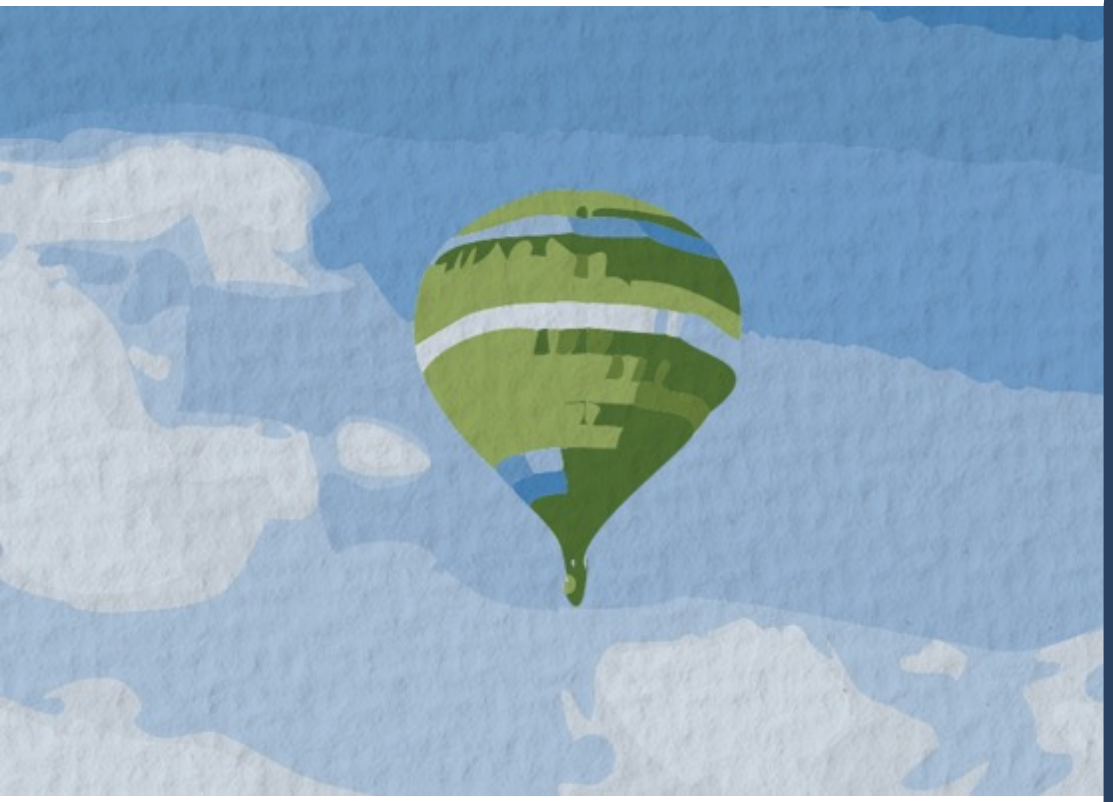


Immutable Backups And Ransomware Protection

New Options at OCI

Mike Miller
Syntax
Michael.Miller@syntax.com

June 17 – 20, 2024 • Caesars Palace • Las Vegas, NV

ASCEND 2024

Agenda

- Introductions
- Ransomware
- OCI backup offerings
  - Block
  - File
  - Object storage

Mike Miller

Senior Solution Architect, Syntax

- Over 25 years of working with enterprise software and information security technologies
- Experience with enterprise software implementation and support, cloud operations, and executing compliance and risk management programs.
- A CISSP, Certified Information Systems Security Professional
- Oracle ACE Associate

Syntax

- Syntax was founded in 1972 in Montreal, Canada with 3,400 employees in 26 countries
- Syntax provides full-stack, full-lifecycle Cloud Managed Services and Application Managed Services focused on leading ERP solutions such as JD Edwards, Oracle E-Business Suite, and SAP
- Syntax is a multicloud partner and supports OCI, AWS, Azure, GCP, and Syntax Enterprise Cloud®
- Our ERP solutions include an array of value-add services, including our AI-driven monitoring and automation platform, CxHub customer experience portal, security management, and FinOps
- Syntax is a global company with 3,400 employees in 26 countries

ORACLE | Service Partner

Expertise in
Cloud Service Solution
OCI Migration
in NAMER–North America

ORACLE | Service Partner

Expertise in
Oracle E-Business Suite
Applications to Oracle Cloud
in North America

ORACLE | Service Partner

Expertise in
JD Edwards Applications
to Oracle Cloud
in North America

ORACLE | Service Partner

Expertise in
Oracle Cloud Platform -
Oracle Cloud Platform Integration
in North America

ORACLE | Service Partner

Expertise in
CSPE: Oracle Cloud Platform -
Oracle Cloud Platform
Data Management
in North America

ORACLE | Service Partner

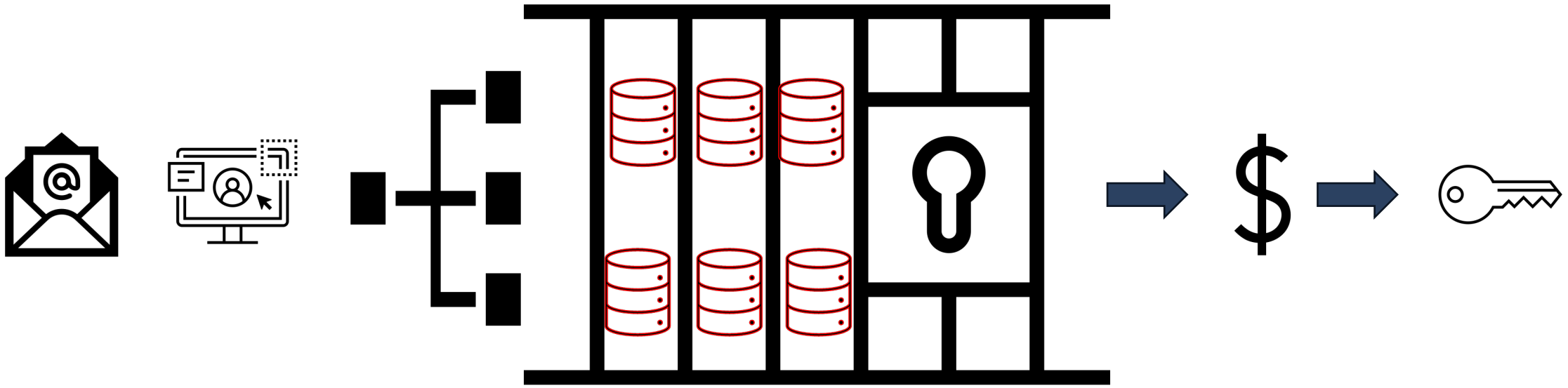
Expertise in
CSPE: Oracle Cloud Platform -
Oracle Database to Oracle Cloud
in North America

Let’s Talk About De-risking Backups

- Always remember to follow the 3-2-1 rule for backups:
  - At all times try to have at least three copies of your backups
  - Store the copies on two different media
  - Keep one backup offsite
- Probability of your OCI tenancy being ransomwared?
  - Non-zero probability
  - Ransomware is just one of many threat vectors
- Really talking about planning ahead
  - Remove Fear and Uncertainty, and Doubt (FUD) about the availability of backups
  - Ransomware is but one threat vector for disaster recovery

Ransomware Kill Chain

Show of hands, how many people keep backups for more than 2 weeks?



A user opens an email containing malware. Once in, the threat actors will most likely conduct resonance and release malware that crawls the network, encrypting anything it can. Hopefully, the initial user is not an admin/power user with elevated privileges…

A demand for money is made to obtain the decryption key

OCI Options and Solutions

Backups and Disaster Recovery

ASCEND 2024

Immutable

immutable adjective

im·mu·ta·ble (ˌ)i(m)-ˈmyü-tə-bəl

Synonyms of *immutable* ›

: not capable of or susceptible to change

immutability (ˌ)i(m)-ˌmyü-tə-ˈbi-lə-tē noun
immutableness (ˌ)i(m)-ˈmyü-tə-bəl-nəs noun
immutably (ˌ)i(m)-ˈmyü-tə-blē adverb

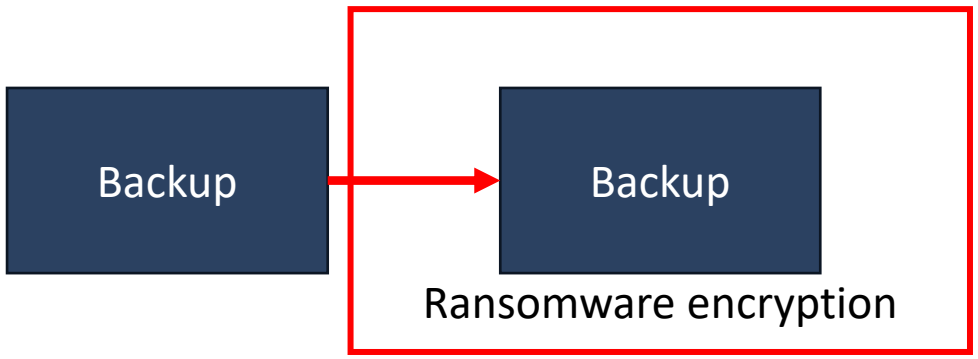
Did you know?

Immutable may describe something that is incapable of change, but the word itself —like all words—is mutable, both capable of and prone to alteration. To put a finer point on it, if language were fixed, we wouldn't have *immutable* itself, which required a variety of mutations of the Latin verb *mutare* ("to change") to reach our tongues (or pens, keyboards, or touchscreens—oh the many permutations of communication!). Other English words that can be traced back to *mutare* include *mutate*, *transmute*, and *commute*. Which reminds us—the mutability of language makes great food for thought during one's commute.

https://www.merriam-webster.com/dictionary/immutable#:~:text=%3A%20not%20capable%20of%20or%20susceptible%20to%20change

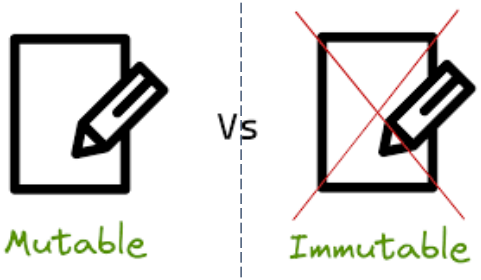
Break The Ransomware Kill Chain With Immutable Backups

Problem

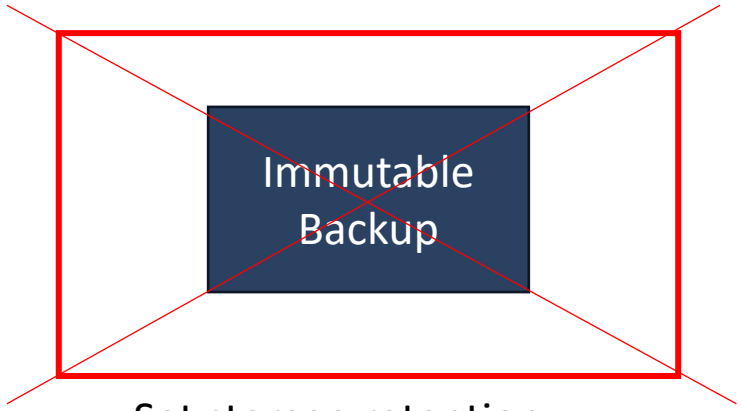


Backup is *re-encrypted* by the ransomware threat actor.

Backup cannot be used until ransomware encryption is removed.



Solution



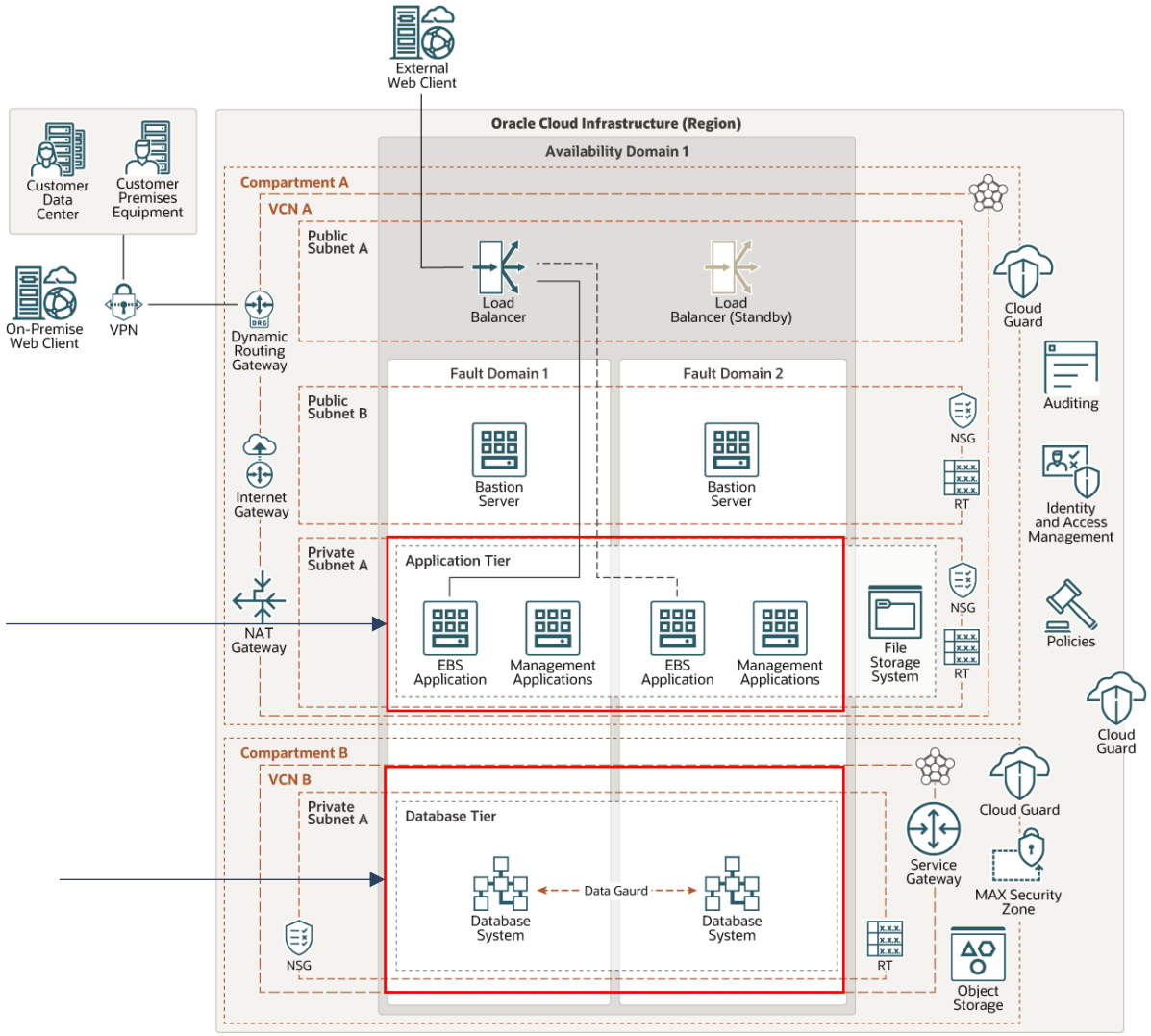
Set storage retention policy rules so that files cannot be altered or deleted until x days from the last modified.

Use Case of Oracle E-Business Suite

Need full tech stack coverage

Middle Tier
Block storage
File Storage

Database Tier
DB as Service

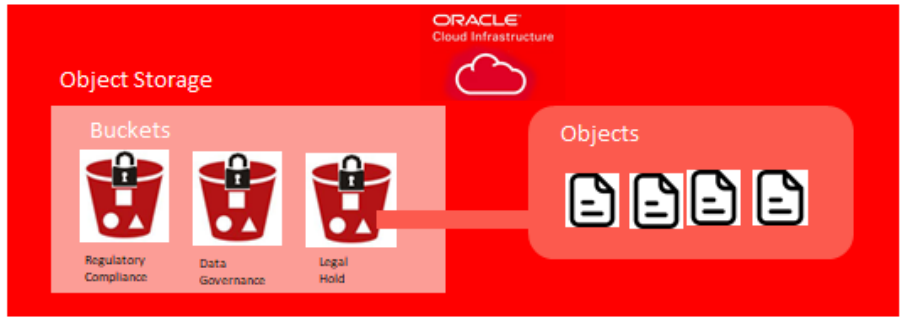


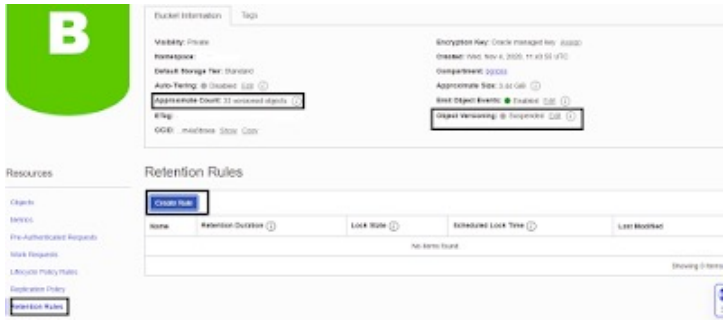
OCI Options and Recommendations

EBS Example	OCI Storage	Recommendation
Middle Tier	Block	Deploy 3rd party CommVault agents, write backups to OCI immutable object storage and replicate to remote OCI region, with min. 14 day rolling policy
$APPL_TOP	File	Backup to OCI immutable object storage and replicate to remote OCI region, with min. 14 day rolling policy
Database	Object	Backup to OCI immutable object storage and replicate to remote OCI region, with min. 14 day rolling policy

ASCEND 2024

OCI Object Storage Retention Rules





Oracle Cloud Infrastructure Documentation

- Data Retention Rules
  - Creating an Object Storage Retention Rule
  - Listing Object Storage Retention Rules
  - Getting an Object Storage Retention Rule's Details
  - Editing an Object Storage Retention Rule
  - Deleting an Object Storage Retention Rule
- Object Lifecycle Management
- Multipart Uploads
- Pre-Authenticated Requests
- Work Requests
- Data Encryption
- Amazon S3 Compatibility API

Object Storage Data Retention Rules

Learn how to use retention rules to preserve Object Storage data.

Retention rules are configured at the bucket level and are applied to all individual objects in the bucket.

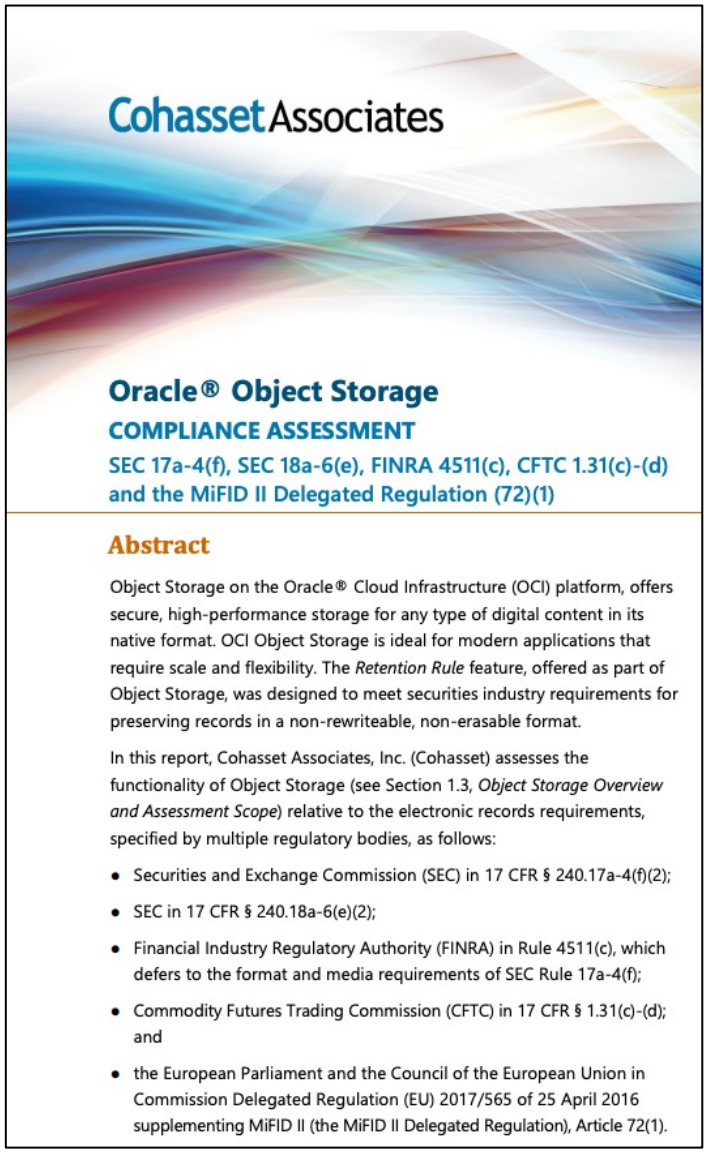
It's important to understand retention duration for time-bound rules. Even though you are creating retention rules for a bucket, the duration of a rule is applied to each object in the bucket individually, and is based on the object's **Last Modified** timestamp. Let's say you have two objects in the bucket, ObjectX and ObjectY. ObjectX was last modified 14 months ago and ObjectY was last modified 3 months ago. You create a retention rule with a duration of 1 year. This rule prevents the modification or deletion of ObjectY for the next 9 months. The rule allows the modification or deletion of ObjectX because the retention rule duration (1 year) is less that the object's **Last Modified** timestamp (14 months). If ObjectX is overwritten some time in the coming year, modification and deletion would be prevented for the rule duration time remaining.

Locking a retention rule is an irreversible operation. Not even a tenancy administrator can delete a locked rule. There is a mandatory 14-day delay before a rule is locked. This delay lets you thoroughly test, modify, or delete the rule or the rule lock before the rule is permanently locked. A rule is active at the time of creation. The lock only controls whether the rule itself can be modified. After a rule is locked, only increases in the duration are allowed. Object modification is prevented and the rule can only be deleted by deleting the bucket. A bucket must be empty before it can be deleted.

For an independent assessment of the Object Storage retention rules feature's ability to meet regulatory requirements for record management and retention, see Cohasset Associate's SEC 17a-4(f), FINRA 4511(c), CFTC 1.31(c)-(d) and MiFID II Compliance Assessment.

https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/usingretentionrules.htm

Meets Requirements for SEC 17a-4(f)



Cohasset Associates

Oracle® Object Storage

COMPLIANCE ASSESSMENT

SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation (72)(1)

Abstract

Object Storage on the Oracle® Cloud Infrastructure (OCI) platform, offers secure, high-performance storage for any type of digital content in its native format. OCI Object Storage is ideal for modern applications that require scale and flexibility. The *Retention Rule* feature, offered as part of Object Storage, was designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Object Storage (see Section 1.3, *Object Storage Overview and Assessment Scope*) relative to the electronic records requirements, specified by multiple regulatory bodies, as follows:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)(2);
- SEC in 17 CFR § 240.18a-6(e)(2);
- Financial Industry Regulatory Authority (FINRA) in Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f);
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d); and
- the European Parliament and the Council of the European Union in Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation), Article 72(1).

OCI Object Storage retention controls were also assessed to meet SEC 17a-4(f), a key regulation for financial services customers

For more information, see the product assessment report https://www.oracle.com/a/ocom/docs/oracle-object-storage-compliance-assessment-report.pdf

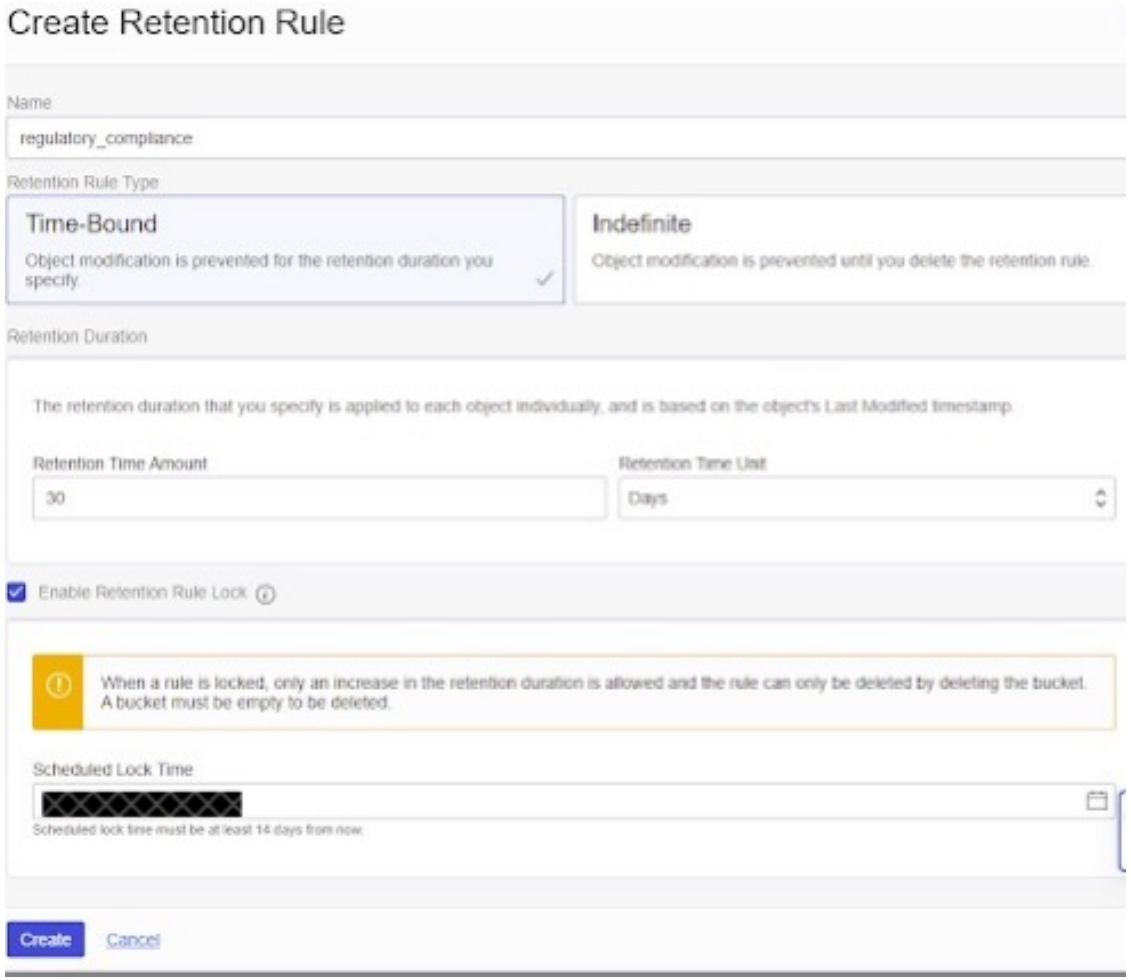
Object Storage Retention Rules

Creating an Object Storage Retention Rule

Create a retention rule for an Object Storage bucket.

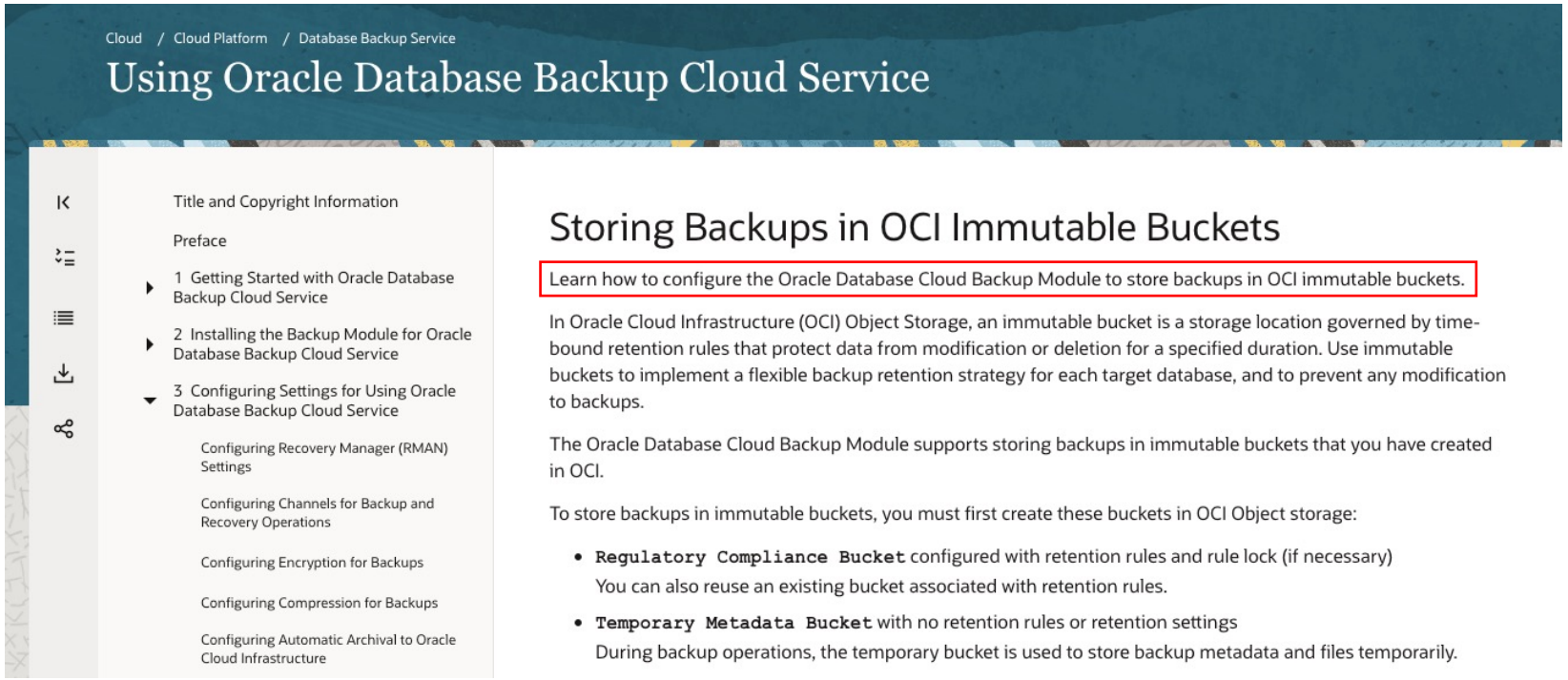
Console | CLI | API

1. Open the navigation menu and click **Storage**. Under **Object Storage & Archive Storage**, click **Buckets**.
2. Select the compartment from the list under **List Scope**. All buckets in that compartment are listed in tabular form. This is the compartment where the bucket you create is located.
3. Click the bucket for which you're creating a retention rule. The bucket's **Details** page appears.
4. Click **Retention Rules** under **Resources**. The **Retention Rules** list appears. All retention rules are listed in tabular form.
5. Click **Create Rule**. The **Create Retention Rule** dialog box appears.
6. Complete the following:
   - **Name**: Enter a name for the rule. The system generates a rule name that reflects the current year, month, day, and time, for example, **retention-rule-20200229-1002**. If you change this name, use letters, numbers, dashes, underscores, and periods.
   - **Retention Type**: Choose the retention rule type that you want to create:
     - **Time-Bound** rules have a user-defined duration. Object modification is prevented for the duration specified. Duration is applied to each object individually, and is based on the object's **Last Modified** timestamp. Enter values for the **Retention Duration** settings that appear.
     - **Indefinite** rules have no duration or expiration. Object modification is prevented until an indefinite rule is deleted.
   - **Retention Duration**: (Time-Bound type rules only) Enter values for the **Retention Time Amount** time amount and **Retention Time Unit** time unit in **Days** or **Years**.
   - **Enable Retention Rule Lock**: (optional) Select the check box to lock the rule. When a rule is locked, only an increase in the retention duration is allowed and the rule can only be deleted by deleting the bucket. A bucket must be empty to be deleted.
7. Click **Create**.



OCI Immutable Database Backups

Standard functionality now with OCI Database as a Service



https://docs.oracle.com/en/cloud/paas/db-backup-cloud/csdbb/storing-backups-oci-immutable-buckets.html
https://blogs.oracle.com/maa/post/oracle-br-year-in-review

The Database Backup Cloud Module now supports the use of OCI Object Storage Locked Retention Rules for compliance and ransomware protection. This Retention Rule prevents any deletion or modification of objects in a designated bucket for a pre-defined period of time.

OCI Immutable Database Backups

- If you have stored your database backups in an existing regular bucket, then you can configure the same bucket to store immutable backups. In this case, first specify the existing bucket and a temporary bucket and then apply retention rules to the bucket in OCI. This ensures that your existing backups are also protected for the duration defined in the retention rule.
- Your databases may have varied demands for backup retention. As a best practice, Oracle recommends that you maintain a separate immutable bucket and a corresponding unique temporary metadata bucket for each target database.

OCI Immutable File Storage Backups

Backing Up Snapshots to Object Storage Using rclone

You might want to back up your File Storage snapshots in another location, such as Object Storage.

You can follow this process to use the rclone utility to back up snapshots.

1. Install rclone using the instructions for your operating system at https://rclone.org/downloads/.
2. Create a `~/.rclone.conf` configuration file containing this information:

```
[myobjectstorage]
 type = s3
 provider = Other
 env_auth = false
access_key_id = <access_key_of_customer_secret_key>
secret_access_key = <key_generated_when_creating_the_customer_secret_key>
 endpoint = <object_namespace>.compat.objectstorage.<region>.oraclecloud.com
```

> **Note**
>
> Refer to Working with Customer Secret Keys for details on obtaining a Customer Secret key.

3. Verify that rclone can access Object Storage:

```
$rclone ls -vv myobjectstorage:/<some_existing_bucket>
```

4. Create a snapshot, if necessary:

```
$sudo mkdir <fss_mount_point>/.snapshot/<snapshot_name>
```

5. Use the `copy`, `copyto`, or `sync` option to copy the snapshot to Object Storage:

```
$rclone copy --progress --metadata --copy-links <fss_mount_point>/.snapshot/<snapshot
```

You can specify an existing object bucket with immutable retention rules

https://docs.oracle.com/en-us/iaas/Content/File/Tasks/backing-up-snapshots-to-object-storage.htm

OCI Block Storage – No Option for Immutable Backups

Differences Between Block Volume Backups and Clones

Consider the following criteria when you decide whether to create a backup or a clone of a volume.

	Volume Backup	Volume Clone
Description	Creates a point-in-time backup of data on a volume. You can restore multiple new volumes from the backup later in the future.	Creates a single point-in-time copy of a volume without having to go through the backup and restore process.
Use case	Retain a backup of the data in a volume, so that you can duplicate an environment later or preserve the data for future use. Meet compliance and regulatory requirements, because the data in a backup remains unchanged over time. Support business continuity requirements. Reduce the risk of outages or data mutation over time.	Rapidly duplicate an existing environment. For example, you can use a clone to test configuration changes without impacting your production environment.
Speed	Slower (minutes or hours)	Faster (seconds)
Cost	Lower cost	Higher cost
Storage location	Object Storage	Block Volume
Retention policy	Policy-based backups expire, manual backups do not expire	No expiration
Volume groups	Supported. You can back up a volume group.	Supported. You can clone a volume group.

https://docs.oracle.com/en-us/iaas/Content/Block/Concepts/blockvolumebackups.htm

OCI Block Storage - How to Move Block volume Backups to Object Storage Buckets (Doc ID 2922140.1)

In this Document

APPLIES TO:

Oracle Cloud Infrastructure Block Storage - Version N/A and later
Information in this document applies to any platform.

GOAL

How to move Block volume backups to Object storage buckets

SOLUTION

Block Storage backups are stored in Object Storage. But these buckets are stored in an isolated tenancy and no users are given access to these buckets.

You are not charged for these backups via ObjectStorage i.e. there is no double billing. You will see billing only from Block Storage Backups (and nothing else).

OCI does not support customers exporting these backup buckets into customers' own tenancy for them to manage.

Cannot specify which object bucket nor retention rules

Commvault

Block Storage Option

ASCEND 2024

What is CommVault?

ORACLE Products Industries Resources Customers Partners Developers Company View Accounts Contact Sales

Customer References >

Commvault offers innovative ransomware protection with OCI

The provider of next-generation data protection-as-a-service allows customers to secure and recover data on OCI at lower total cost of ownership.

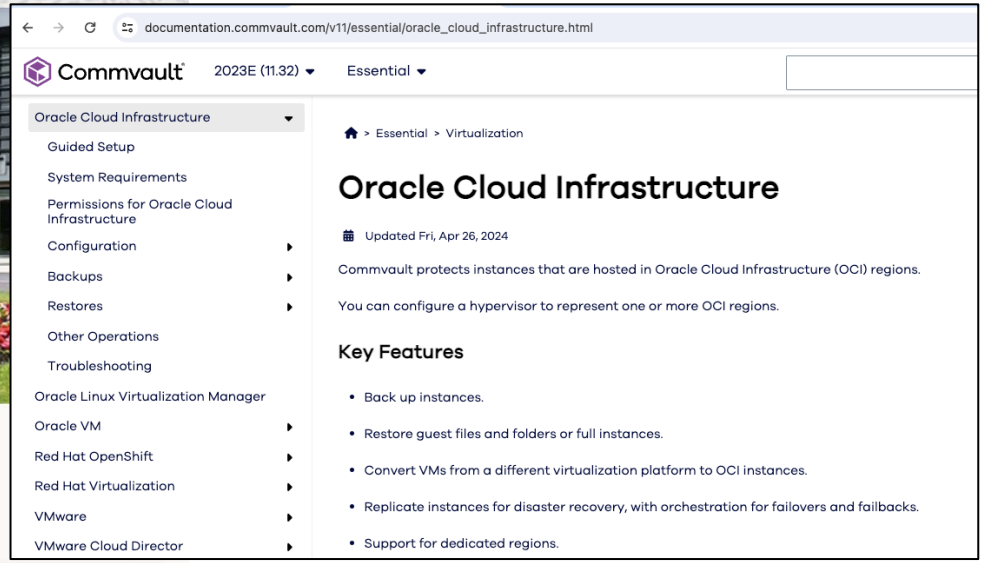
Share:

"OCI and Commvault offer unparalleled cloud services and data security for our customers in support of a broad spectrum of hybrid cloud and multicloud strategies. This partnership advances data protection capabilities from on premises to the cloud, including ransomware protection with air gap storage functionality to help secure, defend, and restore your data."

Alan Atkinson, Chief Partner Officer, Commvault

Products list

Oracle Cloud Infrastructure

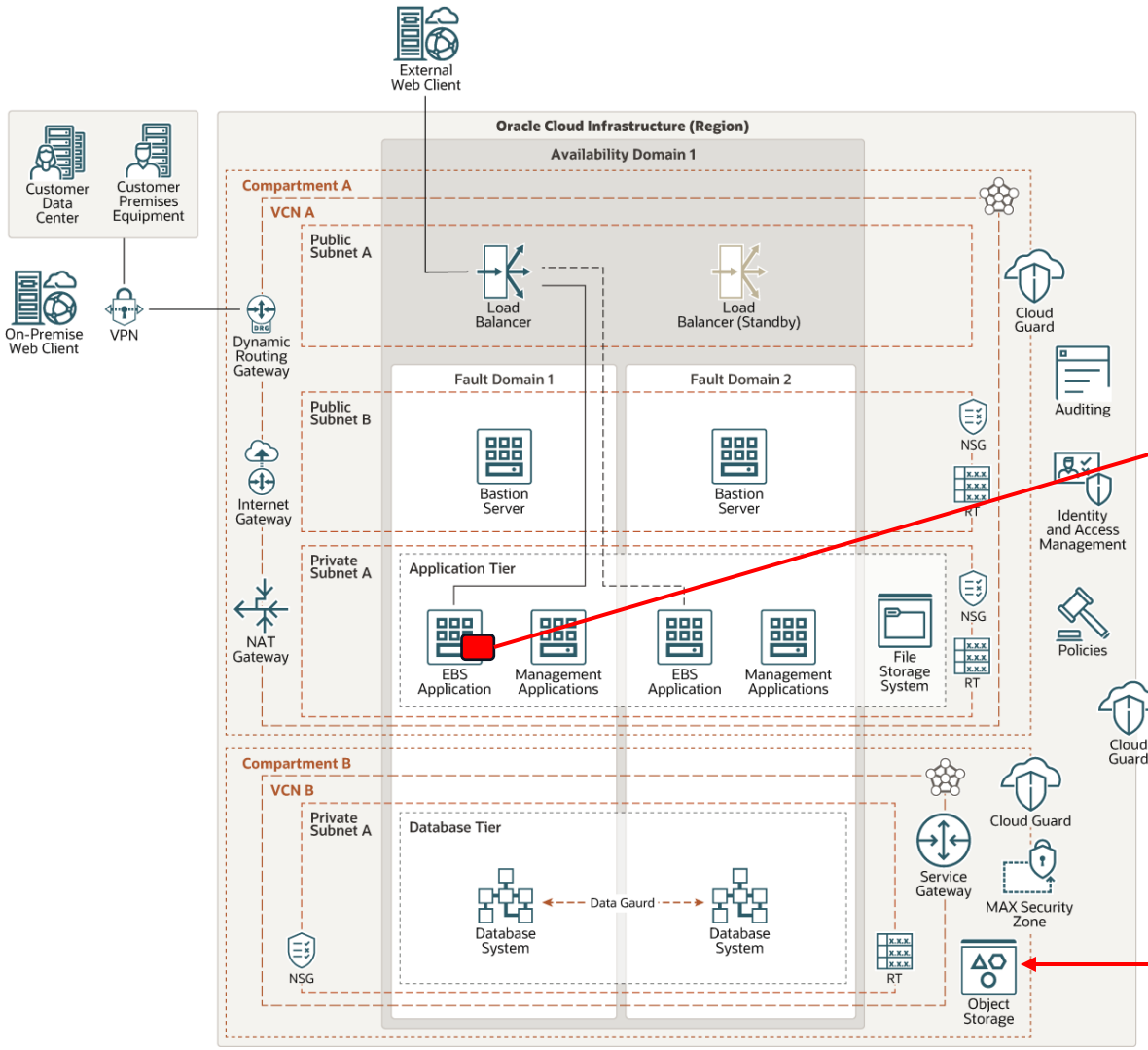


Note functionality to restore a single file(s)

https://www.oracle.com/customers/commvault/

https://www.commvault.com/

Use Case of Oracle E-Business Suite



The CommVault Console creates encrypted backups from its agent ands sends to OCI Object Storage – A specific bucket with immutable retention policies

https://www.commvault.com/supported-technologies/oracle
https://documentation.commvault.com/v11/essential/oracle_cloud_infrastructure.html

Summary

OCI Storage	Recommendation
Block	Deploy 3rd party CommVault agents, write backups to OCI immutable object storage and replicate to remote OCI region, with min. 14 day rolling policy
File	Backup to OCI immutable object storage and replicate to remote OCI region, with min. 14 day rolling policy
Object	Backup to OCI immutable object storage and replicate to remote OCI region, with min. 14 day rolling policy

Q&A

Michael.Miller@syntax.com

ASCEND 2024

Thank You For Attending!

Please complete the session survey in the conference app.

ASCEND 2024