ORACLE

Cloud Infrastructure

Key Management

Level 100

Rohit Rahi

November 2018

ORACLE

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Objectives

After completing this lesson, you should be able to:

- Explain how Oracle Cloud Infrastructure Key Management enables customers to encrypt their data using keys that they control

Key Management

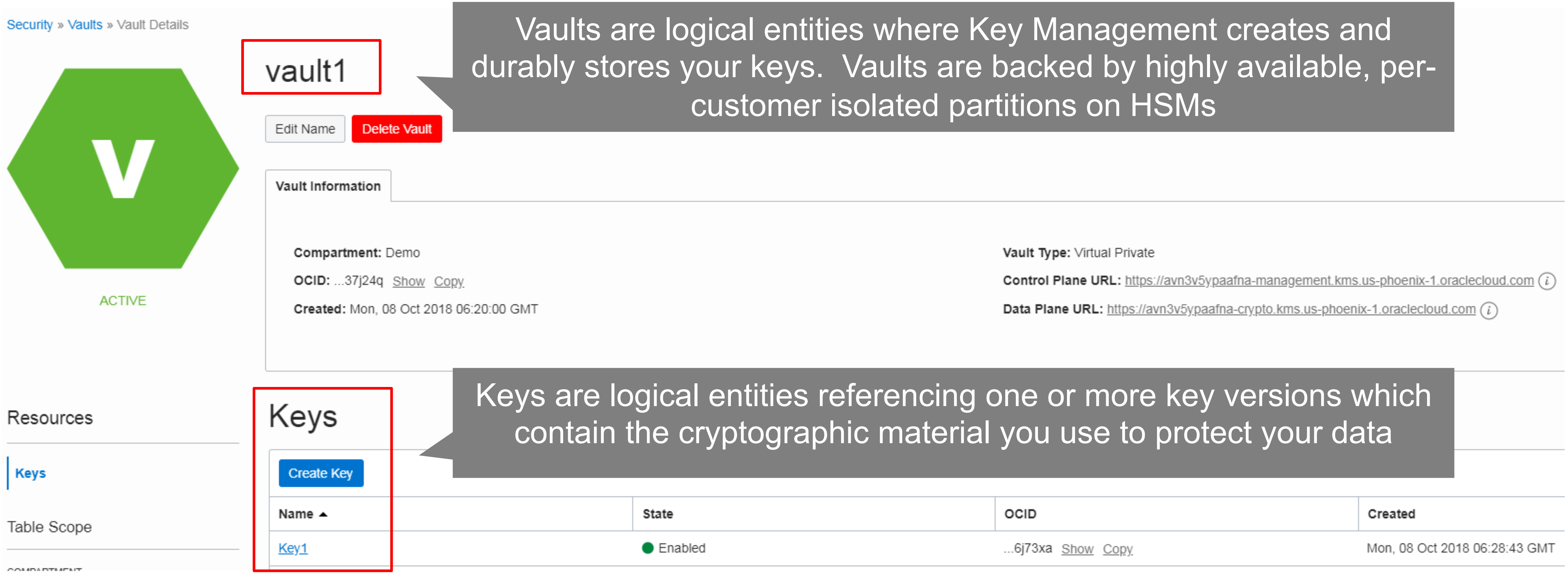
- Oracle Cloud Infrastructure Key Management is a managed service that enables you to encrypt your data using keys that you control
- Oracle Key Management provides you with
  - Centralized key management capabilities
  - Highly available, durable, and secure key storage using per-customer isolated partitions in hardware security modules (HSMs)*
  - Integration with select Oracle Cloud Infrastructure services
- Oracle Key Management uses HSMs that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. This means that the HSM hardware is tamper-evident, has physical safeguards for tamper-resistance, requires identity-based authentication, and deletes keys from the device when it detects tampering.

* A HSM is a physical computing device that safeguards digital keys and provides crypto processing

Key Management capabilities

- Create highly available key vaults to durably store your encryption keys
- Create keys /quickly disable keys (so they can’t be used by anyone) /re-enable disabled keys
- Rotate your keys to meet your security governance and regulatory compliance needs
- Define which Oracle Identity and Access Management (IAM) users or groups can manage keys and key vaults
- Define which IAM users, groups or service can use keys to encrypt and decrypt your data
- Define which IAM users or groups can associate keys with other OCI resources (e.g. block volumes, object storage bucket)
- Monitor the lifecycle of your keys and key vaults using Oracle Audit
- Delete key vaults that you no longer use

Centralized Key Management



vault1

Vaults are logical entities where Key Management creates and durably stores your keys. Vaults are backed by highly available, per-customer isolated partitions on HSMs

Compartment: Demo

OCID: ...37j24q Show Copy

Created: Mon, 08 Oct 2018 06:20:00 GMT

Vault Type: Virtual Private

Control Plane URL: https://avn3v5ypaafna-management.kms.us-phoenix-1.oraclecloud.com

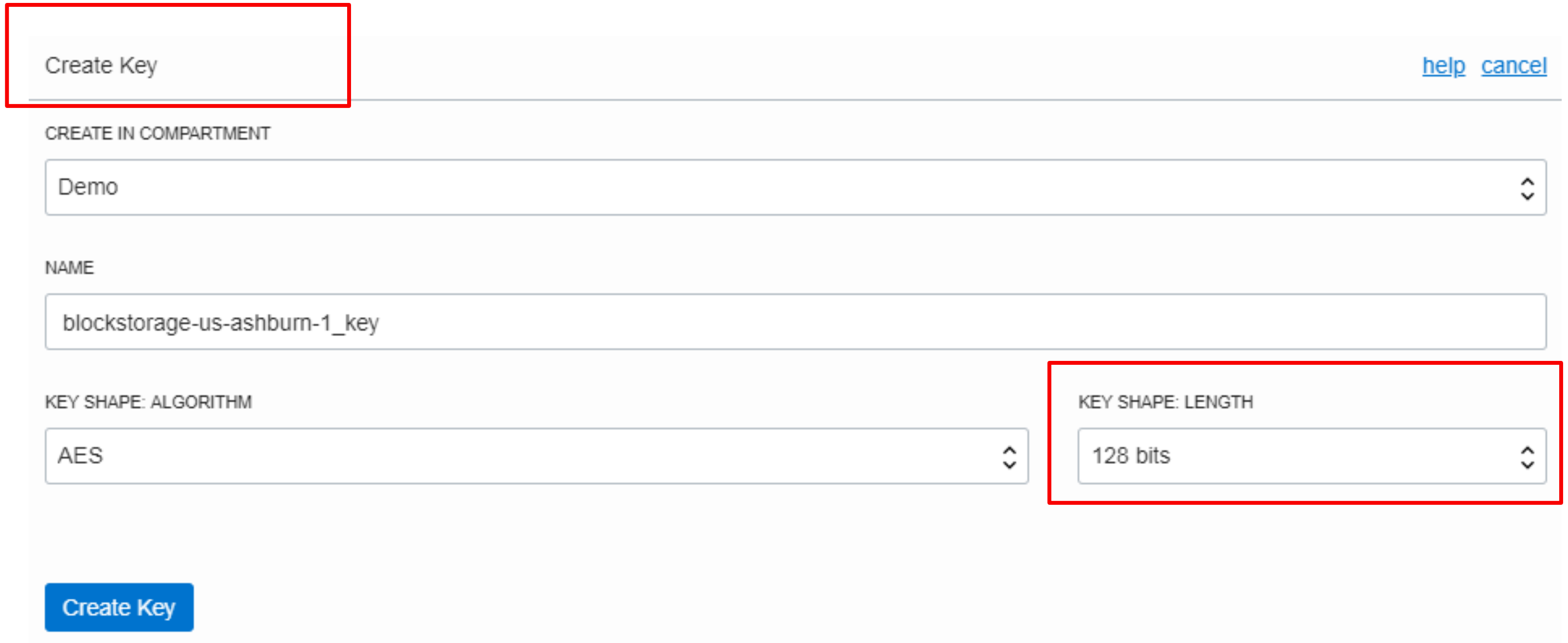
Data Plane URL: https://avn3v5ypaafna-crypto.kms.us-phoenix-1.oraclecloud.com

Keys

Keys are logical entities referencing one or more key versions which contain the cryptographic material you use to protect your data

Name ▲	State	OCID	Created
Key1	● Enabled	...6j73xa Show Copy	Mon, 08 Oct 2018 06:28:43 GMT

Create a Key



Create Key

CREATE IN COMPARTMENT

Demo

NAME

blockstorage-us-ashburn-1_key

KEY SHAPE: ALGORITHM

AES

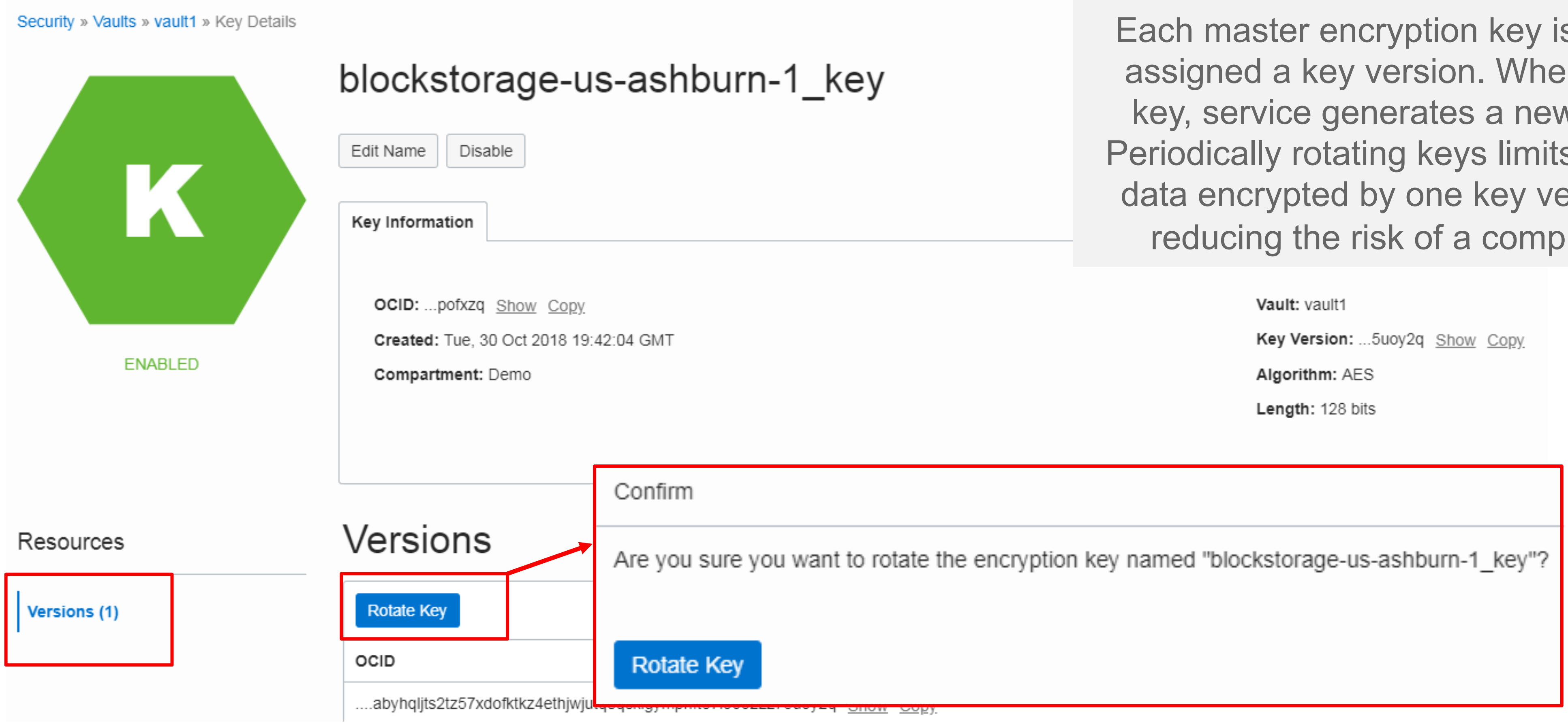
KEY SHAPE: LENGTH

128 bits

Key Management supports Advanced Encryption Standard (AES) *Key Shape Algorithm* with key sizes of 128, 196, and 256 bits

Rotate a Key

Each master encryption key is automatically assigned a key version. When you rotate a key, service generates a new key version. Periodically rotating keys limits the amount of data encrypted by one key version, thereby reducing the risk of a compromised key



Security » Vaults » vault1 » Key Details

blockstorage-us-ashburn-1_key

OCID: ...pofxzq Show Copy

Created: Tue, 30 Oct 2018 19:42:04 GMT

Compartment: Demo

Vault: vault1

Key Version: ...5uoy2q Show Copy

Algorithm: AES

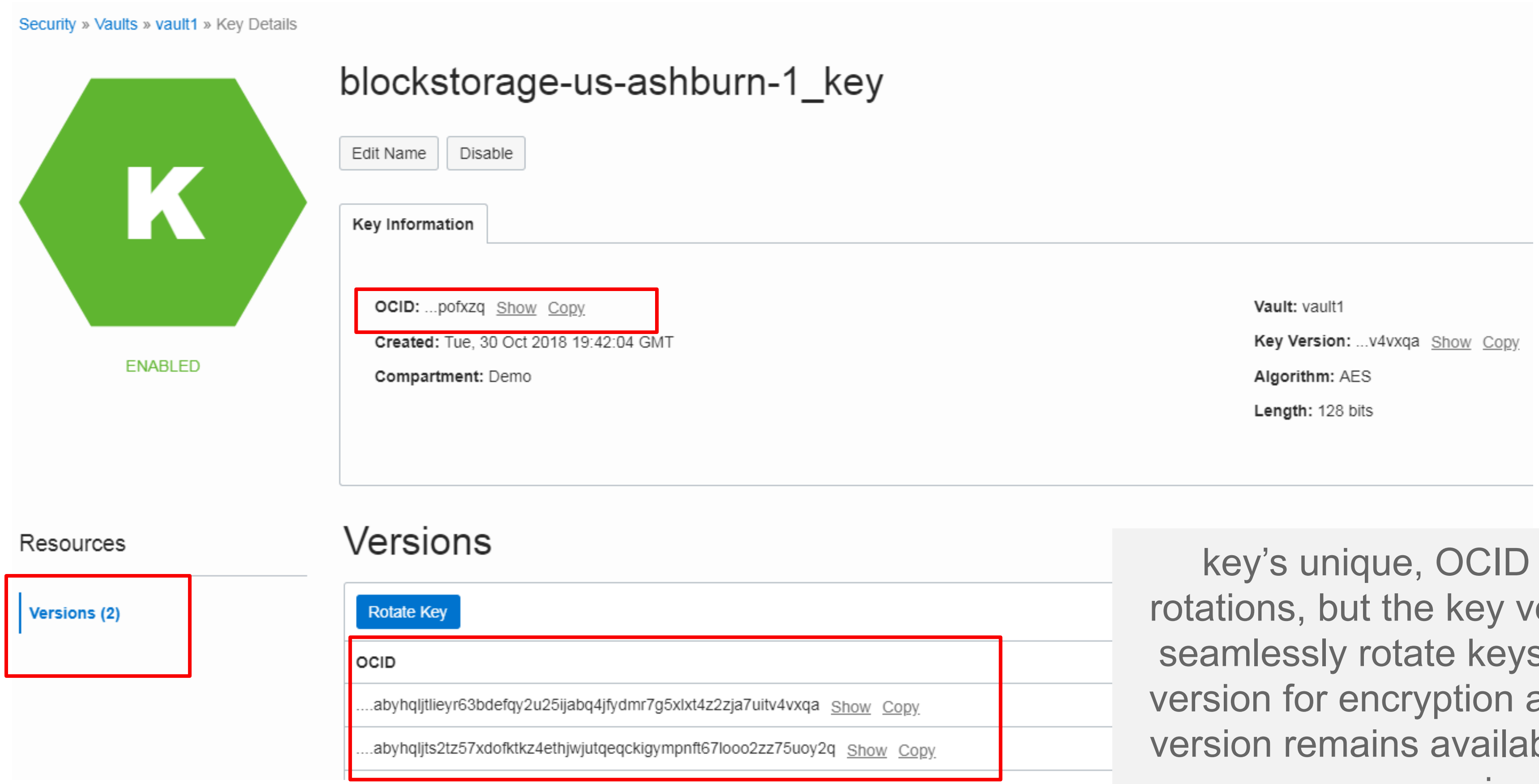
Length: 128 bits

....abyhqljts2tz57xdofktkz4ethjwju

Confirm

Are you sure you want to rotate the encryption key named "blockstorage-us-ashburn-1_key"?

Rotate a Key



Security » Vaults » vault1 » Key Details

blockstorage-us-ashburn-1_key

OCID: ...pofxzq Show Copy

Created: Tue, 30 Oct 2018 19:42:04 GMT

Compartment: Demo

Vault: vault1

Key Version: ...v4vxqa Show Copy

Algorithm: AES

Length: 128 bits

Resources

Versions (2)

Versions

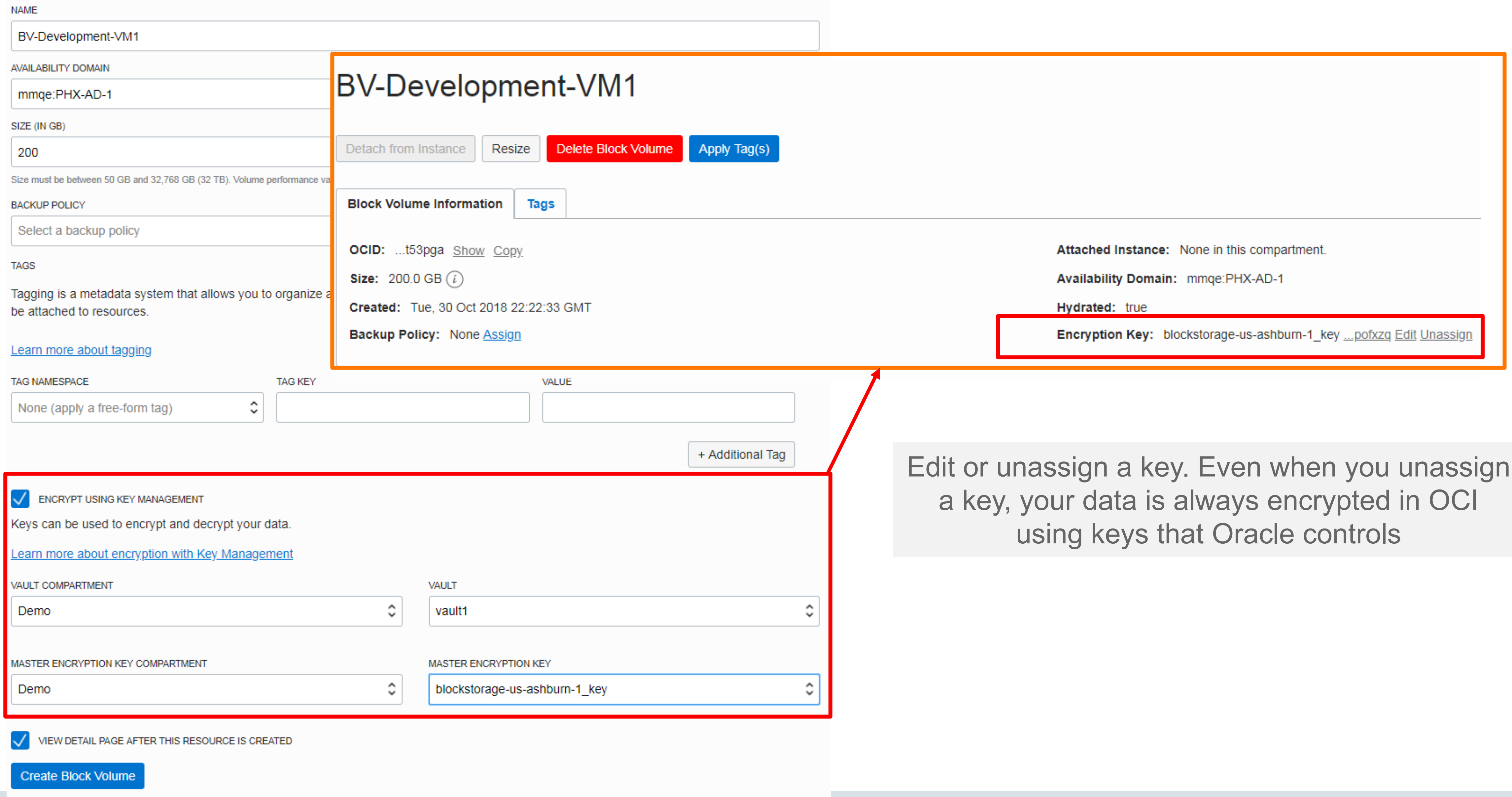
OCID
....abyhqljtlieyr63bdefqy2u25ijabq4jfydmr7g5xlxt4z2zja7uitv4vxqa Show Copy
....abyhqljts2tz57xdofktkz4ethjwjutqeqckigympnft67looo2zz75uoy2q Show Copy

key's unique, OCID remains the same across rotations, but the key version enables the service to seamlessly rotate keys. You can't use an older key version for encryption after you rotate it, but the key version remains available to decrypt any data that it previously encrypted

IAM Integration with Key Management

- Only users, groups, or services that you authorize via an IAM policy can use the keys by invoking Key Management to encrypt or decrypt data. Example policies
- Compartments for keys management should be separated
- Policies
  - This policy allows the group VaultAdministrators to perform all management actions in the VaultCompartment
    - Allow group VaultAdministrators to manage vaults in compartment VaultCompartment
  - This policy allows the group KeyAdministrators to manage keys and use the vaults in the VaultCompartment
    - Allow group KeyAdministrators to manage keys in compartment VaultCompartment
    - Allow group KeyAdministrators to use vaults in compartment VaultCompartment
  - These policies allow Object and Block storage to use keys
    - allow service objectstorage-us-phoenix-1 to manage keys in compartment VaultCompartment
    - allow service blockstorage to manage keys in compartment VaultCompartment

Block Volume Encryption



NAME

BV-Development-VM1

AVAILABILITY DOMAIN

mmqe:PHX-AD-1

SIZE (IN GB)

200

Size must be between 50 GB and 32,768 GB (32 TB). Volume performance va

BACKUP POLICY

Select a backup policy

TAGS

Tagging is a metadata system that allows you to organize a
be attached to resources.

Learn more about tagging

TAG NAMESPACE	TAG KEY	VALUE
None (apply a free-form tag)		

+ Additional Tag

☑ ENCRYPT USING KEY MANAGEMENT

Keys can be used to encrypt and decrypt your data.

Learn more about encryption with Key Management

VAULT COMPARTMENT	VAULT
Demo	vault1

MASTER ENCRYPTION KEY COMPARTMENT	MASTER ENCRYPTION KEY
Demo	blockstorage-us-ashburn-1_key

☑ VIEW DETAIL PAGE AFTER THIS RESOURCE IS CREATED

Create Block Volume

BV-Development-VM1

OCID: ...t53pga Show Copy

Size: 200.0 GB

Created: Tue, 30 Oct 2018 22:22:33 GMT

Backup Policy: None Assign

Attached Instance: None in this compartment.

Availability Domain: mmqe:PHX-AD-1

Hydrated: true

Encryption Key: blockstorage-us-ashburn-1_key ...pofxzq Edit Unassign

Edit or unassign a key. Even when you unassign a key, your data is always encrypted in OCI using keys that Oracle controls

Key Management – Design Considerations

- Regional service, replicates encryption keys across 3 ADs in a region
- Block Volumes and Object Storage are integrated with Key Management
- Rotating a key does not automatically re-encrypt data that was previously encrypted with the old key version; this data is re-encrypted the next time it’s modified by the customer
- If you suspect that a key has been compromised, you should re-encrypt all data protected by that key and disable the prior key version
- You cannot import a key from your existing key management solution to Oracle Key Management. You cannot export encryption keys from the Oracle Key Management key vaults
- You cannot delete keys, but can disable them. You can delete key vaults
- You can schedule the deletion of a key vault by configuring a waiting period for deletion from 7 - 30 days
  - The key vault and all the keys created inside the key vault are deleted at the end of the waiting period, and all the data that was protected by those keys is no longer accessible.
  - After a key vault is deleted, it can’t be recovered

https://cloud.oracle.com/cloud-security/kms/faq

Key Management Pricing

- When using Key Management, you pay an hourly fee for each key vault that you create, and you are charged at the end of the month for that month's usage.
- You are not charged for the keys that you create inside your key vaults and use with supported Oracle Cloud Infrastructure services
- You aren't billed for the use of a key vault that is scheduled for deletion. If you cancel the deletion of your key vault during the waiting period, billing continues

	PAYG	Monthly Flex	Metric
Oracle Key Management	$6.983	$4.655	Virtual Private Vault Per Hour

https://cloud.oracle.com/en_US/cloud-security/pricing

ORACLE

Summary

- Key Management is a managed service that enables you to encrypt your data using keys that you control
- Provides centralized key management capabilities leveraging FIPS 140-2 Security Level 3 Hardware Security Modules
- Currently, integrated with OCI Block Volume and Object Storage services
- IAM integration defines which IAM users, groups or service can use keys to encrypt and decrypt your data

ORACLE®
Cloud Infrastructure

cloud.oracle.com/iaas

cloud.oracle.com/tryit