrity Protection in Storage

- Any other Ceph client does not implement any means to establish integrity
  - Except RGW client

- Object Storage usage of AEAD ciphers
  - Azure, AWS, Google Cloud

CL'SO

Powered by ceph

Thank you!

David Mohren

Motivation: Useful for Ceph?

- AWS, Azure, use AES-GCM already for their object stores