OpenZFS

# Securing the Cloud w/ ZFS Encryption

•••

# Background

OpenZFS

Triton - Cloud Orchestration

Manta - Storage

- Both built on SmartOS
- Both heavily rely on ZFS
- Want to provide ability to protect data at rest

# ZFS Encryption

OpenZFS

- Use ZFS Encryption!

- How to manage keys?

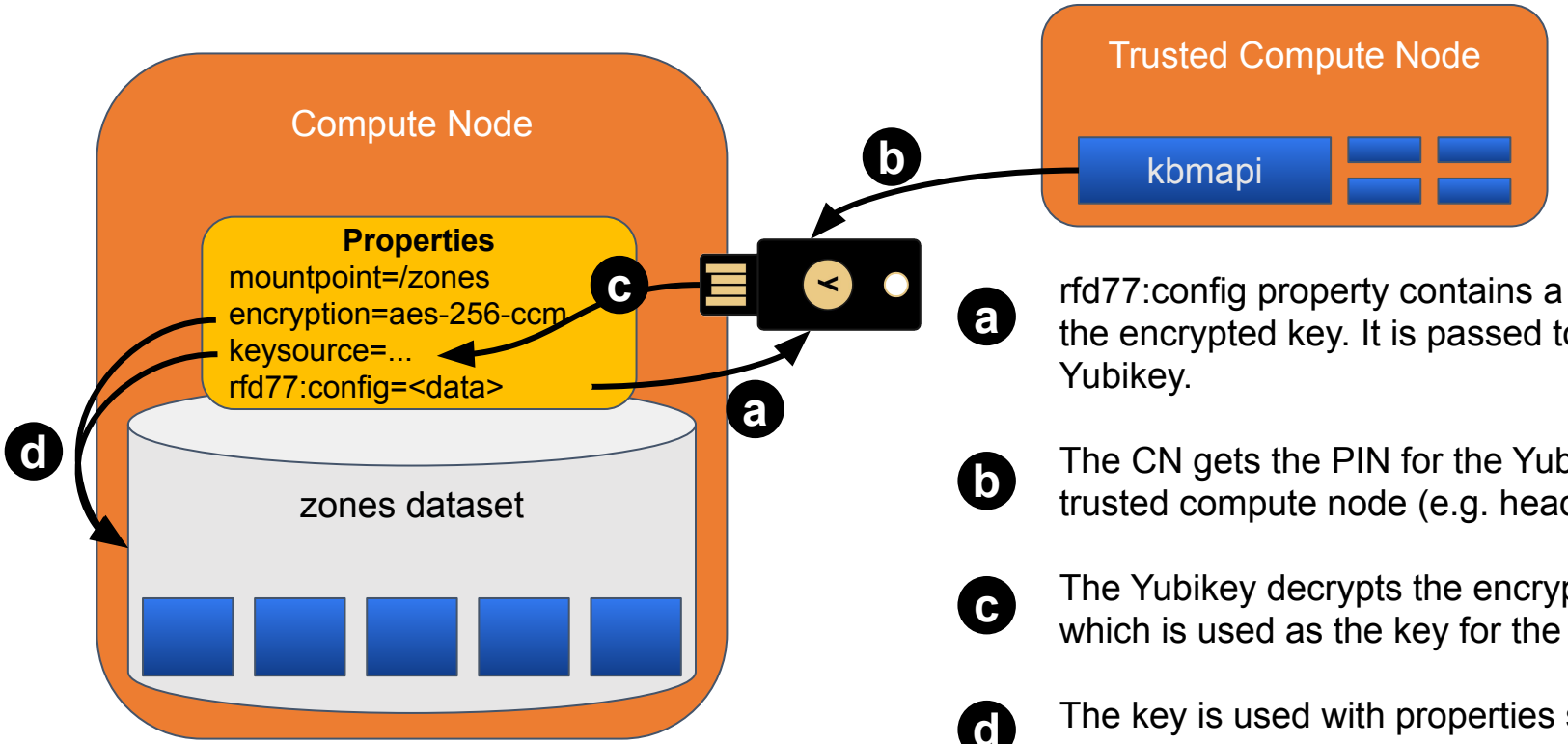
# KBM

OpenZFS

- Key backup and management
- Two main components:
  - KBMAPI - Head node service
  - kbmd - Daemon running on compute notes
- Encrypt entire zpool
  - Heavy use of snapshot and cloning in Triton makes finer grained keying less useful
- Use PIV tokens (e.g. Yubikeys) to protect zpool key
  - Analogous to two factor authentication
  - PIV tokens store public/private key pairs
  - Use public key to protect zpool key
  - Save result in ‘ebox’ -- encrypted zpool key plus metadata, stored as dataset property
  - Only PIV token can decrypt contents of ebox (requires PIN)

# Unlocking a dataset

OpenZFS




**a** rfd77:config property contains a ebox with the encrypted key. It is passed to the Yubikey.

**b** The CN gets the PIN for the Yubikey from a trusted compute node (e.g. headnode).

**c** The Yubikey decrypts the encrypted key, which is used as the key for the dataset.

**d** The key is used with properties stored on the dataset to allow access to encrypted data stored in the dataset.

# Initial Compute Node Setup

OpenZFS

- Initialize PIV token
  - PIV generates public/private key pairs -- private key never leaves token
  - Generate random PIN
  - Register PIV token w/ KBMAPI service
- Generate random zpool key
- Create ebox
- Create zpool w/ zpool key and ebox stored as root dataset property

# Recovery

OpenZFS

- What happens if PIV token is lost/damaged?
  - Keep an escrowed copy of zpool key in ebox
  - Split into M parts (decided by operator)
  - Set threshold value of N parts required to obtain key
  - Each part is encrypted by PIV token assigned to key employees
  - Info about M parts (PIV GUID, public key, etc) + threshold amount == Recovery Config
  - Perform challenge/response until N parts have been processed
  - Unlock pool, replace system PIV token
- Provide mechanism to push new recovery configs

# More Info

OpenZFS

- https://github.com/joyent/rfd/blob/master/rfd/0077/README.adoc
- https://github.com/joyent/rfd/blob/master/rfd/0173/README.adoc