Best Practices for Deploying Cohesity NetBackup on Compute Cloud@Customer and Private Cloud Appliance

A Step-by-Step Guide to Installing, Configuring, and Deploying Cohesity NetBackup with Snapshot Manager on Compute Cloud@Customer and Private Cloud Appliance

Version [1.0]

Public

Purpose statement

This document outlines best practices for deploying Cohesity NetBackup 11.x along with Cohesity NetBackup Snapshot Manager on Compute Cloud@Customer and Oracle Private Cloud Appliance, providing a step-by-step guide for installing, configuring, and implementing backup and restore functionality on both platforms.

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.

Table of contents

Introduction

As enterprises modernize their data protection strategies, ensuring reliable, secure, and scalable backup and recovery across on-premises and hybrid cloud environments has become increasingly critical. Cohesity NetBackup remains a foundational platform for enterprise-grade data protection, offering comprehensive capabilities for backup, recovery, ransomware resilience, and operational continuity across diverse workloads.

Compute Cloud@Customer (C3) and **Private Cloud Appliance (PCA)** provide customers with a cloud-consistent infrastructure experience deployed within their own data centers, enabling greater control, data sovereignty, and compliance while maintaining operational simplicity. When combined with Cohesity NetBackup, these platforms enable organizations to implement robust data protection architectures that align with enterprise security, performance, and availability requirements.

This solution paper outlines best practices for deploying and configuring Cohesity NetBackup on Compute Cloud@Customer and Private Cloud Appliance, focusing on architecture considerations, operating system alignment, snapshot integration, security configuration, and operational guidance.

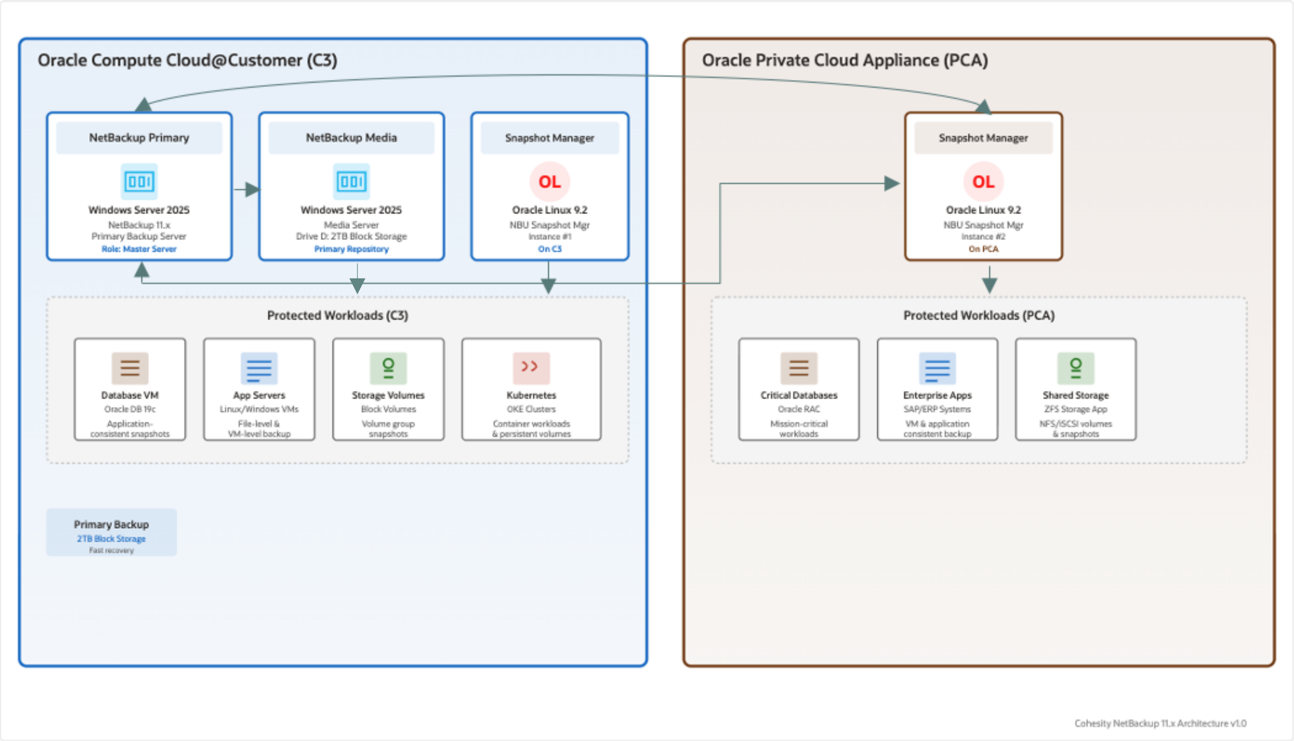
The goal is to help customers achieve a resilient, supportable, and production-ready Cohesity NetBackup deployment that maximizes the capabilities of both platforms while adhering to proven enterprise standards.

Architecture Overview

This architecture presents a comprehensive enterprise backup solution leveraging Cohesity NetBackup 11.x deployed across Oracle's Edge Cloud solutions. The solution provides unified data protection spanning Oracle Compute Cloud@Customer (C3) and Oracle Private Cloud Appliance (PCA), delivering both rapid recovery capabilities and cost-effective long-term data retention.

Cohesity NetBackup 11.x Enterprise Backup Architecture

Cohesity NetBackup on Oracle Compute Cloud@Customer & Private Cloud Appliance



Architecture Components & Data Flows

🟦 **Primary Backup** - Backup to 2TB Block Storage on Media Server

🟩 **Snapshot Operations** - Application-consistent snapshots

🟫 **PCA Infrastructure** - Separate on-premises environment

Key Features

- **Cohesity NetBackup 11.x** - Primary backup server on Windows Server 2025 (C3)
- **Local Storage** - 2TB block storage (D:) on Media Server for fast recovery
- **Dual Snapshot Managers** - Oracle Linux 9.2 instances on both C3 and PCA for distributed snapshot coordination
- **Cross-Infrastructure Protection** - Unified backup management across C3 and PCA environments
- **Application-Aware Backups** - Database, VM, Kubernetes, and storage volume snapshots
- **On-Premises Data Sovereignty** - All backup data remains within customer-controlled infrastructure

Figure 1. Cohesity NetBackup with Oracle Compute Cloud@Customer and Private Cloud Appliance.

Architecture Components

1. Oracle Compute Cloud@Customer (C3) Environment

The C3 infrastructure serves as the primary backup operations center, hosting the core Cohesity NetBackup components:

Cohesity NetBackup Primary Backup Server

- **Platform**: Windows Server 2025
- **Role**: Master Server
- **Function**: Centralized backup management, policy administration, and orchestration of all backup operations across both C3 and PCA environments
- **Capabilities**:
  - Unified management console for multi-site backup operations

  - Policy-based backup scheduling and retention management
  - Integration with OCI Object Storage for cloud tiering
  - Cross-infrastructure snapshot coordination

Cohesity NetBackup Media Server

- **Platform**: Windows Server 2025
- **Storage**: 2TB Block Storage (Drive D:)
- **Role**: Primary Backup Repository (Tier 1)
- **Function**: High-performance backup target for fast data ingestion and rapid recovery operations
- **Benefits**:
  - Low-latency access for backup and restore operations
  - Optimal for meeting aggressive Recovery Time Objectives (RTOs)
  - Local storage for frequently accessed backup data
  - Staging area for data before cloud archival

Cohesity NetBackup Snapshot Manager (C3 Instance)

- **Platform**: Oracle Linux 9.2
- **Function**: Orchestrates VM-consistent snapshots for workloads running on C3

2. Oracle Private Cloud Appliance (PCA) Environment

The PCA infrastructure operates as a separate on-premises environment, hosting mission-critical workloads with their own dedicated snapshot management:

Cohesity NetBackup Snapshot Manager (PCA Instance)

- **Platform**: Oracle Linux 9.2
- **Role**: Cross-Infrastructure Snapshot Coordinator
- **Function**: Orchestrates VM-consistent snapshots for workloads running on PCA

Data Flow Architecture

The architecture implements a tiered backup strategy optimizing for both performance and cost:

1. **Primary Backup Path (Tier 1)**:
   - Cohesity NetBackup agents on protected workloads send backup data to the Media Server
   - Data is written to the 2TB block storage (Drive D:) for fast recovery access
   - Suitable for recent backups requiring rapid restore capabilities
   - Typical retention: 7-30 days
2. **Snapshot Operations**:
   - Snapshot Managers coordinate with Cohesity NetBackup Primary Server
   - Application-consistent snapshots captured at the storage layer
   - Minimal impact on production workloads (crash-consistent)
   - Snapshots cataloged in Cohesity NetBackup for centralized recovery management

Cross-Infrastructure Communication

The architecture leverages Oracle's Compute Cloud@Customer or Private Cloud Appliance network infrastructure for seamless connectivity:

- **Private Network**: Secure communication between C3 and PCA environments

- **API Integration**: RESTful APIs for snapshot management and cloud storage operations
- **Unified Management**: Single Cohesity NetBackup Primary Server orchestrates operations across all environments

Key Architectural Benefits

1. Unified Data Protection

- Single backup solution spanning multiple infrastructure platforms
- Centralized management reduces operational complexity
- Consistent backup policies across hybrid environments
- Unified reporting and compliance auditing

2. Tiered Storage Strategy

- **Tier 1 (Block Storage)**: Fast recovery for recent backups (RPO: minutes to hours)
- Automated data movement based on age and access patterns
- Optimized total cost of ownership (TCO)

3. Application-Consistent Protection

- Snapshot Managers ensure transactional consistency
- Kubernetes-native backup for containerized applications
- Minimizes Recovery Point Objective (RPO) exposure

4. Scalability and Flexibility

- Independent scaling of compute and storage resources
- Add media servers as backup workload grows
- Object storage scales infinitely without capacity planning
- Support for future infrastructure additions (additional C3/PCA sites)

5. Disaster Recovery and Business Continuity

- Multiple recovery points across different storage tiers
- Air-gap protection through cloud isolation
- Supports various disaster recovery scenarios:
    - Site-level failures (entire C3 or PCA outage)
    - Ransomware protection (immutable cloud backups)
    - Long-term data preservation for compliance

6. Operational Efficiency

- Reduced backup windows through snapshot technology
- Minimal impact on production workloads
- Automated backup lifecycle management
- Simplified restore operations through unified catalog

Technical Integration Points

1. **Snapshot Integration**:
    - Cohesity NetBackup Snapshot Manager integrates with Oracle Compute Cloud@Customer and Private Cloud Appliance

   - Supports volume snapshots, volume group snapshots, and boot volume snapshots
   - Coordinates with Oracle Database RMAN for database-aware backups
2. **Network Connectivity**:
   - FastConnect provides dedicated bandwidth for backup traffic
   - Quality of Service (QoS) policies separate backup from production traffic
   - VPN backup for redundant connectivity

Storage Lifecycle Management

Cohesity NetBackup Storage Lifecycle Policies (SLP) automate data movement:

1. **Initial Backup**: Data written to Tier 1 (Block Storage on Media Server)
2. **Tier 1 Expiration**: After 30 days, expire local copy
3. **Long-term Retention**: Maintain cloud copy per retention policy (90 days to 7 years)
4. **Final Expiration**: Automatic deletion based on compliance requirements

Capacity Planning and Sizing

Storage Requirements

Tier 1 (Block Storage - Media Server):

- Capacity: 2TB
- Retention: 7-30 days of recent backups
- Change Rate Consideration: 10-20% daily change rate
- Example Calculation:
  - 500GB of source data
  - 30-day retention
  - 15% daily change rate
  - Required capacity: 500GB + (500GB × 0.15 × 30) = ~2.75TB
  - With deduplication (2:1 ratio): ~1.4TB

Network Bandwidth Requirements

Backup Traffic:

- Initial full backup: Size of protected data ÷ backup window
- Example: 5TB ÷ 8 hours = 625GB/hour = ~1.4 Gbps
- Incremental backups: Daily change rate × workload size
- Example: 5TB × 15% = 750GB ÷ 8 hours = ~210 Mbps

Security Considerations

Data Protection

1. **Encryption**:
   - In-transit: TLS 1.2+ for all network communications
   - At-rest: AES-256 encryption on block storage and object storage
2. **Access Control**:
   - Role-Based Access Control (RBAC) in Cohesity NetBackup
   - Least-privilege principles for backup administrators
   - Multi-factor authentication (MFA) for administrative access
3. **Network Isolation**:
   - Dedicated backup network segments
   - Firewall rules restrict access to backup infrastructure

Compliance and Auditing

1. **Audit Trails**:
   - Cohesity NetBackup maintains comprehensive audit logs
   - All backup, restore, and administrative actions logged
   - Integration with SIEM platforms for security monitoring
2. **Retention Enforcement**:
   - Policy-based retention prevents premature deletion
   - Legal hold capabilities for litigation support
   - Compliance reports for regulatory requirements (GDPR, HIPAA, SOX)
3. **Immutability**:
   - Prevents deletion or modification during retention period
   - Protection against insider threats and ransomware

Operational Best Practices

1. Backup Policy Design

- Implement consistent naming conventions for policies
- Separate policies by application tier (Platinum, Gold, Silver, Bronze)
- Define clear RPO/RTO objectives for each tier
- Document backup schedules and retention requirements

2. Monitoring and Alerting

- Configure Cohesity NetBackup OpsCenter for centralized monitoring
- Set up alerts for backup failures, capacity thresholds, and performance issues
- Establish escalation procedures for critical failures
- Regular review of backup success rates and trends

3. Testing and Validation

- Schedule regular restore tests (monthly minimum)
- Validate disaster recovery procedures quarterly
- Test cross-site recovery capabilities
- Document restore procedures and maintain runbooks

4. Capacity Management

- Monitor Tier 1 storage utilization (alert at 80% capacity)
- Review deduplication ratios and adjust retention as needed
- Forecast growth and plan capacity expansion proactively

5. Change Management

- Test Cohesity NetBackup upgrades in non-production environment
- Coordinate snapshot manager updates with Oracle platform updates
- Maintain change log for backup infrastructure modifications
- Back up Cohesity NetBackup catalog and configuration regularly

Future Expansion Capabilities

This architecture supports future enhancements and expansions:

1. **Additional Sites**:
   - Deploy additional C3 or PCA environments
   - Extend snapshot management to new sites
   - Centralized management from single Primary Server
2. **Advanced Data Management**:
   - Implement Cohesity NetBackup deduplication appliances for greater efficiency
   - Add backup acceleration for large-scale environments
   - Deploy Cohesity NetBackup Auto Image Replication for site-to-site protection

Deployment Considerations and Prerequisites

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

- **Private Cloud Appliance Access:** Ensure you have an active account with the appropriate permissions to create and manage resources on the Compute Cloud@Customer or Private Cloud Appliance.
- **Create a Cohesity NetBackup User and Group on Windows 2025:** Before installing Cohesity NetBackup on Windows 2025, it is recommended to create a **Cohesity NetBackup** user and group on the Windows 2025 server which will be utilized as Cohesity NetBackup Master and Media servers. Refer to Cohesity NetBackup official Installation Guide.
- **Cohesity NetBackup Account:** Obtain the latest compatible **Cohesity NetBackup** platform release from the https://www.veritas.com/support/en_US/downloads using your active **Cohesity NetBackup** account. (Note: This document was created using **Cohesity NetBackup** platform release 11.1. Please consult the **Cohesity NetBackup** 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 2025 VM on Compute Cloud@Customer or Private Cloud Appliance.
- **Network Verification:** Verify network connectivity from the Windows 2025 VM on the Compute Cloud@Customer or Private Cloud Appliance. Ensure DNS resolution and firewall rules allow **Cohesity NetBackup** communication.
- **Firewall Configurations:** Configure firewalls (Windows Firewall, Compute Cloud@Customer or Private Cloud Appliance network firewalls) to allow communication between **Cohesity NetBackup** components. In some cases, firewalls may need to be temporarily disabled or configured to allow the required traffic. . Refer to Cohesity NetBackup official Installation Guide for the specific ports needed to be allowed.
- **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 **Cohesity NetBackup** Command Center.
- **VCN, Subnets, and Security Lists:** Verify that Virtual Cloud Network (VCN), subnet, and security list configurations permit necessary connections for **Cohesity NetBackup** communication.
- **Clock Synchronization:** Ensure all Cohesity NetBackup instances part of the architecture running on Compute Cloud@Customer or Private Cloud Appliance are synchronized to a reliable NTP server to avoid time-related authentication and communication issues.
- **Users and Groups Configuration on Compute Cloud@Customer and Private Cloud Appliance.** For securing the **Cohesity NetBackup** environment on Compute Cloud@Customer and Private Cloud Appliance, it is essential to create dedicated users and groups with appropriate access controls, adhering to the principle of least privilege. This approach limits unnecessary access, enhances security, and simplifies permission management for both on-premises and cloud-integrated resources. Follow the steps below to configure the Identity and Access Management (IAM) settings for Cohesity NetBackup in your Compute Cloud@Customer or Private Cloud Appliance environments:
  - **Create Cohesity NetBackup User and Group**

- **Create User:**
    - Navigate to **Identity** > **Users** in the PCA management console.
    - Click **Create User**, provide a **name**, **description**, and **email address**, and click **Create** to add the user.
- **Create Group:**
    - Navigate to **Identity** > **Groups** and click **Create Group**.
    - Provide a **name** and **description** for the group and click **Create** to create the group.
- **Add User to Group:**
    - After creating the group, click on group name, and under **Group Members**, click **Add User to Group**.
    - Select the user created earlier from the drop-down list and add them to the group

- **Assign API Keys**
    - In the Compute Cloud@Customer or Private Cloud Appliance management consoles, click on the **User**name.
    - Under **Resources**, select **API Keys** and upload the **public key file**.
- **Define IAM Policies:** To ensure that the Cohesity NetBackup user and group have the necessary permissions for managing resources within Compute Cloud@Customer or Private Cloud Appliance, you need to configure specific IAM policies both at the tenancy and compartment levels. On create a new dynamic group with the following rules.

1. Open the **navigation menu** and select **Identity & Security**. Under **Identity**, select **Domains**. Under **Identity domain**, select **Dynamic groups**. Refer to create a dynamic group
2. Select **Create Dynamic Group**.
3. Enter the following:
    - **Name:** A unique name for the group. The name must be unique across all groups in your tenancy (dynamic groups and user groups). You can't change this later. Avoid entering confidential information.
    - **Description:** A friendly description.
4. Enter the **Matching Rules**. Resources that meet the rule criteria are members of the group.
    - **Rule 1:** Enter a rule following the guidelines in Writing Matching Rules to Define Dynamic Groups. You can manually enter the rule in the text box or launch the rule builder.
    - Enter additional rules as needed. To add a rule, select **+Additional Rule**.
5. If you have permissions to create a resource, then you also have permissions to apply *free-form* tags to that resource. To apply a *defined* tag, you must have permissions to use the tag *namespace*. For more information about tagging, see Resource Tags. If you're not sure whether to apply tags, skip this option or ask an administrator. You can apply tags later.
6. Select **Create Dynamic Group**.

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

- allow group <group-name> to inspect compartments in tenancy
- allow group <group-name> to inspect 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'}

Cohesity NetBackup Installation and Configuration

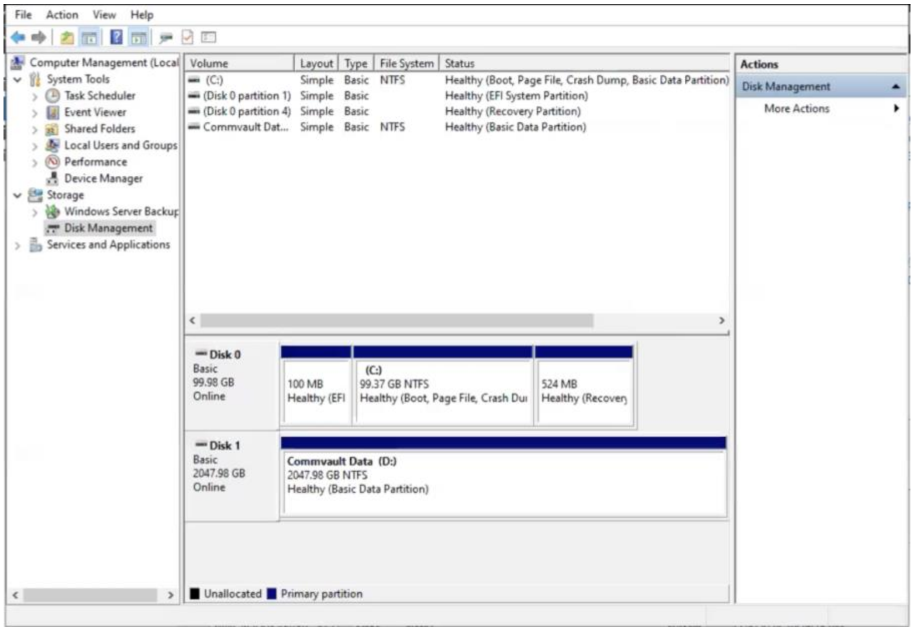
Cohesity NetBackup Primary and Media servers based on Windows Platform

The following steps outline the process for installing and configuring **Cohesity NetBackup Primary and Media servers** on a Windows 2025 VM on the Compute Cloud@Customer or Private Cloud Appliance.

On Windows VMs, **Cohesity NetBackup** Primary installation can be downloaded and licensed from the Download Center - https://www.veritas.com/support/en_US/downloads

- **Provision Windows 2025 VM on Compute Cloud@Customer or Private Cloud Appliance.** In our architecture, we are working with a Cohesity NetBackup Master and Media servers on the Compute Cloud@Customer, however, the same can be deployed on Private Cloud Appliance. For detailed instructions on creating a new instance on Private Cloud Appliance or Compute Cloud@Customer, refer to the official documentation: Compute Instances Deployment.
- **Create and Attach a Block Volume:** Create and attach a block volume to the Windows 2025 instance. This volume will be used for **Cohesity NetBackup** data storage. To create and attach a block volume, consult the Private Cloud Appliance or Compute Cloud@Customer documentation. Documentation for instructions: Learn how to create and attach a block volume
- **Access the Windows Instance:** Connect to the Windows Server 2025 instance using a Windows App (formerly known as Windows Remote Desktop Client).
- **Initialize and Format the Block Volume**
    - After connecting to the Windows 2025 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.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Basic Data Partition)
(Disk 0 partition 1)	Simple	Basic		Healthy (EFI System Partition)
(Disk 0 partition 4)	Simple	Basic		Healthy (Recovery Partition)
Commvault Dat...	Simple	Basic	NTFS	Healthy (Basic Data Partition)

Disk 0 Basic 99.98 GB Online	100 MB Healthy (EFI	(C:) 99.37 GB NTFS Healthy (Boot, Page File, Crash Du	524 MB Healthy (Recoven
Disk 1 Basic 2047.98 GB Online	**Commvault Data (D:)** 2047.98 GB NTFS Healthy (Basic Data Partition)		

Figure 2. Windows 2025 Disk Management for Cohesity NetBackup backup storage.

- Install Cohesity NetBackup Primary Server Software on Windows 2025. Refer to [Cohesity NetBackup official Installation Guide](#).

Cohesity NetBackup Snapshot Manager Servers based on Oracle Linux 9.x Platform

- **Provision Oracle Linux 9.x VM instances on Compute Cloud@Customer and Private Cloud Appliance.** In our architecture we are working with Compute Cloud@Customer and Private Cloud Appliance, so we need to deploy two instances running Cohesity NetBackup Snapshot manager, one in the Compute Cloud@Customer and other on Private Cloud Appliance. This will ensure protection of instances running in both platforms. For detailed instructions on creating a new instance on Private Cloud Appliance or Compute Cloud@Customer, refer to the official documentation: [Compute Instances Deployment.](#)
- Install Cohesity NetBackup Snapshot Manager Server Software on Oracle Linux 9.2 instances running on Compute Cloud@Customer or Private Cloud Appliance following the steps listed below:

NOTE: Refer to the official Cohesity NetBackup snapshot manager prerequisite: https://www.veritas.com/content/support/en_US/doc/140789355-170163285-0/v140791746-170163285

- Update the Oracle Linux 9.x instance and install the following packages:

```
dnf update -y
dnf install -y lvm2-<version>
dnf install -y systemd-udev-<version>
dnf install -y podman-plugins
dnf install -y udica policycoreutils-devel
```

- Un-tar the image file using the following command:

```
tar -xvf NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
```

- Enable and start the podman-restart service

```
sudo systemctl enable --now podman-restart.service
```

- Verify it's enabled and running

```
sudo systemctl status podman-restart.service
```

- Also verify podman.socket is still running

```
sudo systemctl status podman.socket
```

- Create /cloudpoint directory with correct permissions:

```
sudo mkdir -p /cloudpoint
sudo chmod 755 /cloudpoint
```

- Set proper SELinux context (if SELinux is enforcing)

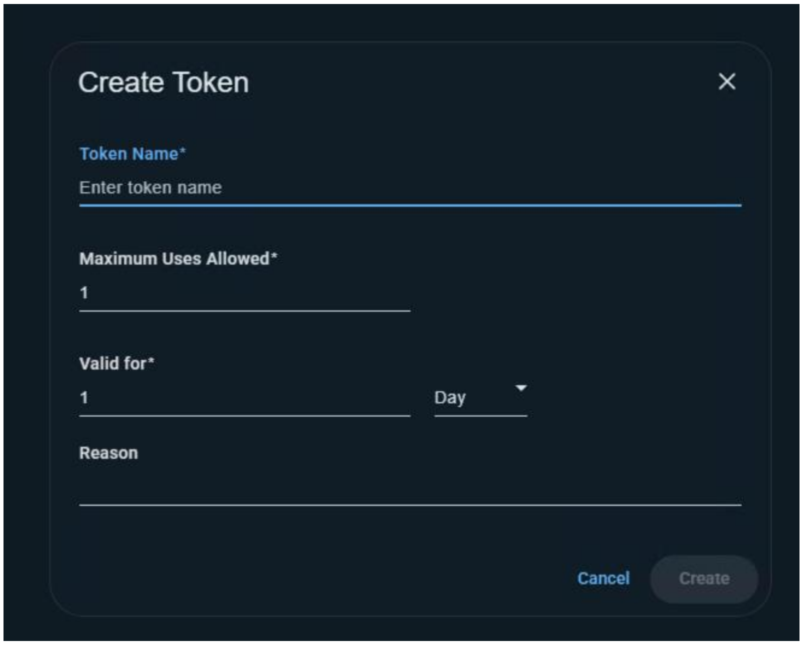
```
sudo semanage fcontext -a -t container_file_t "/cloudpoint(/.*)?"
sudo restorecon -Rv /cloudpoint
```

- Run the **Cohesity NetBackup Snapshot Manager preinstallation checks** to verify that all required configurations are in place before proceeding with the Snapshot Manager installation.
  Note: Ensure that **all validation checks complete successfully** before continuing.

```
./flexsnap_preinstall.sh
Checking for disk space                  ...  done
Checking for swap space                  ...  done
Checking for host networking             ...  done
Validate host resources                  ...  done
Validate SELINUX                         ...  done
Validating the required permissions for /cloudpoint directory ...  done
Check for podman installation            ...  done
Validate podman version support          ...  done
Check for podman socket file             ...  done
Checking for required packages           ...  done
Validate required services health        ...  done
Loading Snapshot Manager service images  ...  done
Copying flexsnap_configure script        ...  done
```

- Go to Cohesity NetBackup management interface, click security, then token. Create a new token to be utilized by the Snapshot Manager server.
  - click the "+ Add" button to create a new token:
  - Click "+ Add" button
  - Give it a name (e.g., "snapshot_manager_token")
  - Set the validity period (e.g., 24 hours or longer)
  - Select the appropriate permissions/scope (usually "Full" or "Administrator" for Snapshot Manager installation)

- Click Create or Save
- Copy the token that's generated (you'll only see it once!). This Token will be utilized on the next step of the installation.



Create Token

Token Name*
Enter token name

Maximum Uses Allowed*
1

Valid for*
1
Day

Reason

Figure 3. Cohesity NetBackup management UI Token Configuration.

- Copy the Compute Cloud@Customer or Private Cloud Appliance certificate. In your web browser past the IaaS FQDN of your Compute Cloud@Customer or Private Cloud Appliance. Example: https://iaas.the0FQDN-of-your-C3-or-PCA/cachain then copy the content to the following file in your Cohesity NetBackup Snapshot Manager:

  `cloudpoint/eca/trusted/cacerts.pem`

- Run the flexsnap_configure install command below to install Cohesity NetBackup Snapshot Manager on Oracle Linux 9.x. NOTE: The installation will ask for information such as, name of the Cohesity NetBackup primary server, IP address or FQDN, the Token previously created.

```
/usr/sbin/flexsnap_configure install -i \
  --add-host <Add the FQDN or Name of your NetBakup Server:IP address of you Cohesity NetBackup Server>
```

Example:

```
/usr/sbin/flexsnap_configure install -i \
  --add-host Cohesity NetBackup01.your.domain:X.X.X.X

Provide Cohesity NetBackup Primary details: Name of the Cohesity NetBackup primary server
Cohesity NetBackup primary server IP Address or FQDN: IP Address or FQDN of your Primary
Cohesity NetBackup Server
Start configuring with Cohesity NetBackup CA certificate.
Provide Cohesity NetBackup authentication token: Paste the token created on the previous step.
Cohesity NetBackup Snapshot Manager hostname for TLS certificate (64 char FQDN limit): Enter the
name of your Cohesity NetBackup Snapshot Manager Server
Port (default:443): Hit Enter
Configuration started at time: Tue Jan  6 00:09:52 UTC 2026
Podman server version: 5.6.0
This is a fresh install of Cohesity NetBackup Snapshot Manager 11.1.0.0-1049
Cleaning up stale Cohesity NetBackup Snapshot Manager assets if any
Container removal started at time: Tue Jan  6 00:09:52 UTC 2026
Container removal completed at time: Tue Jan  6 00:09:52 UTC 2026
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Waiting for Snapshot Manager configuration to complete (21/21) ...done
Configuration complete at time Tue Jan  6 00:14:48 UTC 2026!
Please register Snapshot Manager with Cohesity NetBackup primary server
```

- Check that all containers are running, all containers need to be running and healthy as listed below:

```
podman ps
```

```
CONTAINER ID  IMAGE                                                COMMAND               CREATED        STATUS
PORTS                                         NAMES
37156efae8a2  localhost/veritas/flexsnap-fluentd:11.1.0.0-1049                           9 minutes ago  Up 9
minutes            0.0.0.0:24224->24224/tcp                      flexsnap-fluentd
51e7303e7c2e  localhost/veritas/flexsnap-postgresql:11.1.0.0-1049                        9 minutes ago  Up 7
minutes (healthy)  13787/tcp                                     flexsnap-postgresql
8d9196f41d0e  localhost/veritas/flexsnap-rabbitmq:11.1.0.0-1049                          9 minutes ago  Up 9
minutes (healthy)  5671/tcp                                      flexsnap-rabbitmq
7972842bfb32  localhost/veritas/flexsnap-core:11.1.0.0-1049                              9 minutes ago  Up 8
minutes (healthy)  9000/tcp                                      flexsnap-certauth
0f627275e1d2  localhost/veritas/flexsnap-core:11.1.0.0-1049                              9 minutes ago  Up 6
minutes (healthy)  8472/tcp                                      flexsnap-api-gateway
9292fe5a454e  localhost/veritas/flexsnap-core:11.1.0.0-1049                              9 minutes ago  Up 4
minutes (healthy)                                                flexsnap-coordinator
9b38123fc5ac  localhost/veritas/flexsnap-core:11.1.0.0-1049                              9 minutes ago  Up 4
minutes (healthy)                                                flexsnap-listener
1f8b0e2d73cf  localhost/veritas/flexsnap-core:11.1.0.0-1049                              9 minutes ago  Up 4
minutes (healthy)                                                flexsnap-agent
653568fc7c87  localhost/veritas/flexsnap-core:11.1.0.0-1049        --config /etc/fle...  9 minutes ago  Up 4
minutes (healthy)                                                flexsnap-onhostagent
695adffbeab3  localhost/veritas/flexsnap-core:11.1.0.0-1049                              9 minutes ago  Up 4
minutes (healthy)                                                flexsnap-scheduler
1716b5b8e769  localhost/veritas/flexsnap-core:11.1.0.0-1049                              9 minutes ago  Up 4
minutes (healthy)                                                flexsnap-policy
311132118c74  localhost/veritas/flexsnap-core:11.1.0.0-1049                              9 minutes ago  Up 4
minutes (healthy)                                                flexsnap-notification
e62fc1207b13  localhost/veritas/flexsnap-nginx:11.1.0.0-1049                             9 minutes ago  Up 6
minutes (healthy)  0.0.0.0:443->443/tcp, 0.0.0.0:5671->5671/tcp  flexsnap-nginx
d137b8bc9747  localhost/veritas/flexsnap-core:11.1.0.0-1049        general               4 minutes ago  Up 4
minutes                                                          flexsnap-workflow-general-0-min
8043fbafdd10  localhost/veritas/flexsnap-core:11.1.0.0-1049        system                4 minutes ago  Up 4
minutes                                                          flexsnap-workflow-system-0-min
```

- Ensure you've added the firewall rules on the Snapshot Manager servers.

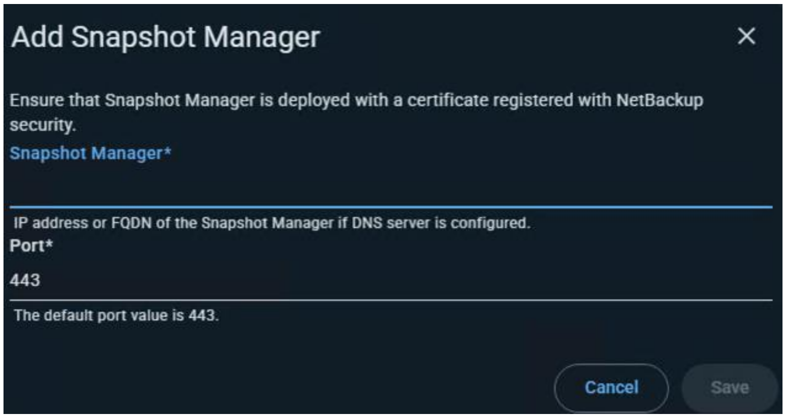
```
sudo firewall-cmd --permanent --add-port=13724/tcp
sudo firewall-cmd --permanent --add-port=13782/tcp
sudo firewall-cmd --permanent --add-port=13783/tcp
sudo firewall-cmd --permanent --add-port=1556/tcp
sudo firewall-cmd --permanent --add-port=443/tcp
sudo firewall-cmd –reload
```

- Check the Snapshot Manager status

```
/usr/sbin/flexsnap_configure status
{ "healthy": "true", "start_time": "Tue, 06 Jan 2026 19:54:08 UTC", "uptime": "25:14:26.589241",
"status": ""OK"", "unhealthy_services": "[]", "host": "localhost" }
```

The installation completed successfully! Now you need to register the Snapshot Manager with your Cohesity NetBackup primary server. Here's what to do:

- On Cohesity NetBackup Web UI management interface, perform the following configuration:
    - Log into Cohesity NetBackup web UI: https://Cohesity NetBackup01/webui
    - Go to Cloud → Snapshot Managers
    - Click Add
    - Add your Cohesity NetBackup Snapshot server FQDN or IP Address
    - Use the default port 443
    - Click Save.



Add Snapshot Manager

Ensure that Snapshot Manager is deployed with a certificate registered with NetBackup security.

Snapshot Manager*

IP address or FQDN of the Snapshot Manager if DNS server is configured.

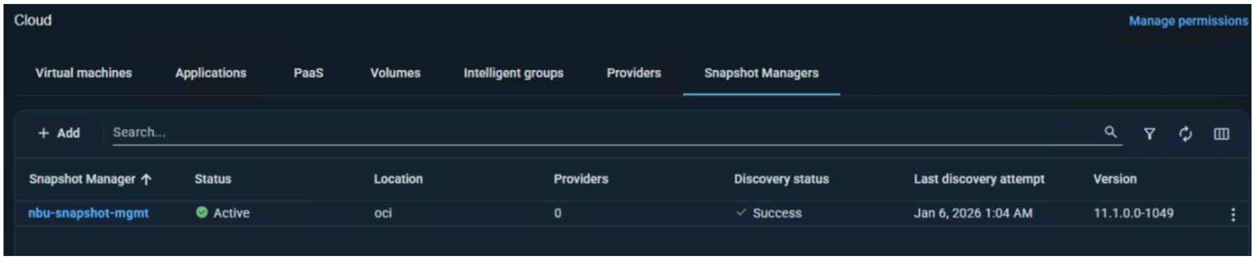
Port*

443

The default port value is 443.

Figure 4. Cohesity NetBackup management UI Snapshot Manager Servers Configuration.

After few seconds your new Cohesity NetBackup Snapshot Manager server will be available on the UI:



Snapshot Manager ↑	Status	Location	Providers	Discovery status	Last discovery attempt	Version
nbu-snapshot-mgmt	● Active	oci	0	✓ Success	Jan 6, 2026 1:04 AM	11.1.0.0-1049

Figure 5. Cohesity NetBackup management UI – List of Snapshot Manager Servers.

- Now you need to configure cloud providers OCI for Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA), so Cohesity NetBackup can discover and protect the virtual instances. On Cohesity NetBackup Web UI management interface, perform the following configuration:
  - Add OCI Provider - Click on Providers tab
  - Configure OCI credentials for Compute Cloud@Customer or Private Cloud Appliance access
  - Discover assets - VMs, volumes, databases on C3/PCA
  - Create protection policies - Define backup schedules and retention

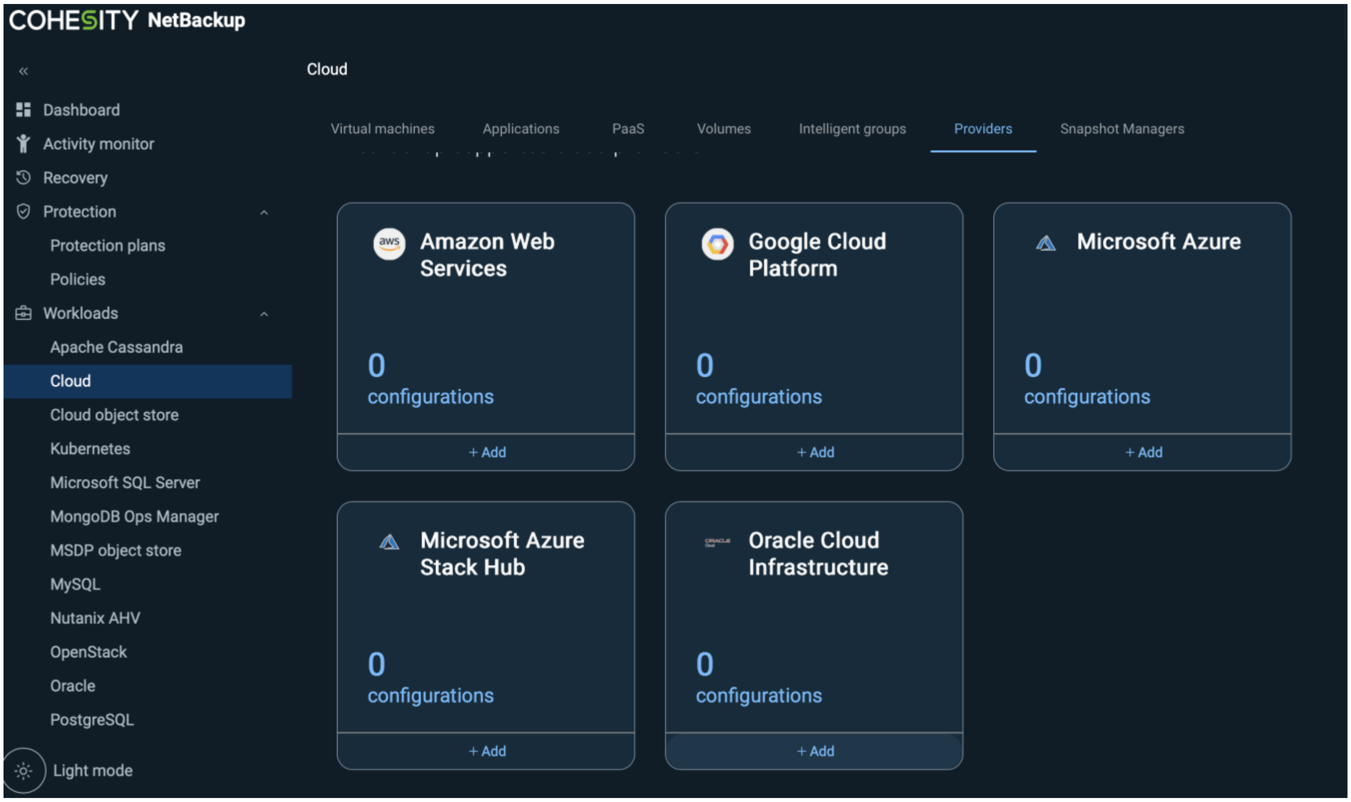
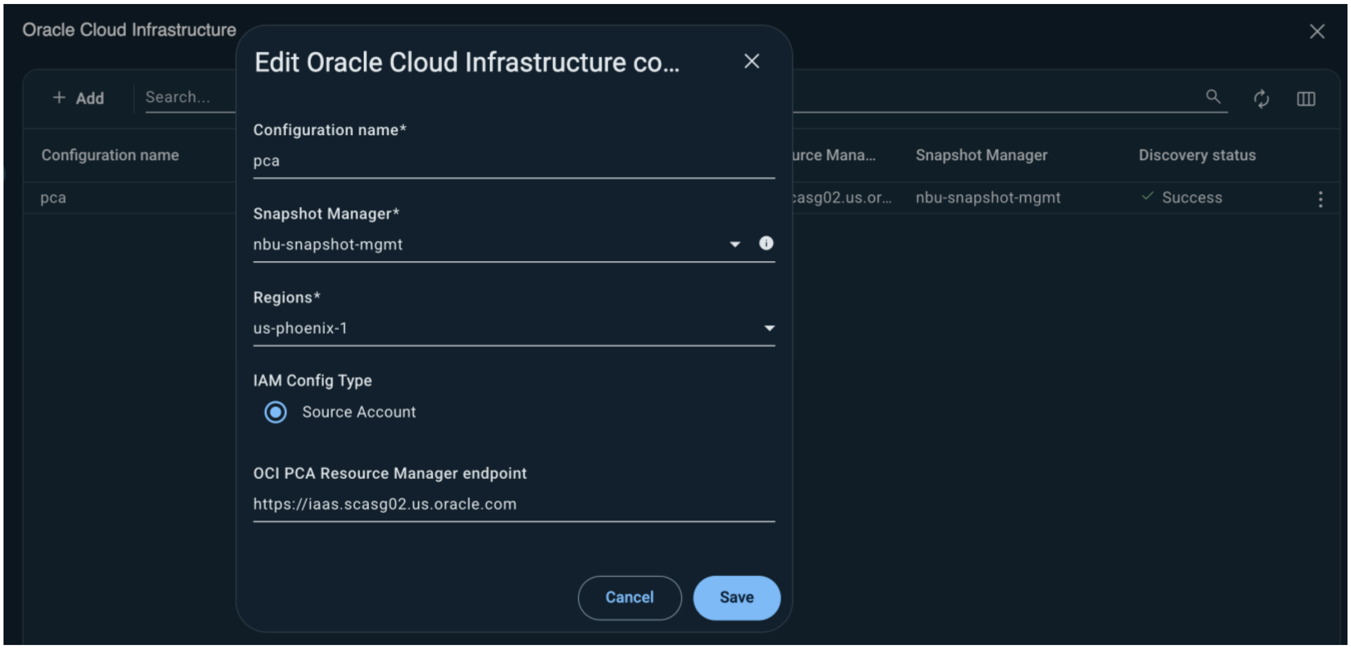


Figure 6. Cohesity NetBackup management UI OCI Provider Configuration.

- On Oracle Cloud Infrastructure click **Add.**
- Enter a name for the confirmation, on this example we are using **pca**.
- Enter the **Cohesity NetBackup Snapshot Manager** server, on this example, we are working with the **nbu-snasphost-mgmt.**
- **Region.** Enter the region nearby.
  - **NOTE**: The region on this screen will be override by Cohesity NetBackup process during the communication with Private Cloud Appliance or Compute Cloud@Customer. Since it is a mandatory field, on the example below we are using us-phoenix-1 as example.

  - Select IAM Config Type – Source Account
  - On the OCI Resource Manager endpoint, enter the IaaS FQDN of your Compute Cloud@Customer or Private Cloud Appliance.
  - Click Save, then the Compute Cloud@Customer or Private Cloud Appliance will be available and listed under Oracle Cloud Infrastructure. After few seconds, all virtual instances on Compute Cloud@Customer or

Private Cloud Appliance will be listed under **Cloud** Tab and available to be protected and added to backup policies. See the screenshots below:



Edit Oracle Cloud Infrastructure co...

Configuration name*
pca

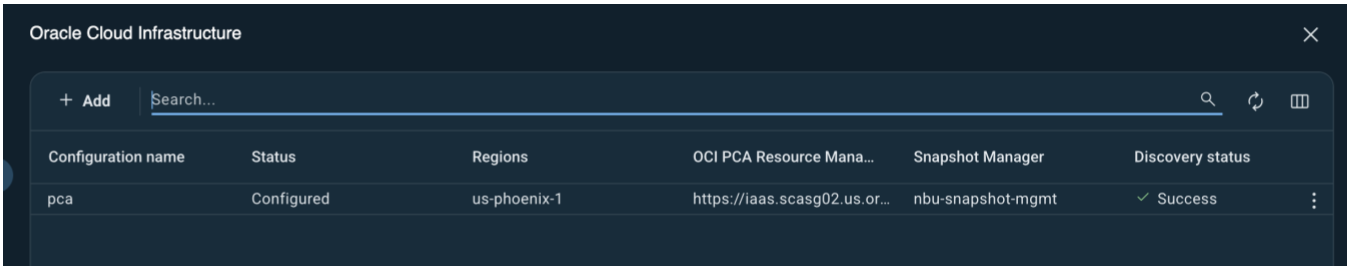
Snapshot Manager*
nbu-snapshot-mgmt

Regions*
us-phoenix-1

IAM Config Type
● Source Account

OCI PCA Resource Manager endpoint
https://iaas.scasg02.us.oracle.com

Figure 7. Cohesity NetBackup management UI - Compute Cloud@Customer or Private Cloud Appliance credentials configuration.



Configuration name	Status	Regions	OCI PCA Resource Mana...	Snapshot Manager	Discovery status
pca	Configured	us-phoenix-1	https://iaas.scasg02.us.or...	nbu-snapshot-mgmt	✓ Success

Figure 8. Cohesity NetBackup management UI – List of Compute Cloud@Customer or Private Cloud Appliance configured.

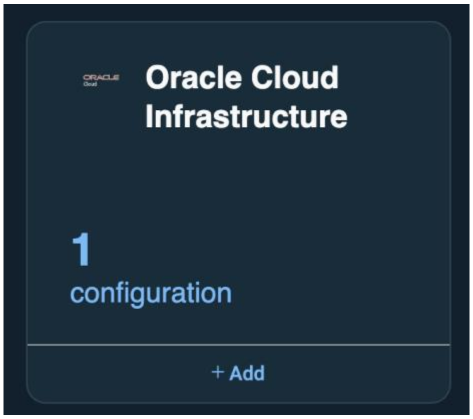
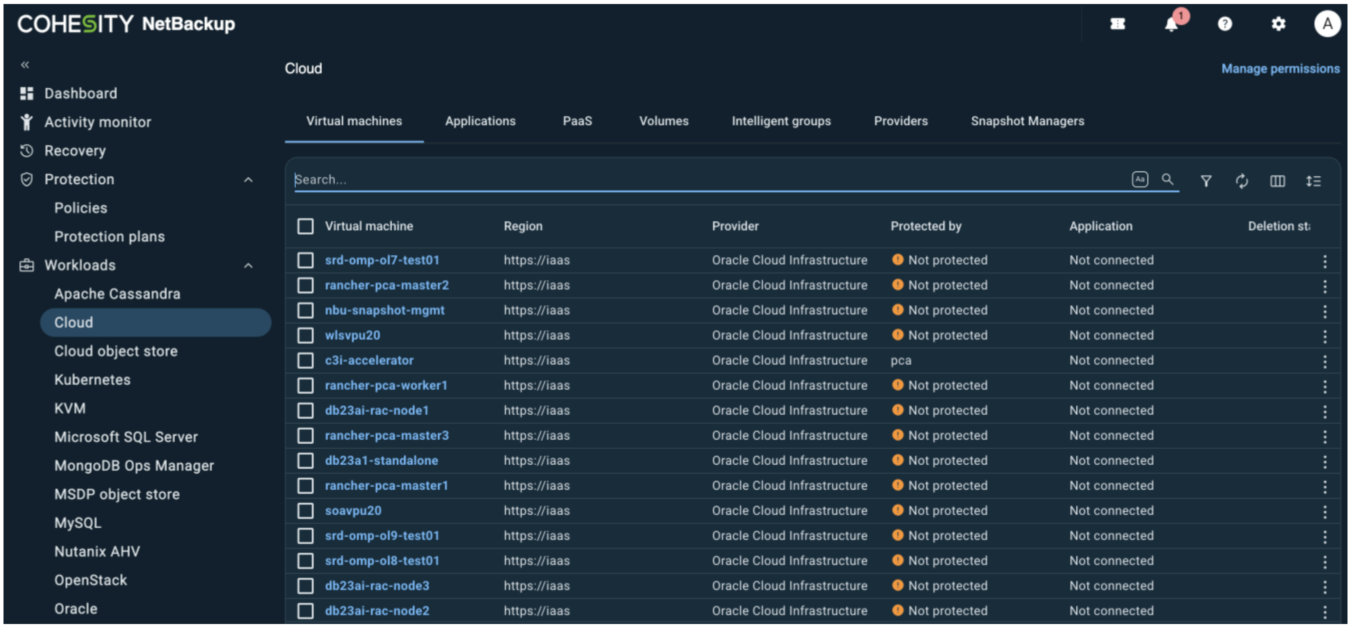


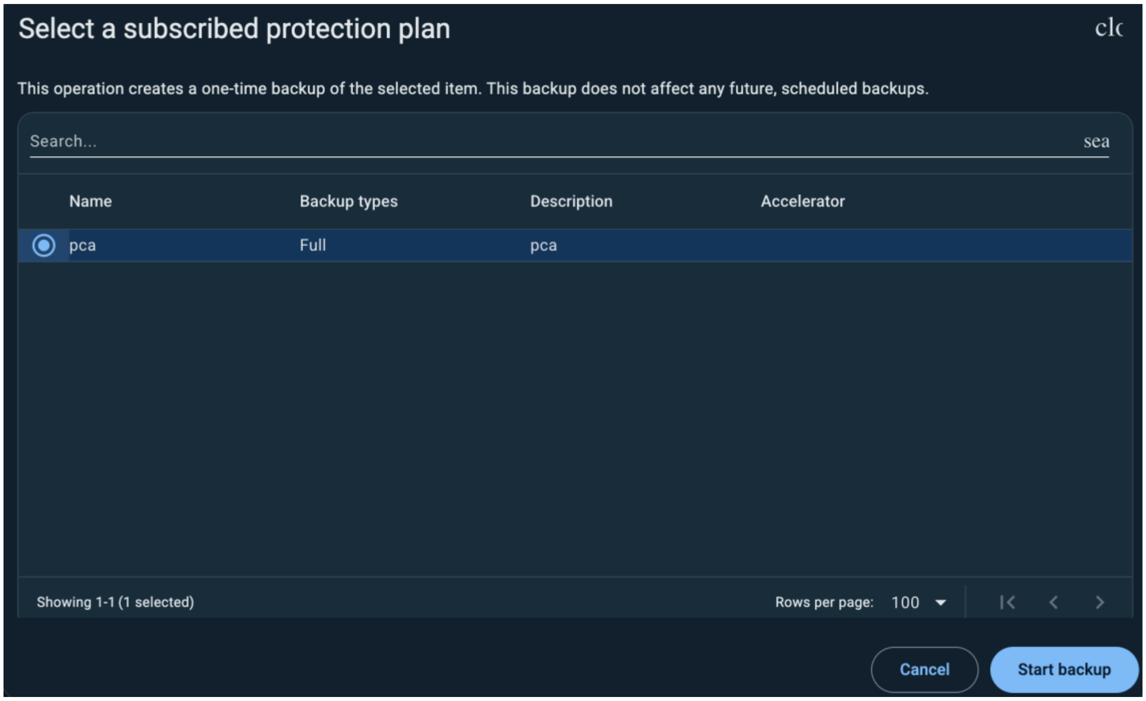
Figure 9. Cohesity NetBackup management UI - Compute Cloud@Customer or Private Cloud Appliance configured under Oracle Cloud Infrastructure (OCI) provider.



Virtual machine	Region	Provider	Protected by	Application	Deletion st
srd-omp-ol7-test01	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
rancher-pca-master2	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
nbu-snapshot-mgmt	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
wlsvpu20	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
c3i-accelerator	https://iaas	Oracle Cloud Infrastructure	pca	Not connected	
rancher-pca-worker1	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
db23ai-rac-node1	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
rancher-pca-master3	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
db23a1-standalone	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
rancher-pca-master1	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
soavpu20	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
srd-omp-ol9-test01	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
srd-omp-ol8-test01	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
db23ai-rac-node3	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	
db23ai-rac-node2	https://iaas	Oracle Cloud Infrastructure	Not protected	Not connected	

Figure 10. Cohesity NetBackup management UI – List of Windows and Linux instances from Compute Cloud@Customer or Private Cloud Appliance ready to be protected.

Backing up an instance via Snapshot Manager:



Select a subscribed protection plan

This operation creates a one-time backup of the selected item. This backup does not affect any future, scheduled backups.

	Name	Backup types	Description	Accelerator
●	pca	Full	pca	

Showing 1-1 (1 selected)

Rows per page: 100

Figure 11. Cohesity NetBackup management UI – Protection Plan.

Final Configuration Steps

As a final step, configure the local storage repository by assigning the previously provisioned Unit D (2 TB) on the Windows Server 2025 Cohesity NetBackup Primary Server as the primary backup storage target for the Cohesity NetBackup infrastructure. Once storage configuration is complete, proceed with defining and enabling the required backup policies.

For detailed instructions, refer to the official Cohesity NetBackup documentation:

- Configuring storage
- Configuring Backup Policies

Backup and Restore Overview

The backup and restore workflow ensure comprehensive data protection by enabling primary backups to local storage. This architecture enables key enterprise use cases, including disaster recovery, workload mobility, and regulatory compliance.

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: Anderson Souza