ORACLE

Best Practices for Deploying Commvault on Oracle Compute Cloud@Customer

A Step-by-Step Guide to Installing, Configuring, and Deploying Backup and Restore on Compute Cloud@Customer

Version [1.0]

Public

ORACLE

Purpose statement

This document outlines best practices for deploying Commvault on Oracle Private Cloud Appliance (PCA), providing a step-by-step guide for installing, configuring, and implementing backup and restore functionality on the PCA.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. 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, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

ORACLE

Table of contents

Introduction

Compute Cloud@Customer (OC3) provides on-premises Infrastructure as a Service (IaaS) with Oracle Cloud Infrastructure (OCI) API compatibility, offering localized control to meet stringent data sovereignty and compliance requirements. This guide demonstrates a typical hybrid data protection scenario implemented with Commvault, where restores are executed on OC3 to maintain data locality, while backups can be offloaded to OCI object storage for long-term archiving, as long as compliance requirements are met.

This content is provided for informational purposes and self-supported guidance only. Consultancy or other assistance related to the content is not covered under the Oracle Support contract or associated service requests. If you have questions or additional needs, then please do reach out to your Oracle Sales contact directly.

Commvault Architecture Overview

Here is a reference to the official Commvault documentation: Commvault Documentation Link.

The CommCell is the foundational management unit in Commvault, consisting of all the components necessary for data protection and management. It includes key elements such as the CommServe (the central management server), MediaAgents, Command Center, and protected systems. The CommCell provides a unified environment for managing backups, restores, and data protection policies, with centralized configuration, monitoring, and administration for all operations.

Commvault can be deployed in different configurations depending on the scale of the environment. In a small deployment, an all-in-one configuration is commonly used, where the CommServe, MediaAgent, and Command Center are installed on a single server. This configuration simplifies deployment and management, providing efficient data protection and recovery within a smaller scope. For larger deployments, Commvault scales by distributing components such as CommServe and MediaAgents across multiple servers. This horizontal scaling allows for the handling of larger data volumes, more complex backup operations, and additional clients, while still maintaining centralized management across the entire environment.

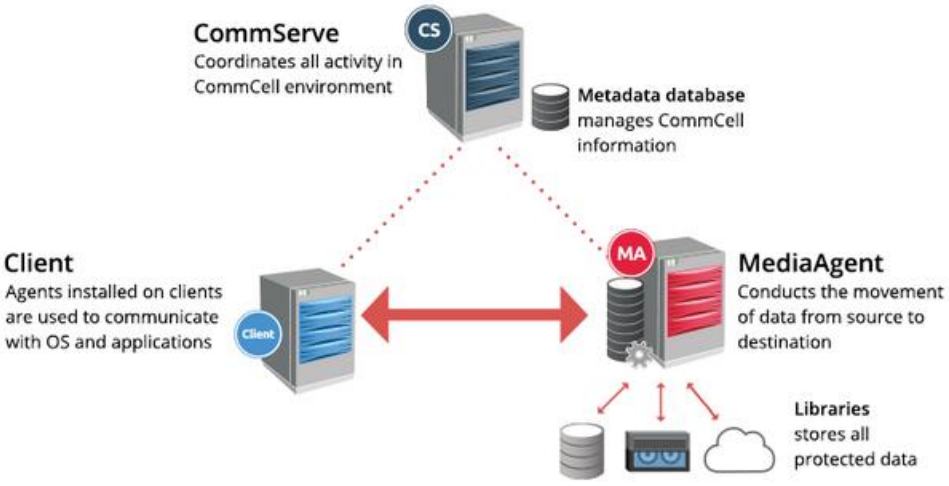


Table1: Commvault Architecture Components

CommServe Server	• Central management component of the CommCell environment. • Coordinates and executes all CommCell operations. • Maintains Microsoft SQL Server databases containing configuration, security, and operational history.
Command Center	• Web-based interface for configuring backups, restores, and data protection policies. • Supports scheduling tasks and monitoring operations. • Uses pre-set options to minimize configuration. • Provides an operational interface for tenants in multi-tenant environments. • CommCell Console (Java-based) is still available for advanced configurations.

MediaAgents	• Manages the movement of backup and restore data. • Can be deployed on a dedicated server or co-located with the CommServe, depending on the Oracle Compute Cloud@Customer (OC3) deployment architecture. • Sends backups to OCI Object Storage for secure long-term archiving. • Utilizes OC3's fast local storage for quick restores.

Protected Servers and Clients	• Represents systems and applications protected by Commvault.
	• In the Command Center:
	  ○ **Servers** refer to Commvault infrastructure (MediaAgents, backup servers).
	  ○ **Clients** refer to logical entities being backed up (file systems, databases, virtual machines).
	• On OC3, clients are the VMs and applications running on the appliance.

Access Nodes (Proxies)	• Also known as proxies or VSA clients. • Simplify virtual machine backups on PCA. • Eliminate the need to install Commvault software on each guest OS. • Minimize resource consumption and streamline management. • Facilitate file recovery by staging backup data. • Can function as MediaAgents for data movement. • Essential for efficient VM protection in virtualized OC3 environments.

Deployment Considerations and Prerequisites

While a large enterprise Commvault deployment would typically distribute these components across multiple virtual machines for scalability and resilience, this guide demonstrates an all-in-one installation on a single Oracle Compute Cloud@Customer VM for simplified configuration.

For this installation and configuration, we have used Commvault platform release 11.36, demonstrating an all-in-one Commvault configuration on both a Windows 2022 VM and a Linux VM within the Oracle Compute Cloud@Customer, M3.10.3 Appliance. This all-in-one setup hosts the CommServe, MediaAgent, and Virtual Server Agent (VSA) on a single VM for simplified configuration in both operating system environments.

Prerequisites

Prior to commencing the installation, it is essential to ensure that all necessary prerequisites are satisfied.

- **Oracle Compute Cloud@Customer (OC3) Access:** Ensure you have an active account with the appropriate permissions to create and manage resources on the OC3.
- **Oracle Cloud Infrastructure (OCI) Access:** Confirm that you have the necessary access and permissions in OCI to create and manage resources, including Object Storage buckets.
- **Create a Commvault User and Group:** It is recommended to create a Commvault user and group, and assign them their API keys.
- **Commvault Account:** Obtain the latest compatible Commvault platform release from the Commvault Store using your active Commvault account. (Note: This document was created using Commvault platform release 11.36. Please consult the Commvault documentation for any version-specific changes.)
- **Remote Desktop Access:** Ensure you have access to a remote desktop client (e.g., Windows Remote Desktop Connection) to connect to the Windows 2022 VM on OC3.
- **Network Verification:** Verify network connectivity from the Windows 2022 VM in OC3 to OCI object storage and ensure DNS resolution and firewall rules allow Commvault communication.
- **Firewall Configurations:** Configure firewalls (Windows Firewall, PCA network firewalls) to allow communication between Commvault components. In some cases, firewalls may need to be temporarily disabled or configured to allow the required traffic.
- **FQDN Resolution:** Ensure that Fully Qualified Domain Names (FQDN) for CommServe and Access Nodes are resolvable within your network. The FQDN will be needed when configuring CommServe and Access Nodes in the Commvault Command Center.

- **VCN, Subnets, and Security Lists:** Verify that Virtual Cloud Network (VCN), subnet, and security list configurations permit necessary connections for Commvault communication.
- **System Requirements:** For the all-in-one Commvault configuration, the Windows 2022 VM must meet the following minimum hardware requirements: 16 CPU cores, 32 GB RAM, and 2 TB SSD storage.
- **OCI API Key Configuration:**
    - Create a Commvault user and group in OCI Identity and Access Management (IAM).
    - Generate an OCI API key pair for the Commvault user and record the fingerprint.
    - Create IAM policies at the tenancy and compartment levels to grant the Commvault user the necessary permissions to access and manage OCI Object Storage buckets. See the required permissions in the Commvault documentation: https://documentation.commvault.com/2024e/essential/permissions_for_oracle_cloud_infrastructure.html
- **Clock Synchronization:** Ensure all systems, including OCI instances, OC3, and MediaAgents, are synchronized to a reliable NTP server to avoid time-related authentication and communication issues.

Important Considerations

- ✓ **Public IP for External Access: If external network access is required for backup or restore operations, ensure a public IP address is assigned to the C3. Note that restore operations may fail without a public IP.**
- ✓ **The Out of Place Restore UI may take longer to load lists of networks and subnets, since search query support is not available.**
- ✓ **iSCSI attachments to the access node are not supported. By default, only attachments with paravirtualized mode are used.**
- ✓ **Oracle Compute Cloud@Customer does not support `AddImageShapeCompatibilityEntry`. Therefore, if an image associated with the source instance is deleted, the restore will fail.**

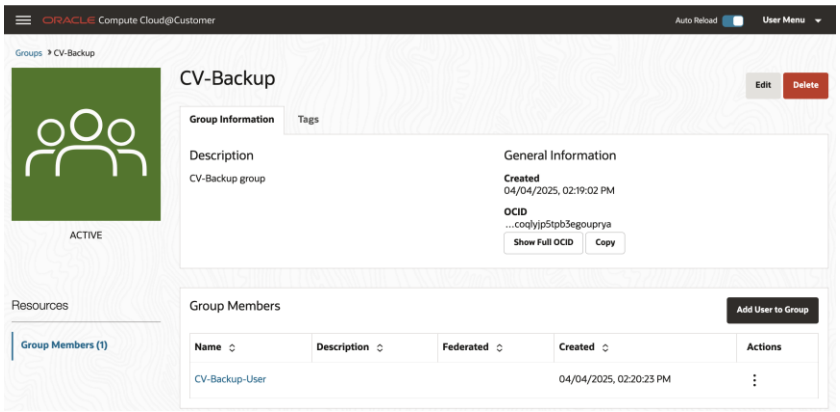
Configure Oracle Compute Cloud@Customer Identity and Access Management for Commvault

For securing the Commvault environment in Oracle Compute Cloud@Customer (OC3), it is essential to create dedicated users and groups with appropriate access controls in **Oracle Cloud Infrastructure (OCI)**, following the principle of least privilege. This centralized approach ensures consistency across Oracle environments, simplifies permission management, and enhances overall security.

✓ Note: IAM for OC3 is managed through the OCI Console. Users and groups are created in OCI and are synchronized with OC3. However, group membership must be explicitly assigned again within the OC3 environment. This ensures that users have the appropriate group-based access within OC3. API key fingerprints are generated in OCI and used in OC3 for CLI or SDK authentication.

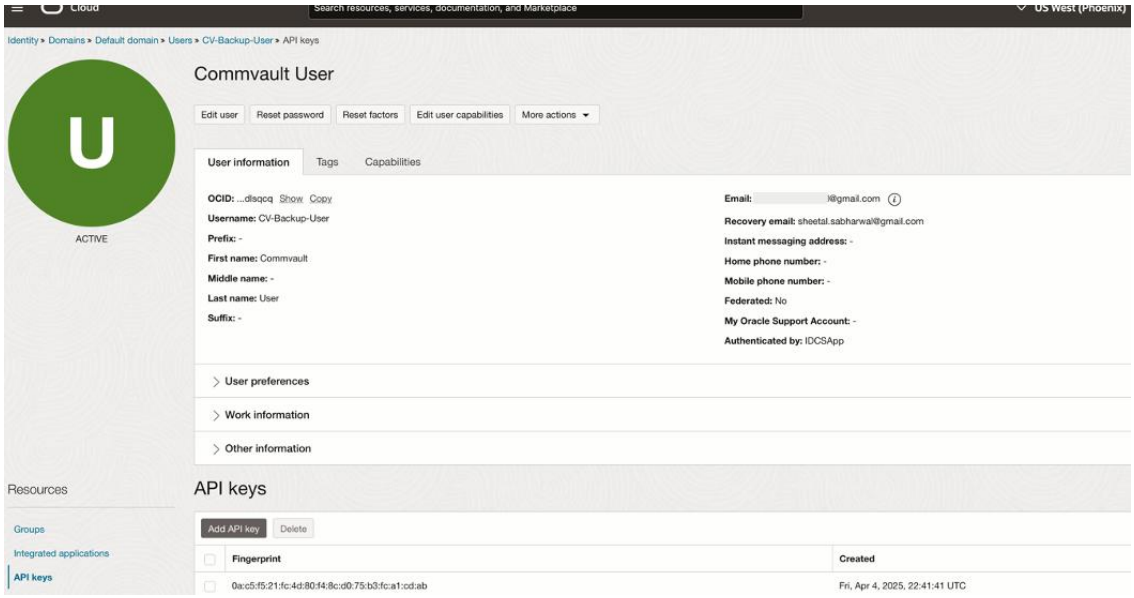
1. **Create Commvault User and Group**

- **Create User in OCI:**
    i. Navigate to **Identity > Users** in the OCI management console.
    ii. Click **Create User**, provide a **name**, **description**, and **email address**, and click **Create** to add the user.
- **Create Group in OCI:**
    i. Navigate to **Identity > Groups** and click **Create Group**.
    ii. Provide a **name** and **description** for the group and click **Create** to create the group.
- **Add User to Group in OC3:** Once the user and group is created in OCI, within seconds you will see them in OC3.
    i. In the OC3 Console, go to **Identity > Groups**, click on the group name.
    ii. Under **Group Members**, click **Add User to Group**, select the user from the drop-down list, and add them.



2. **Assign API Keys**

- In the OCI Console, click the **username** under **Identity > Users**
- Under **Resources**, select **API Keys**, then click **Add API Key**.
- Upload a public key or generate one using the dialog. Save the private key securely.
- A fingerprint will be generated—make a note of it. This is needed for authentication when configuring Commvault and accessing Oracle Cloud Infrastructure (OCI) resources.

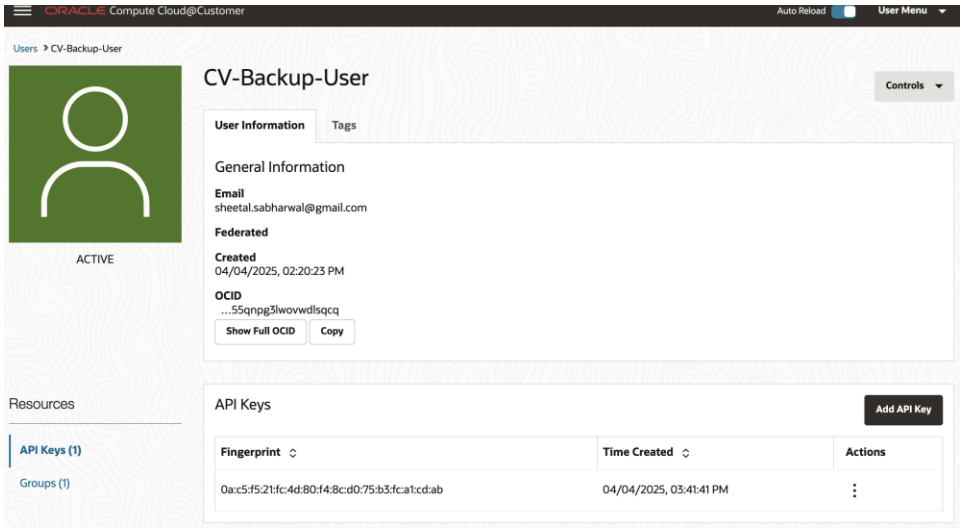


3. **Register API Key in OC3:** Even though the user is synced from OCI, you must register the same public key in OC3 for CLI/SDK operations in the OC3 environment.

- In the OC3 Console, navigate to Identity > Users and select the same user.
- Go to the API Keys section.
- Click Add API Key, and upload the same public key file (.pem format) used in OCI.
- Once uploaded, OC3 will generate a separate fingerprint. Make a note of this fingerprint — it will be used when configuring CLI or SDK-based tools (such as Commvault) to access OC3 resources.

✓ Note: OCI and Oracle Compute Cloud@Customer (OC3) use independent key registries. Even if the user is synced, API keys must be registered separately in OC3 to enable secure authentication within the OC3 environment.

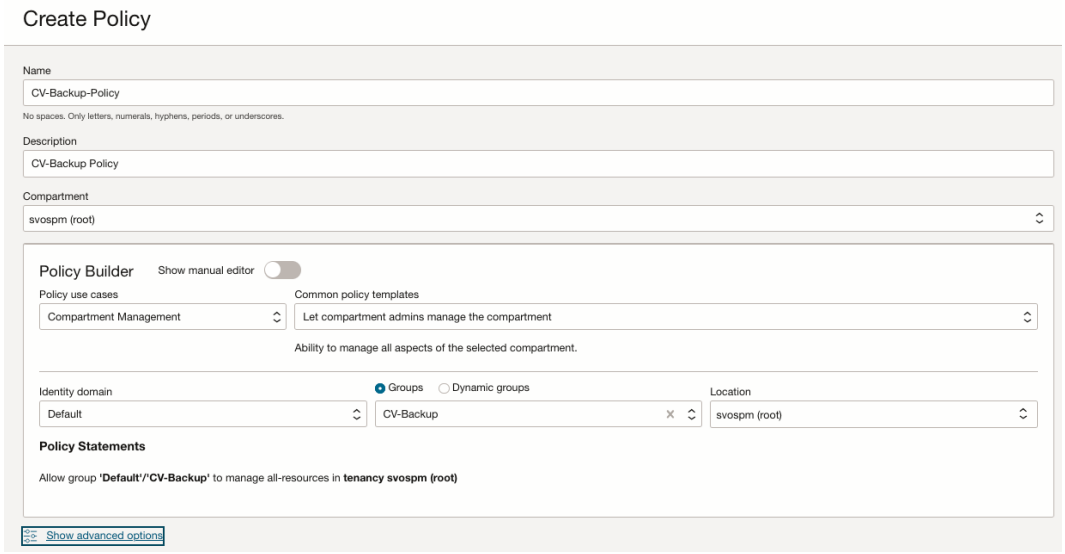
✓ If you upload the same public key in both OCI and OC3, the fingerprint will be identical. However, the key must still be explicitly added in OC3, as key stores are independent between OCI and OC3.



4. **Define IAM Policies**

> ✓ Note: IAM policy definitions are only possible in OCI. Oracle Compute Cloud@Customer (OC3) inherits and enforces these policies, but you cannot define or modify them directly from the OC3 interface.

To ensure that the Commvault user and group have the necessary permissions for managing resources within OC3, you need to configure specific IAM policies both at the tenancy and compartment levels in OCI.



At the Tenancy Level: Create the following IAM policies to allow the group to inspect and use key OCI resources:

- allow group <group-name> to inspect compartments in tenancy
- allow group <group-name> to use vcns in tenancy
- allow group <group-name> to use subnets in tenancy
- allow group <group-name> to use vnics in tenancy
- allow group <group-name> to use tag-namespaces in tenancy

At the Compartment Level: Define these IAM policies for more granular control within specific compartments:

- allow group <group-name> to inspect vcns in compartment <compartment-name>
- allow group <group-name> to inspect vnic-attachments in compartment <compartment-name>
- allow group <group-name> to manage buckets in compartment <compartment-name> where any {request.permission='BUCKET_CREATE', request.permission='BUCKET_INSPECT', request.permission='PAR_MANAGE'}
- allow group <group-name> to use subnets in compartment <compartment-name>
- allow group <group-name> to use vnics in compartment <compartment-name>
- allow group <group-name> to manage boot-volume-backups in compartment <compartment-name>
- allow group <group-name> to manage instance-images in compartment <compartment-name>
- allow group <group-name> to manage instances in compartment <compartment-name>
- allow group <group-name> to manage objects in compartment <compartment-name>
- allow group <group-name> to manage volume-attachments in compartment <compartment-name>
- allow group <group-name> to manage volume-backups in compartment <compartment-name>
- allow group <group-name> to manage volumes in compartment <compartment-name>
- allow group <group-name> to manage buckets in compartment <compartment-name> where any {request.permission='BUCKET_READ', request.permission='BUCKET_UPDATE', request.permission='BUCKET_CREATE', request.permission='BUCKET_INSPECT'}

Commvault Installation and Configuration

On Windows VMs, Commvault installation can be performed using the Download Manager, an interactive wizard that simplifies local installations and custom package creation (see

https://documentation.commvault.com/11.20/installing_commvault_locally_on_windows_computers_using_download_manager.html). Note: Download Manager is not supported on Linux VMs.

Commvault Windows Based Installation

The following steps outline the process for installing and configuring Commvault on a Windows 2022 VM within the Oracle Compute Cloud@Customer(OC3) for an all-in-one data protection solution.

1. **Provision Windows 2022 VM on OC3**
2. **Install Commvault Software**
3. **Configure CommServe**

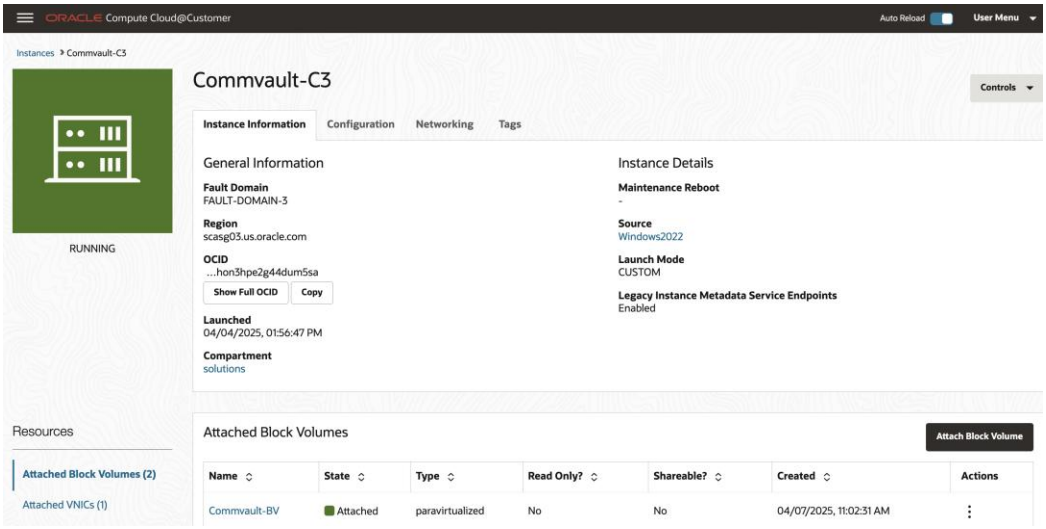
1. Provision Windows 2022 VM on OC3

1.1. Create the Windows 2022 Instance

- Provision a Windows Server 2022 virtual machine on your OC3.
- For detailed instructions on creating a new instance in OC3, refer to the official OC3 documentation: Tutorial: Launching Your First Instance.

1.2. Create and Attach a Block Volume

- Create and attach a block volume to the Windows 2022 instance. This volume will be used for Commvault data storage.
- To create and attach a block volume, consult the OC3 documentation for instructions: Attach the Block Volume to an Instance

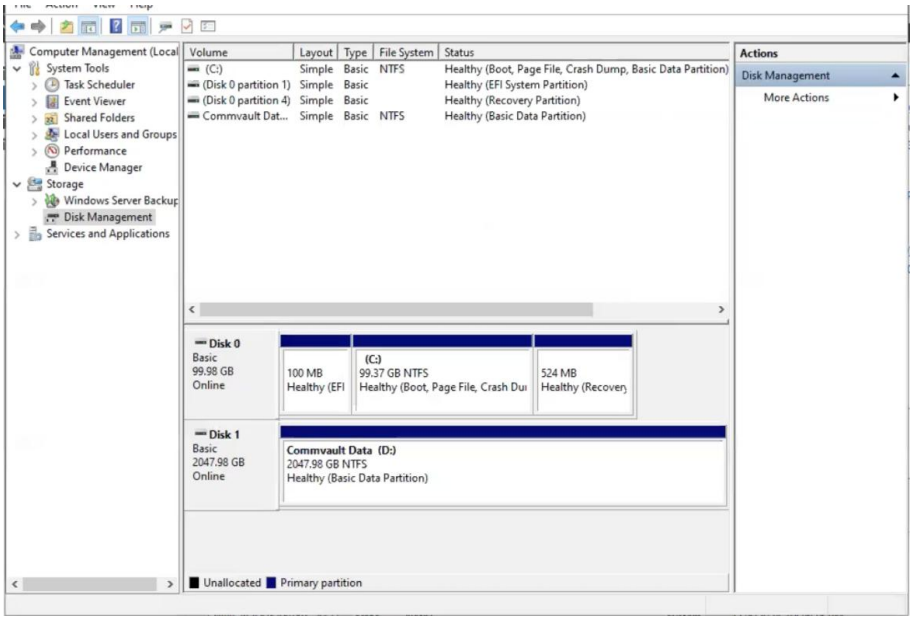


1.3. Access the Windows Instance

- Connect to the Windows Server 2022 instance using a Windows App (formerly known as Windows Remote Desktop Client).

1.4. Initialize and Format the Block Volume

- After connecting to the Windows 2022 instance, open Disk Management by right-clicking the Start Menu and selecting Disk Management.
- Locate the newly attached, unallocated disk and right-click it to Initialize. Select GPT (GUID Partition Table), especially for disks larger than 2 TB.
- Right-click the unallocated space and choose New Simple Volume.
- Follow the wizard to assign a drive letter (e.g., D:), select the desired file system (typically NTFS or ReFS), and provide a volume label.
- Once formatted, the volume will appear as a new drive under This PC, ready for use.



2. Install Commvault Software

2.1. Download the Commvault Media Kit:

- Download the latest compatible version of the Commvault Express Media Kit directly onto the Windows 2022 VM on OC3 from the Commvault Store using your Commvault account. You can access and download the kit here: Commvault Express Media Kit.
- For detailed installation instructions, refer to the Commvault 11.36 Quick Start Guide: https://documentation.commvault.com/2024e/essential/quick_start_guide.html

2.2. Extract the Installation Files:

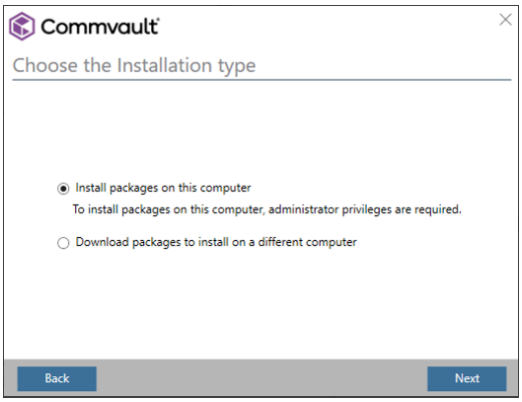
- Log on to the Windows 2022 VM as a user with administrator privileges.
- Navigate to the folder containing the Commvault media kit file.
- Right-click the file and select "**Run as administrator**."
- In the "**Download Manager**" dialog box, confirm the destination folder for installer files (or select a different folder) and click "**Extract**."
- The Commvault installation wizard will open, providing a link to review the **license agreement**.

2.3. Accept the License Agreement

- Select the "**I Agree**" checkbox and click "**Next**."

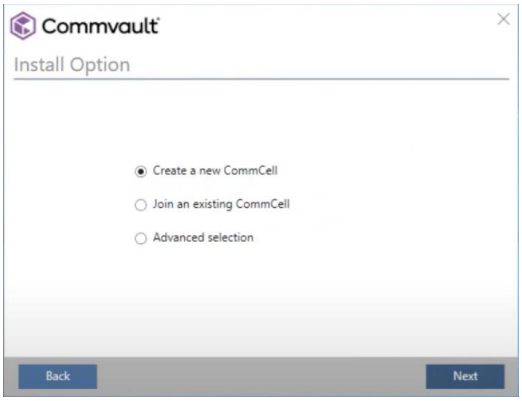
2.4. Select Installation Type

- Choose the desired installation type and click "**Next**."



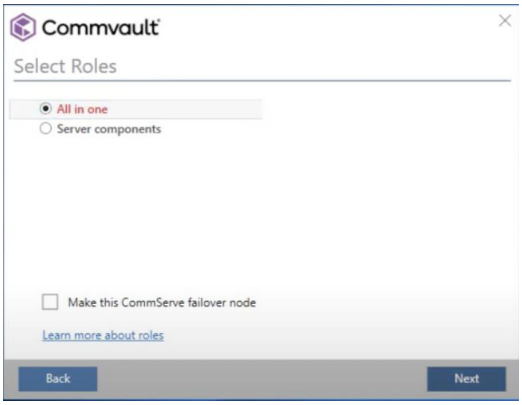
2.5. Select Installation Option

- Choose "**Create a new CommCell**" and click "**Next**."



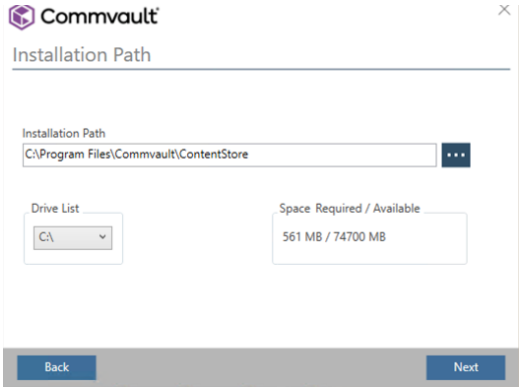
2.6. Select Roles

- Choose the "**All-in-one configuration**" option and click "**Next**."



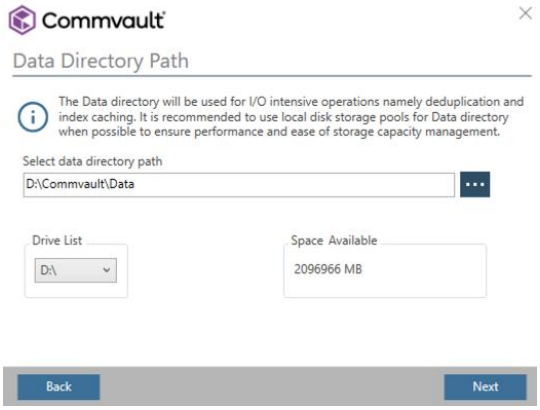
2.7. Confirm Installation Path

- Confirm the installation path or select a different folder. Verify sufficient space, then click "**Next**."



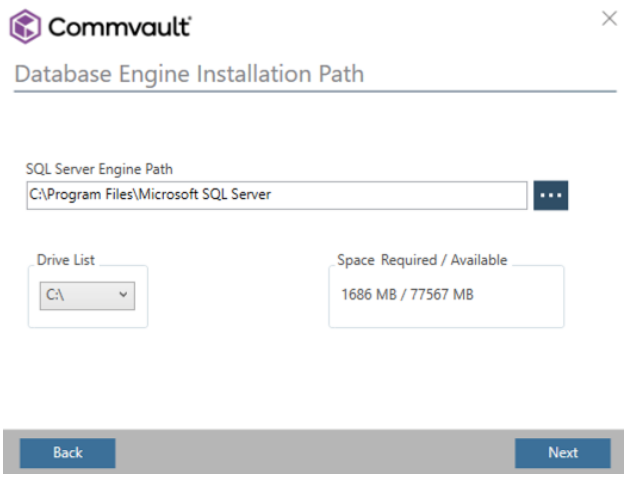
2.8. Data Directory Path

- Click "**Next**."



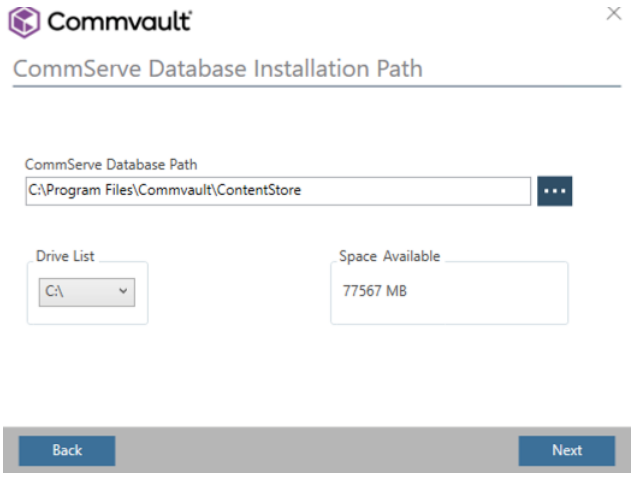
2.9. SQL Server Engine Path

- Click "**Next**."



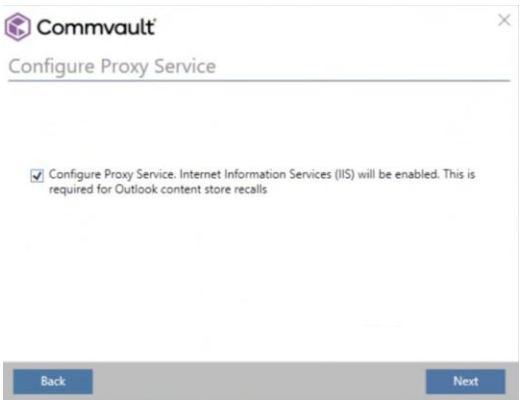
2.10. CommServe Database Path

- Specify the "**CommServe Database Path**" and click "**Next**."



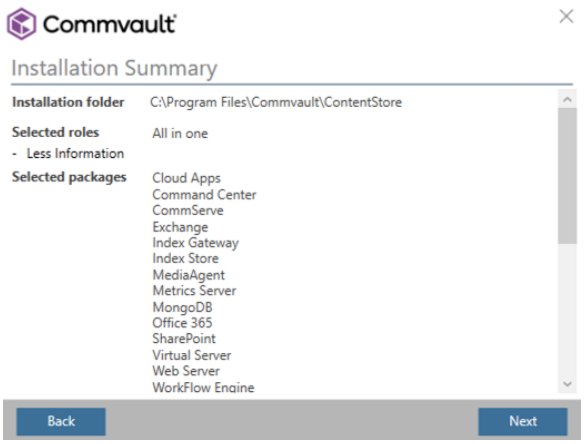
2.11. Configure Proxy Service (Optional)

- If needed, select "**Configure Proxy Service**" and click "**Next**."



2.12. Installation Summary

- Review the summary and click "**Next**."

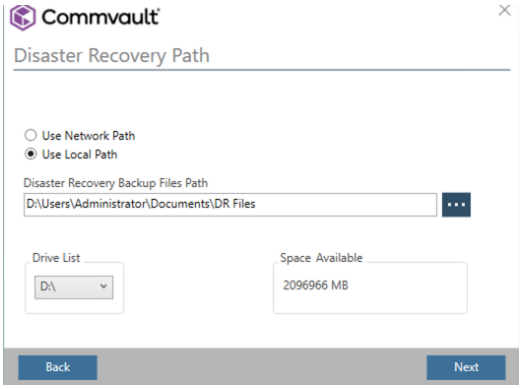


2.13. Start Installation

- Click "**Next**" to begin installation

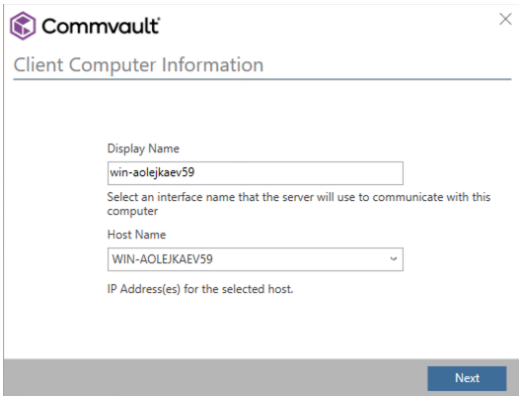
2.14. Data Recovery Path

- Click "Next"



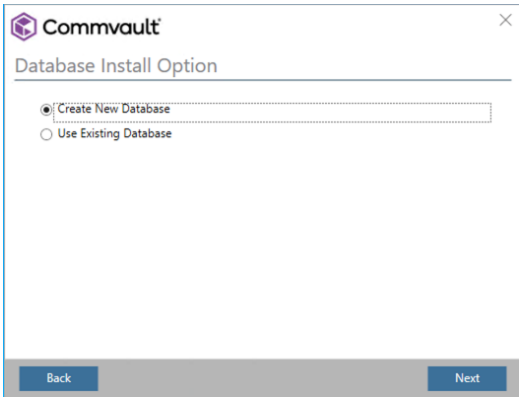
2.15. Client Computer Information

- Enter "**Client Name**" and "**Host Name**," then click "**Next**."



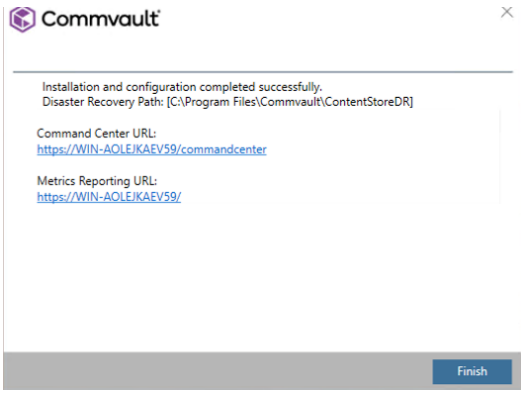
2.16. Select Database Install Option

- Choose "**Use existing account**" or "**Create new account**" and click "**Next**."



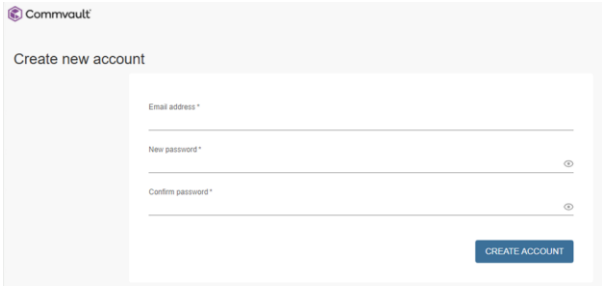
2.17. Finish Installation

- Click "**Finish**." The Command Center will open in the default browser.



2.18. Configure Command Center Administrator

- Enter the administrator email and password. Enter the activation code, followed by contact and mailing information. Click "**Register**" to complete setup.



3. Configure CommServe

3.1. Configure CommCell User Credentials

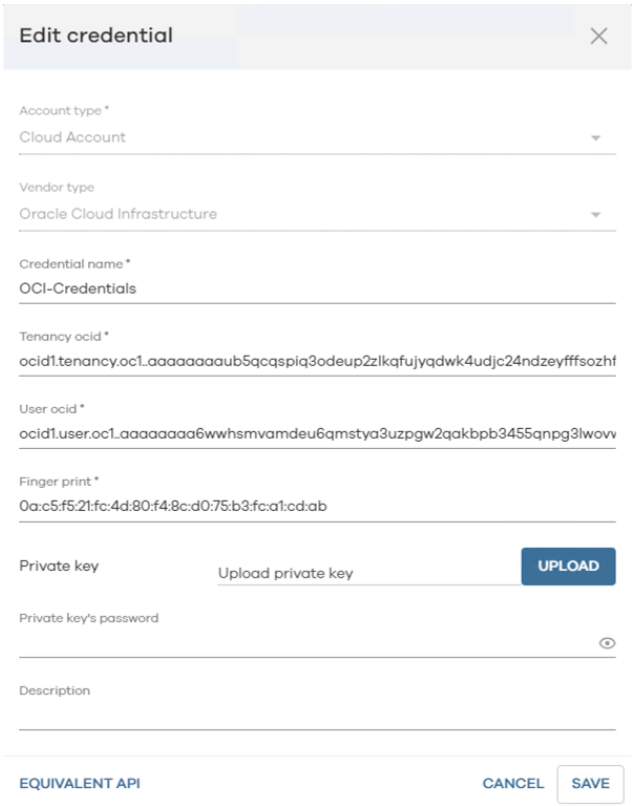
Since **Oracle Compute Cloud@Customer (C3)** is an extension of OCI, only **one set of OCI credentials** is required to access both VM resources and OCI Object Storage. Follow these steps to configure the OCI credentials in Commvault:

1. **Navigate to Credential Vault:**
    - In the Commvault Command Center, go to **Manage > Security**.
    - Click the **Credential Vault** tile.
2. **Add Credentials:**
    - Click **Add**.
    - Select **Account Type** as **Cloud Account**.
    - Select **Vendor Type** as **Oracle Cloud Infrastructure**.
    - Provide a **Credential** name (e.g., "OCI-C3-Credentials").
    - Enter the **Tenancy OCID, User OCID and Fingerprint** associated with C3 user.
    - Upload the corresponding **Private Key** file.
    - Click **Save**.

Note: For instructions on generating API signing keys in OCI, refer to the OCI documentation:

https://docs.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm

User Credentials for Commvault to access OC3



Note on Commvault Credentials for C3

Oracle Compute Cloud@Customer (OC3) Credential:

- ✓ **When Adding the Hypervisor: Use the OCI credentials to register the C3 environment in Commvault and enable VM discovery and management.**
- ✓ **When Performing VM Operations: Use the same OCI credentials for VM-related operations (e.g., snapshots, VM restores).**
- ✓ **When Adding Cloud Storage: Use the same OCI credentials to configure access to OCI Object Storage.**
- ✓ **During Backup and Restore Operations: Use the credentials to write to and read from the designated OCI Object Storage bucket.**

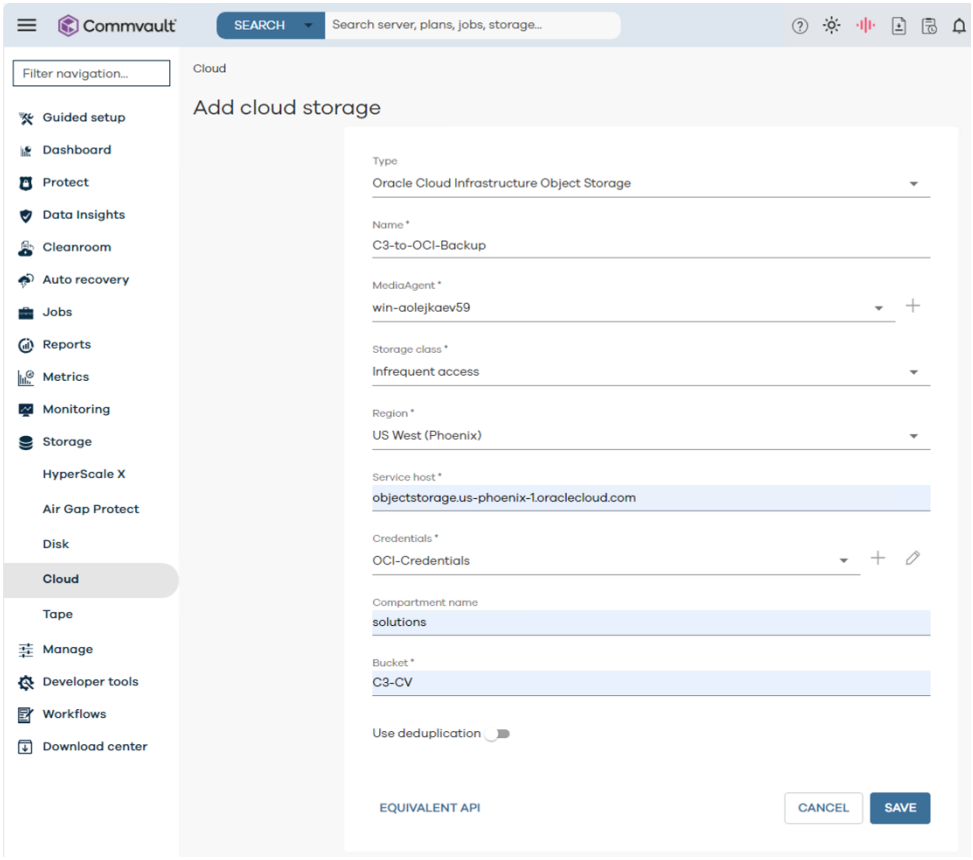
3.2. Configure Storage (OCI Object Storage as a Backup Target)

To configure Commvault to use OCI Object Storage as a backup target for your Oracle Compute Cloud@Customer environment:

- **Navigate to Cloud Storage:** In the Commvault Command Center, go to **Storage > Cloud**.
- **Add Cloud Storage:** Click **Add** in the top-right corner.
- **Configure OCI Object Storage:**
  - **Type:** Select Oracle Cloud Infrastructure.
  - **Name:** Provide a descriptive name.

- **MediaAgent:** Select the MediaAgent (installed on the same VM as the CommServe in an all-in-one configuration).
- **Service host:** Enter the object storage API endpoint (e.g., objectstorage.us-phoenix-1.oraclecloud.com).
- **Credential Name:** Choose the OCI credential created earlier.
- **Compartment:** Select the OCI compartment.
- **Bucket Name:** Enter the name of the OCI bucket for backups.

- **Click Save.**

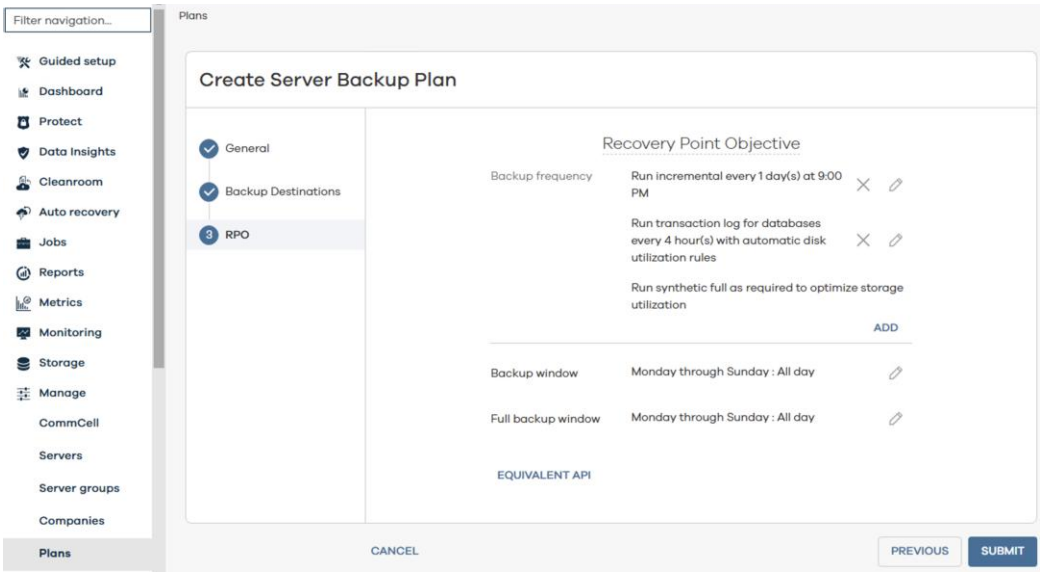


3.3. Configure Server Backup Plan

For full details, refer to the official Commvault documentation. Creating a Server Plan

- Go to **Manage > Plans** in **Commvault Command Center**.
- Click **Create Plan** and select **Server Backup**.
- Enter a name or select an existing base plan.
- Add **Backup Copy** and set retention rules.
- Optionally, add **Snapshot Copy** and configure retention.
- Set backup schedules, time zones, and log frequencies.
- Enable backup copy and configure actions for delayed snapshots.
- Review and click **Save**.

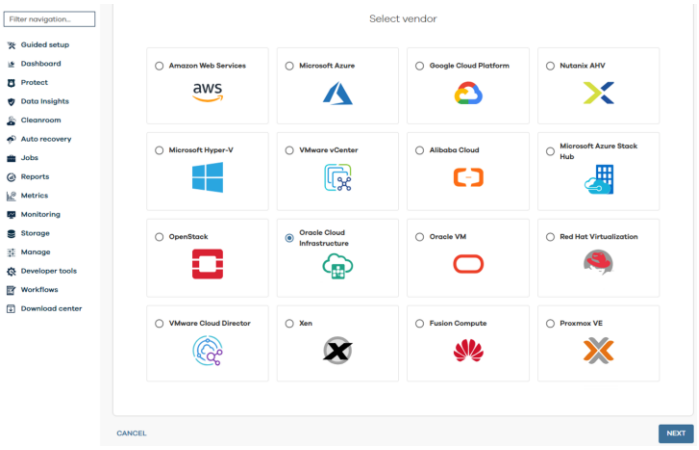
For detailed instructions on each step and additional configuration options, refer to the Commvault documentation.



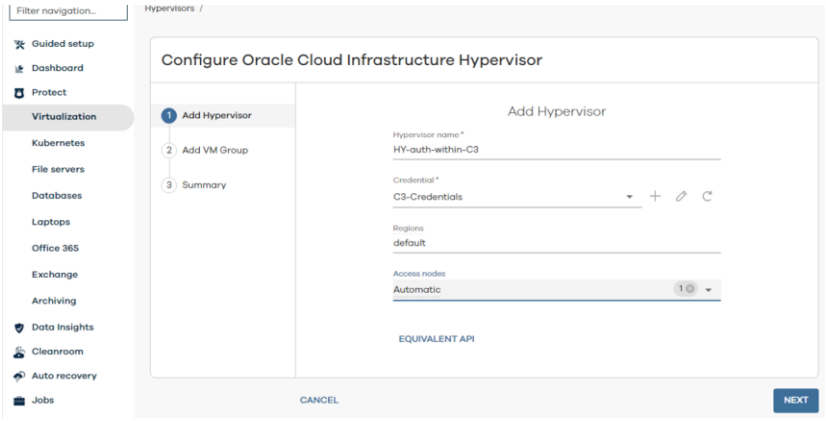
3.4. Configure Hypervisor and VM Group:

For full details, refer to the official Commvault documentation. Adding an Oracle Cloud Infrastructure Hypervisor

- **Configure Hypervisor:**
  - Go to **Protect > Virtualization** in the Command Center navigation pane.
  - Click **Add** hypervisor.
  - Select **Oracle Cloud Infrastructure**, then click **Next**.



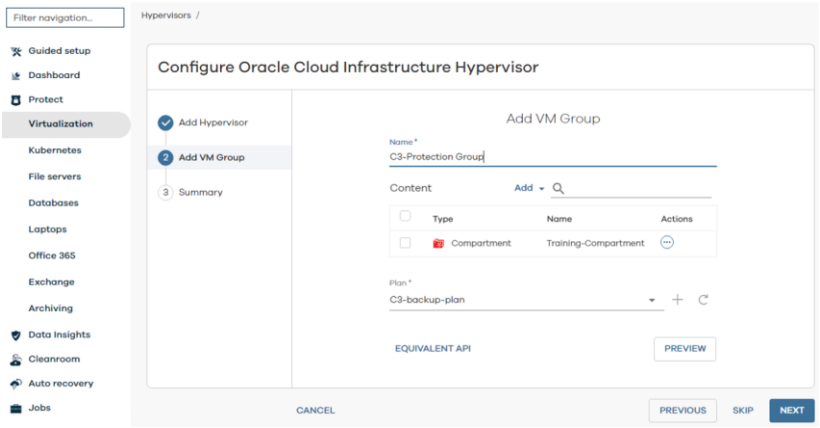
  - Enter a descriptive name for the hypervisor.
  - Choose saved credentials or create new ones:
  - Select **Credentials** created in the prior step.
  - Leave **Regions** field as default.
  - Select an **Access node** (previously deployed proxy).
  - Click **Next**.



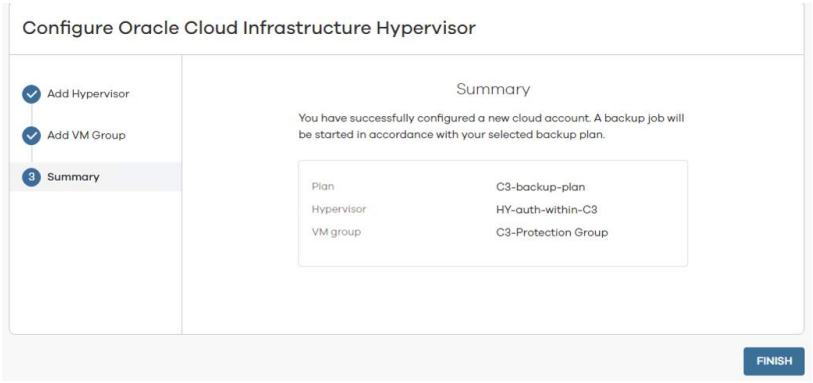
- **Configure VM Group:**

  For full details, refer to the official Commvault documentation Adding a VM Group for Oracle Cloud Infrastructure.

  - Go to **Protect > Virtualization** in the Command Center.
  - Click the **VM groups** tab, then **Add VM group**.
  - Provide the hypervisor, backup plan, and a descriptive name for the VM group.
  - Click **Add > Content** to add instances.
  - Choose **Region View**, **Instance View**, or **Tag View** to select VMs.
  - Click **Add > Rule** to define a rule for auto-discovery of instances.



  - Click **Next** to save the VM group.
  - Review **Summary** and click **Finish.**



Commvault Linux Based Installation

For Linux-based installations on C3, you can follow the same installation steps documented for PCA. Refer to the Commvault on Oracle Private Cloud Appliance Best Practices Guide for the command-line installation process after transferring the package to the target system.

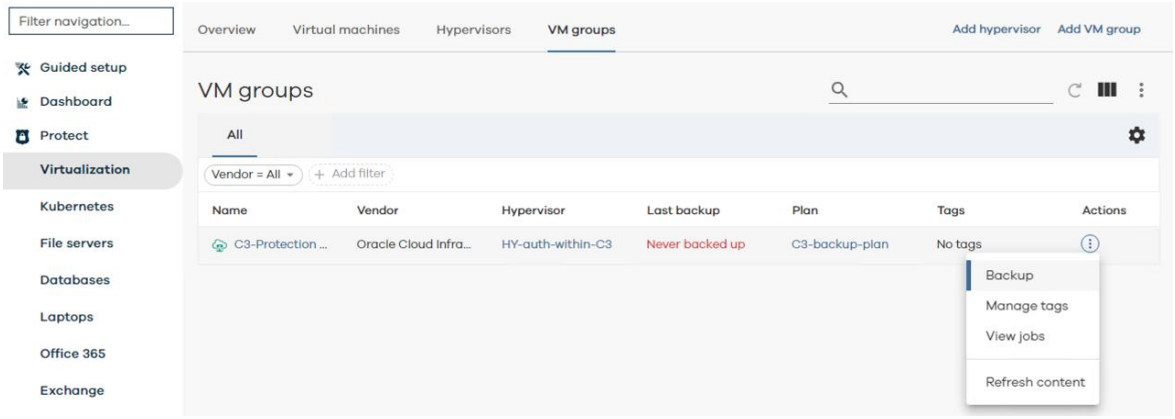
Backup and Restore of VM Workloads

The backup and restore process ensures data protection by allowing backups to OCI while enabling recovery on C3. This supports disaster recovery, workload mobility, and compliance requirements.

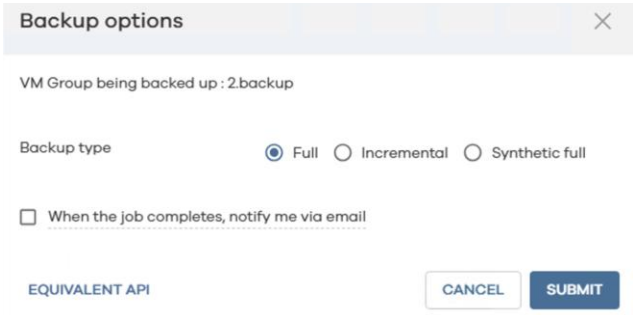
Backup to OCI Bucket

For full details, refer to the official Commvault documentation Performing Backups for OCI Instances or VM Groups.

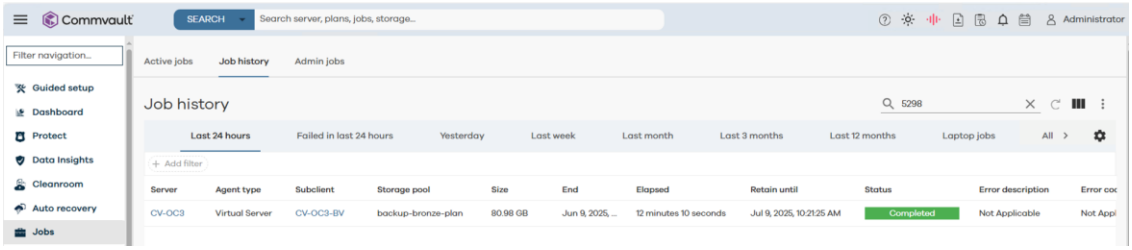
1. From the Command Center, navigate to **Protect > Virtualization.**
2. Go to the instance or VM group you want to back up:
3. For a single instance, select **Virtual Machines**, click the **action button**, and choose **Back up**.



4. For all instances in a VM group, select VM Groups, click the action button, and choose **Back up**.
    - In the Backup options dialog box, select the Backup type.



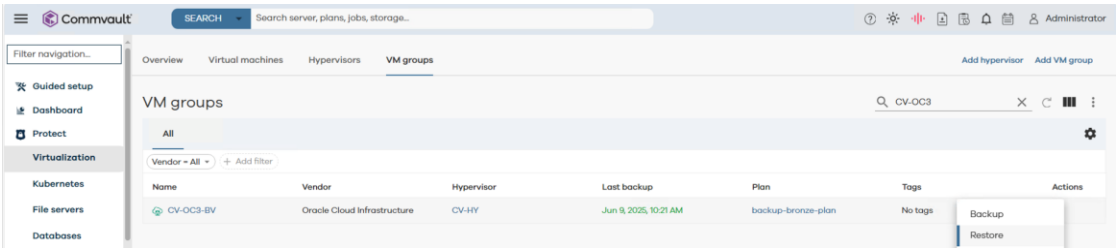
- If backing up a single instance, you can set a custom Retention period by clicking Edit retention settings.
- Click Submit to start the backup.



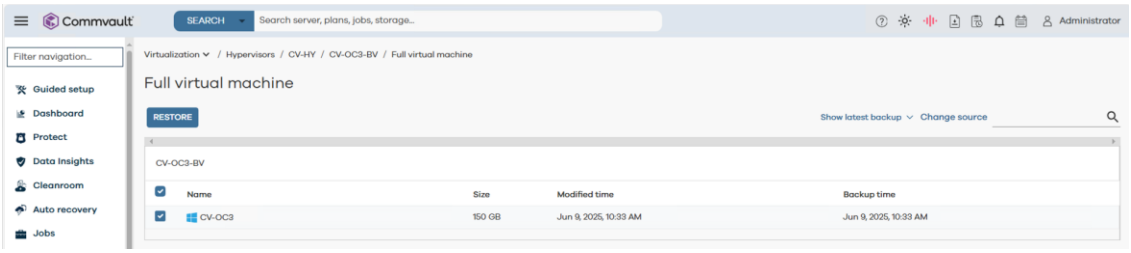
Restore

Restoring instances from OCI backups can be done to either the original location or a different location. By default, an instance is restored to the original hypervisor, using the same proxy that was used during the backup process. For full details, refer to the official Commvault documentation Restore Full Instances for OCI.

1. From the **Command Center** navigation pane, go to **Protect > Virtualization**.
2. Click the **VM Groups** tab and select **Restore** for the desired VM group.



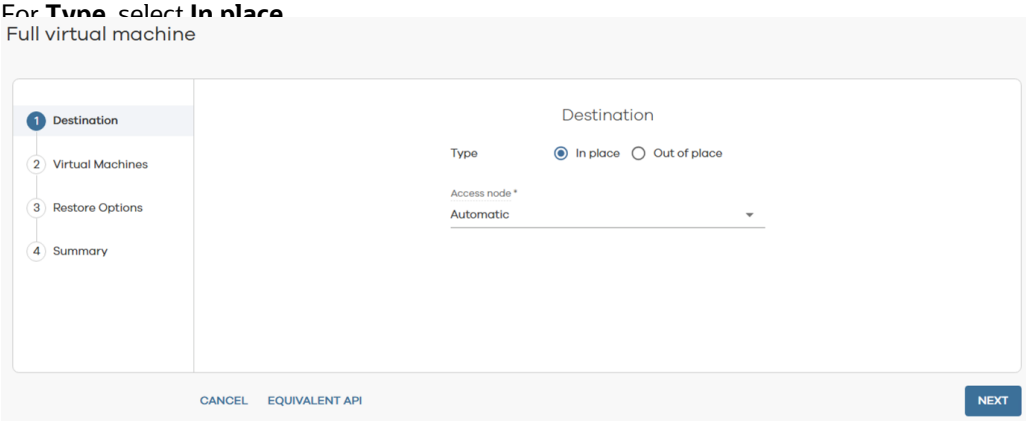
3. On the **Full virtual machine** page, select the instances to restore and click **Restore**.



In Place Restores

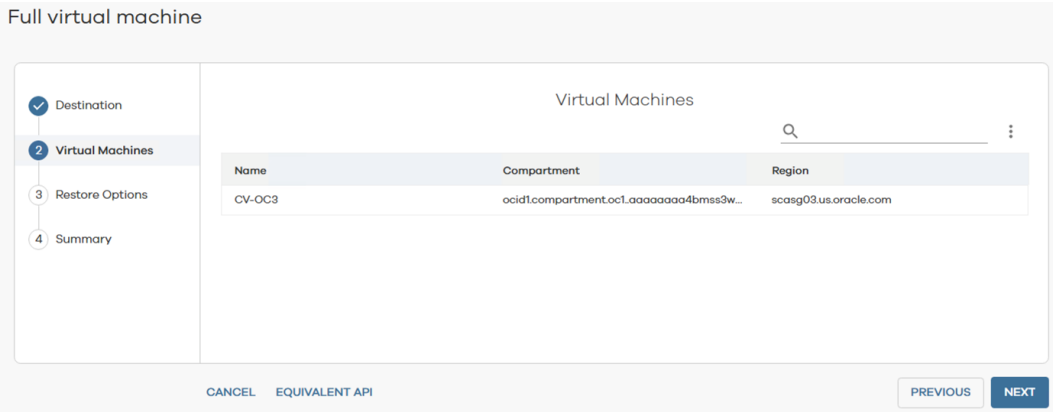
1. **Specify the Restore Destination**:

- For **Type**, select **In place**

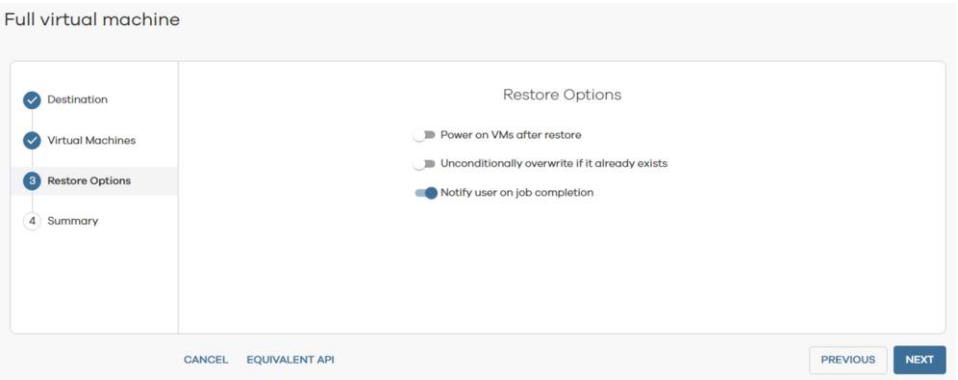


- For **Access node**, select **Automatic** or a specific from the drop-down .
- Click **Next**.

2. **Virtual Machine Settings**:
   - You can configure restore options and/or continue.
   - Click **Next**.

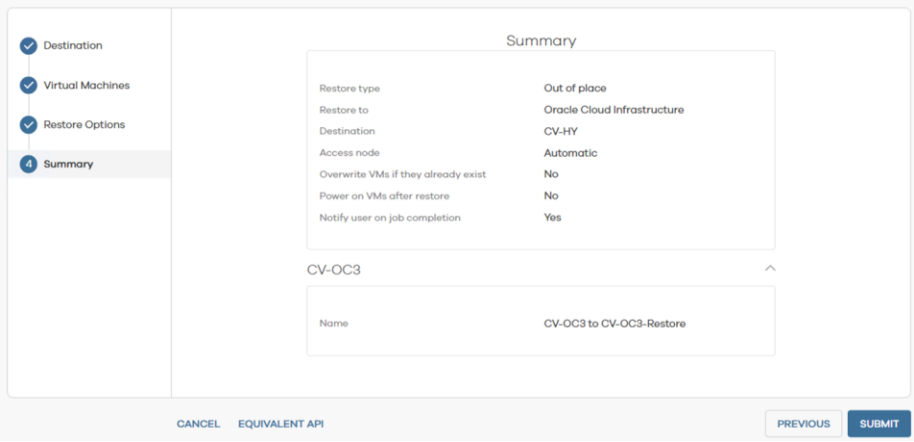


3. **Specify the Restore Options**:
   - **Power on VMs after restore**: Automatically restart virtual machines.
   - **Unconditionally overwrite if it already exists**: Overwrite existing virtual machines with the restored instance.
   - Click **Next**.



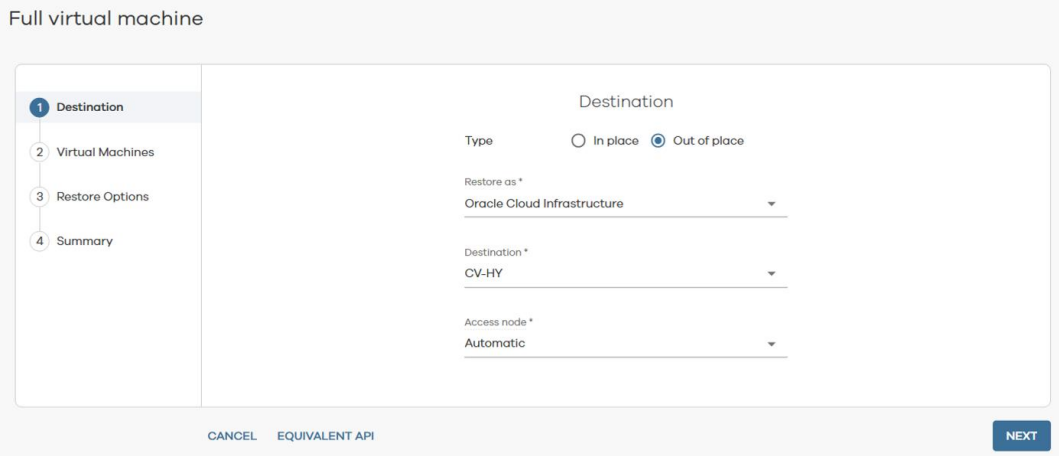
4. **Review and Start the Restore**:

- Review settings and click **Submit** to initiate the restore.

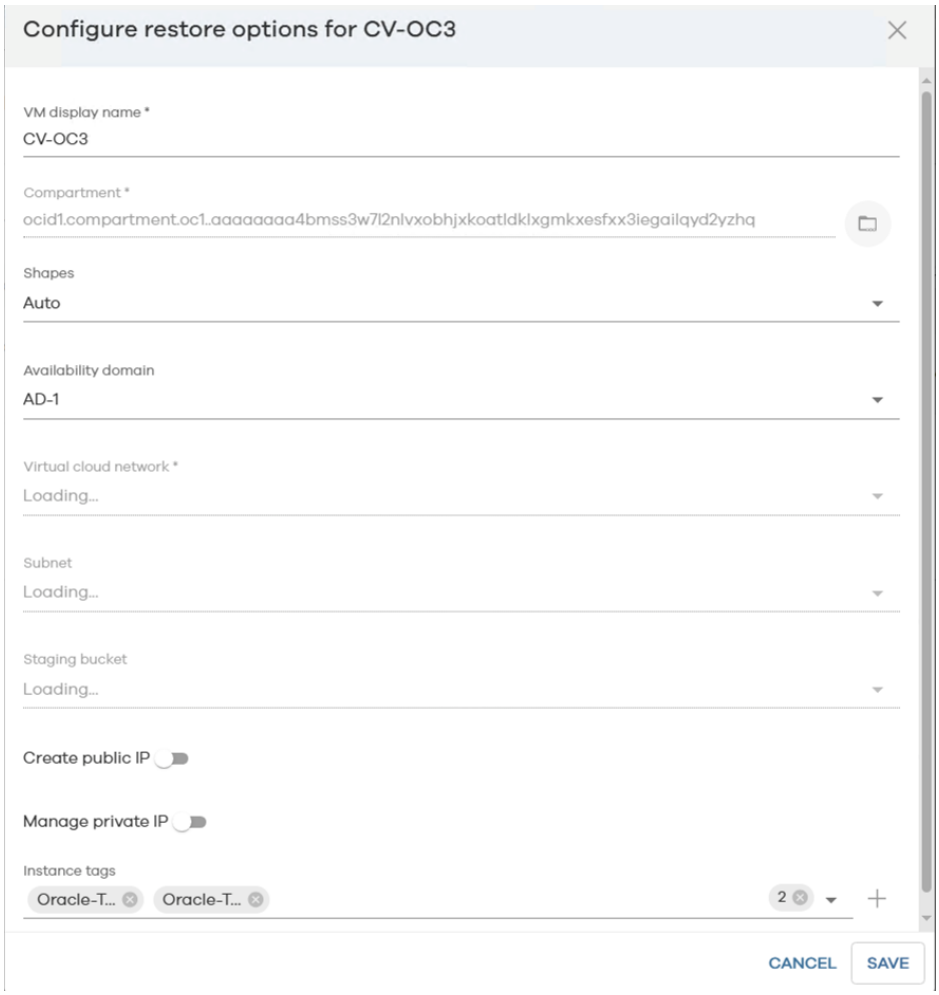


Out-of-Place Restores

1. **Specify the Restore Destination**:
   - For **Type**, select **Out of place** and choose the destination hypervisor.
   - Select **Automatic** or another proxy for the **Access node**.
   - Click **Next**.

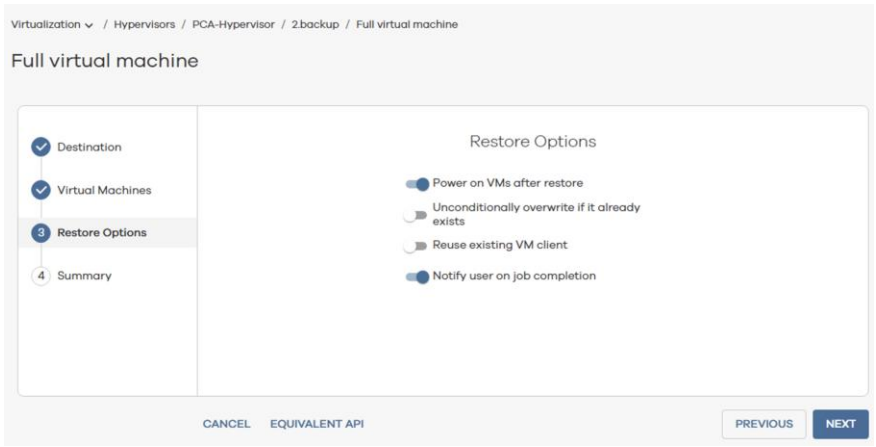


2. **Specify the Virtual Machines and Settings**:
   - Select the virtual machines to restore, and configure options like **Compartment**, **Shapes**, **VNC**, and **Tags**.



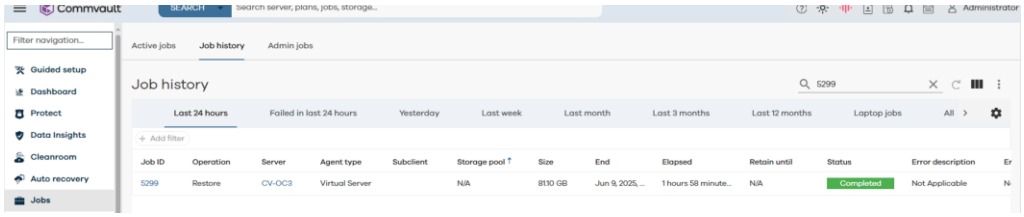
- Click **Next**.

3. **Specify the Restore Options**:
   - **Power on VMs after restore**: Restart VMs after the restore.
   - **Unconditionally overwrite if it already exists**: Overwrite any existing VM.



- Click **Next**.

4. **Review and Start the Restore**:
   - Review settings and click **Submit** to begin the restore.



Note: An **In-Place Restore** will overwrite the existing VM and requires the same name. An **Out-of-Place Restore** without selecting **"Configure restore options"** restores the VM to the same location using default settings, so a new display name is needed to avoid overwriting the original. An **Out-of-Place Restore with "Configure"** lets you choose a different host, storage location, and VM name.

ORACLE

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Author: Sheetal Sabharwal, Oracle **Contributors**: Sean Thompson, Oracle, Commvault team: Nikhil Bhatt, Hema Madala and Sandeep Nashikkar