# Reference Architecture for HPE VM essentials based HPE Private Cloud PC3000 Data Protection with Commvault

# Contents


Executive summary ..... 4
Target audience ..... 5
Solution overview ..... 5
Solution portfolio ..... 6
Secondary and Archive Storage ..... 7
Network Switches ..... 8
Design principles, assumptions and constrains ..... 8
Solution scope (in scope / out of scope) ..... 8
Data protection strategy ..... 9
Adherence to 3:2:1 backup strategy ..... 9
Comprehensive protection of data and configuration ..... 10
Backup recovery objectives (RPO / RTO) ..... 11
Compatibility (firmware and software versions) * ..... 11
Integrated solution architecture ..... 12
Logical architecture – HPE Infrastructure ..... 12
Connectivity and design decisions ..... 14
Integration of HPE Private Cloud PC3000 with Commvault ..... 14
Layer 2 (L2) network Integration ..... 14
Layer 3 (L3) network integration ..... 15
Commvault in the HPE Private Cloud PC3000 rack ..... 16
HPE StoreOnce vs HPE Alletra Storage MP X10000 with data protection accelerator nodes ..... 17
Deployment and configuration guidance ..... 18
HPE Private Cloud PC3000 (HPE Morpheus Software-VM essentials) ..... 18
Compute ..... 18
Network ..... 18
Storage ..... 19
Deployment and automation guidance ..... 19
Commvault components ..... 19
CommServe ..... 19
MediaAgents ..... 20
Deploying Commvault Access node packages on PC3000 system ..... 20
HPE StoreOnce ..... 21
HPE Alletra Storage MP X10000 with data protection accelerator node ..... 21

Commvault Grid ..... 22
Hardware architecture and Bill of Materials ..... 22
HPE Private Cloud PC3000 ..... 22
Compute tier (HPE ProLiant DL for Commvault CommServe and MediaAgent) ..... 22
Backup target tier ..... 23
Primary backup HPE StoreOnce ..... 23
Primary backup HPE Alletra Storage MP X10000 ..... 23
Commvault Grid ..... 23
Security and governance ..... 24
Security design scenarios ..... 24
On-site backups requiring maximum deduplication efficiency ..... 24
Off-site backups requiring high security during transit ..... 25
Security features of HPE Private Cloud PC3000 and backup infrastructure ..... 25
HPE Private Cloud PC3000 ..... 25
Commvault ..... 26
HPE StoreOnce ..... 28
HPE Alletra X10000 with Data Protection Accelerator Nodes ..... 29
Operations and monitoring ..... 29
Scalability ..... 29
Scalability of HPE Private Cloud PC3000 ..... 29
Scalability of Commvault components ..... 30
Scalability of backup storage tier ..... 30
Monitoring ..... 30
HPE Private Cloud PC3000 ..... 30
Monitoring using HPE OpsRamp ..... 31
Support and maintenance ..... 31
Lifecycle management (firmware and software) ..... 31
HPE Private Cloud PC3000 ..... 31
Commvault Software ..... 32
Storage platforms ..... 32
Limitations and known issues ..... 32
Summary ..... 32
Resources and additional links ..... 34

# Executive summary

Organizations build private clouds to obtain cloud agility and automation while retaining control over security, compliance, performance, data location, and infrastructure operations. Private cloud built on proprietary hardware require data protection since resiliency built through virtualization and infrastructure do not eliminate the risk of data loss. While a private cloud can provide high availability for compute, storage, and networking resources, it does not inherently protect against accidental deletion, ransomware, data corruption, application failures, malicious actions, or site-level disasters. In such scenarios, data protection solutions provide independent backup, recovery, and retention capabilities that enable organizations to meet business continuity, compliance requirements.

HPE Private Cloud PC3000 (formerly known as Private Cloud Business Edition, or PCBE) is an integrated private cloud solution from Hewlett Packard Enterprise designed to deliver a cloud-like operating model on premises. PC3000 is a self-managed virtualization platform built with modern hyperconverged infrastructure and HPE Morpheus Software - VM essentials, providing an alternative virtualization solution that is compatible with VMware. The solution is available in a OPEX model with HPE Alletra Storage MP B10000, or in an as-a-service model with HPE GreenLake Flex.

This reference architecture describes a data protection solution for **HPE Private Cloud PC3000** built with **Commvault® software** as part of the **Commvault Data Platform**. Commvault CommServe and Command Center as the central data protection platform that orchestrates backup, recovery, replication, and retention policies across virtual, physical, cloud, and application workloads. In this solution, Commvault integrates with **HPE Morpheus Software - VM essentials** cluster to protect virtualized workloads running on **PC3000** built with **HPE ProLiant DL Compute** and **HPE Alletra Storage MP B10000** iSCSI storage for modern workloads. Backup and recovery data is stored on **HPE StoreOnce** and **HPE Alletra Storage MP X10000**, while **HPE Storage Tape** and **HPE Cloud Bank** provide archival and long-term retention tiers. The combined solution delivers a scalable, cyber-resilient data protection framework that supports efficient backup, rapid recovery, immutable storage, and long-term data retention requirements.

Commvault CommServe provides the centralized control plane that governs job orchestration, policy enforcement, configuration, and metadata handling, while other Commvault core components including MediaAgents, and Access nodes -execute high-performance data movement, compression, encryption, and deduplication. The proposed architecture adopts a foundational **tiered data protection model** aligned with enterprise best practices and the **3-2-1 rule** with:

— Production data residing on HPE Alletra Storage MP B10000

— Primary backup copy residing on HPE StoreOnce or HPE Alletra Storage MP X10000 with data protection accelerator node located on-site optimized for fast backup ingestion and rapid operational recovery through performance-tier repositories

— Secondary backup copy residing on HPE Storage Tape or HPE Cloud Bank located off-site designed for scalable retention using cloud object storage.

By integrating Commvault CommServe with HPE Private Cloud PC3000-powered by enterprise-grade compute, storage, and networking-this reference architecture establishes a highly resilient and scalable data protection foundation. It empowers organizations to adapt to evolving business demands, strengthen cyber resilience, and deliver predictable, policy-driven recovery outcomes aligned with enterprise SLAs, while consistently meeting defined RPO and RTO targets.

## Target audience

This document is intended for stakeholders involved in designing, implementing, and operating data protection solution for HPE Private Cloud PC3000. HPE partners and system integrators can use this reference architecture as a standardized blueprint for delivering consistent, validated solutions across customer environments. It provides clear guidance on infrastructure design, integration patterns, and deployment approaches, enabling repeatable and scalable implementations.

Enterprise customers and IT decision-makers can use this document to align their data protection strategy with modern infrastructure capabilities. It supports informed decision-making across key areas such as architecture, scalability, connectivity, resilience, and security helping balance performance, cost, and risk.

Pre-sales engineers and solution architects will benefit from structured design guidance, decision frameworks, and reference configurations that simplify the translation of business requirements into technical solutions.

# Solution overview

This reference architecture presents a complete on-premises data protection solution built with **Commvault CommServe** integrated with HPE Private Cloud PC3000. PC3000 is built on HPE ProLiant DL servers, and uses HPE Morpheus Software - VM essentials for virtualization, with HPE Alletra Storage MP B10000 as the primary iSCSI storage for production applications.

In this architecture, the Commvault is deployed externally to the PC3000 rack using a distributed and scale-out(Commvault Grid) architecture, where it functions as the centralized control plane for orchestration, policy management, and metadata services. This externalized deployment enhances isolation, resilience, and independent lifecycle management of the control plane, ensuring backup and recovery operations remain available even during infrastructure-level disruptions within the rack. Data movement and processing are handled by distributed Commvault components-including access nodes and MediaAgents-enabling independent scaling to sustain performance and operational flexibility as workloads grow. Commvault host-based protection provides agentless, image-level backups for workloads running on the HPE Private Cloud PC3000, specifically within the HPE Morpheus Software - VM essentials cluster.

Backup and recovery of PC3000 workloads follow a tiered protection model based on 3-2-1 design principles, that ensures resilience by maintaining 3 copies of workload data across 2 different media types and 1 located off-site. Primary backup targets include HPE StoreOnce or HPE Alletra Storage MP X10000 with Data Protection Accelerator Node, offering high-performance backup ingestion, storage efficiency through deduplication or object storage, and seamless integration with Commvault. Secondary protection for backups is provided using HPE StoreOnce CloudBank or HPE Storage Tape, delivering air-gapped, long-term retention for compliance and ransomware resilience.

A key differentiator of this solution is the tight integration between **Commvault CommServe** and HPE storage platforms, enabling storage-efficient backup operations with source and target side deduplication, reduced data movement, and optimized recovery workflows. The reference architecture incorporates deployment and configuration best practices for Commvault, HPE StoreOnce, and HPE Alletra Storage MP X10000 integration with PC3000.

The solution can optionally integrate with HPE OpsRamp for monitoring and observability, providing unified visibility into infrastructure health, performance, and backup operations, while enhancing operational governance. Security is embedded across the design through features such as immutability, encryption, access control, and controlled recovery workflows, ensuring protection against cyber threats and enabling trusted data recovery.

By combining Commvault software-defined data protection capabilities with HPE's high-performance storage ecosystem, this solution delivers a resilient, and efficient foundation for enterprise data protection, enabling predictable outcomes that can align with business SLAs and compliance requirements.

# Solution portfolio

The solution portfolio covers HPE Private Cloud PC3000, Commvault components, HPE Storage platforms such as HPE StoreOnce, HPE Alletra Storage MP X10000, Cloud Bank and Storage Tape where each component plays a defined role within the data protection architecture and integrates tightly with the overall framework.

### HPE Private Cloud PC3000

HPE Private Cloud PC3000 is a self-managed virtualization platform built with modern hyperconverged infrastructure and HPE Morpheus Software - VM essentials, providing an alternative virtualization solution that is compatible with VMware. This reference architecture focus is mainly on PC3000 built on HPE Alletra Storage MP B10000 storage platform.

HPE Private Cloud PC3000 streamlines deployment and lifecycle management, making it well suited for "VM vending" use cases. Its built-in KVM-based hypervisor, HVM, provides a modern alternative virtualization platform designed to address several common customer challenges:

1. **Lower licensing costs** by offering compelling per socket pricing beneficial for high density environments.
2. **Hypervisor choice** – HPE Morpheus Software-VM essentials includes HPE's KVM-based hypervisor, HVM, and can be deployed alongside existing third-party clusters under a single management plane with HPE Morpheus Manager. This eliminates the need for an "either/or" decision or a rip-and-replace approach, allowing workloads to be prioritized and migrated at customer's own pace.
3. **Simplicity, scale, resiliency and protection** – Automated installation and lifecycle management ensures the systems are kept up to date and the solution is ideal for remote and branch locations with limited IT resources onsite.
4. **Future-ready platform** - HPE PC3000 is available in traditional consumption models or in an as-a-service model with HPE GreenLake Flex. HPE Morpheus Software offers a simple upgrade path to HPE Morpheus Software-VM essentials, which includes multi-cloud management, Kubernetes support, governance, and FinOps capabilities.

### Commvault components

This section describes the core components of the Commvault, encompassing both the control plane responsible for orchestration and management, and the data plane that handles backup data processing and movement. The interaction between these core components is described in the subsequent "Integrated solution architecture" section of this document.

#### CommServe server

CommServe server can be deployed on physical server or virtual machine running Linux or Windows.  CommServe Server running Command Center, Orchestrates Commvault backup/restore jobs, manages MediaAgents, maintains the job history, security settings, and configuration database, stores authoritative metadata for the entire Commvault deployment.

#### MediaAgent server

MediaAgent server can be deployed on physical server of virtual machine running Linux or Windows. Responsible for ingest, deduplication, encryption, indexing, and routing data to HPE storage targets.

### Primary Backup Storage

Primary Backup Storage serves as the first level of backup and is provided through either HPE StoreOnce or HPE Alletra Storage MP X10000 with Data Protection Accelerator Node, based on performance and capacity needs.

#### HPE StoreOnce

HPE StoreOnce serves as the primary backup storage tier providing a deduplicated platform optimized for enterprise data protection across HPE Morpheus Software - VM essentials workloads. Integrated through the StoreOnce Catalyst protocol, it reduces storage consumption and network utilization while supporting high-performance backup and recovery.

#### Key design characteristics

— **Efficient data reduction:** StoreOnce performs high-efficiency, source-side deduplication and compression, storing only unique data blocks.

— **Commvault MediaAgent-based integration:** MediaAgent integrates with HPE StoreOnce using Catalyst libraries, where the MediaAgent writes backup data directly to the StoreOnce Catalyst store. Multiple MediaAgents can be configured for scalability, load balancing, and high availability

— **Optimized data transport:** The gateway, using the Catalyst library, enables communication between the proxy and StoreOnce and supports dedupe-aware transfer through block fingerprinting and optimized ingestion.

— **Scalable protection:** StoreOnce supports scalable storage, efficient backup chain management, and optional immutability for ransomware protection and long-term retention.

#### HPE Alletra Storage MP X10000 with Data Protection Accelerator Nodes

HPE Alletra Storage MP X10000 with Data Protection Accelerator Nodes provides a scalable, all-flash object storage platform for modern data protection environments. leveraging native S3 object storage together with StoreOnce Catalyst-based acceleration, deduplication, and compression, it serves as a high-performance backup and recovery storage tier for enterprise data protection workloads.

#### Key design characteristics

— **Cloud-scale object storage:** HPE Alletra Storage MP X10000 is designed for exabyte-scale capacity and high-throughput ingest, enabling Commvault to store backup data directly in S3-compatible buckets without traditional block-based repository constructs.

— **Data Protection Accelerator Nodes:** The data protection accelerator node is a purpose-built, all-flash data protection appliance running HPE StoreOnce Catalyst software. w  hich integrates HPE Alletra Storage MP X10000 as object-based primary backup storage for Commvault.

— **Security and retention:** The platform supports immutability through object lock, providing strong ransomware protection and long-term retention capabilities.

### Secondary and Archive Storage

#### HPE Storage Tape

HPE Storage Tape (StoreEver) is integrated with Commvault as a secondary backup tier, providing a cost-effective and secure solution for long-term retention. Commvault enables policy-based backup-to-tape jobs, allowing data from primary repositories such as HPE StoreOnce or object storage to be automatically copied to tape based on retention requirements.

Tape offers inherent air-gap protection, strengthening resilience against ransomware and cyber threats, while significantly reducing storage costs for archival data. Commvault manages tape media, cataloging, and restores, and supports encryption and lifecycle management to ensure data security and compliance, making it ideal for long-term archival and regulatory use cases.

**HPE Cloud Bank**

HPE Cloud Bank Storage enables tiering of deduplicated backup data from HPE StoreOnce to low-cost external object storage. Utilizing the Catalyst Copy API, the HPE StoreOnce system deduplicates and compresses the data, then replicates only the changes and metadata directly to the Cloud Bank target. Cloud Bank integrates directly with public clouds (like AWS and Azure) or on-premises object storage, dramatically lowering costs for long-term data retention and disaster recovery.

**Network Switches**

HPE Aruba Networking platform based on high-performance, enterprise-grade switching infrastructure is used to provide both management and data path connectivity between HPE Private Cloud PC3000, **Commvault** components, and primary backup storage tier.

The solution also supports bring-your-own-network (BYON) environments for both HPE PC3000 and backup infrastructure (Commvault, StoreOnce, Alletra Storage MP X10000), enabling integration with existing network fabrics while ensuring seamless interoperability.

# Design principles, assumptions and constrains

This section outlines the foundational design principles governing the backup architecture leveraging HPE Infrastructure and Commvault.

## Solution scope (in scope / out of scope)

What's in scope for this reference architecture:

1. Highly available backup and restore architecture for HPE Private Cloud PC3000 with Commvault
2. On-site Layer 2 / Layer 3 network integration of HPE Private Cloud PC3000 with the Commvault
3. Position HPE storage platforms (HPE Alletra MP B10000 and HPE StoreOnce) to deliver production workload storage and backup repository tiers within the Commvault architecture
4. Hardware architecture and Bill of Materials (BOM)
5. Deployment and configuration best practices for integrating Commvault with HPE Private Cloud PC3000 and HPE storage platforms
6. Monitoring Commvault backup and recovery deployments through the HPE Hybrid Observability platform, OpsRamp, for enhanced visibility and operational control

What's not in scope for this reference architecture:

1. Detailed configuration steps for Commvault installation and its integration with HPE Private Cloud PC3000 and HPE Storage platforms
2. Performance considerations (covering aspects such as backup throughput, IOPS, backup window optimization)
3. Details about licensing and procurement
4. Day-2 operational procedures such as alerting and troubleshooting

# Data protection strategy

### Adherence to 3:2:1 backup strategy

The recommended architecture implements classic 3-2-1 Data protection strategy that ensures data resilience by maintaining multiple, independent copies of data across different storage types and locations.

— Keep **3 copies of data**: one on primary workload storage (e.g., HPE Alletra Storage MP B10000), one on primary backup tier (e.g., HPE StoreOnce) and one on secondary backup tier (e.g., HPE Storage Tape)

— Store copies on at least **2 different media types** (e.g., Alletra iSCSI LUN and StoreOnce catalyst repository)

— Maintain **1 copy offsite** to protect against site failures and ransomware (e.g., HPE Storage Tape)

**Note**

While the 3-2-1 data protection rule remains a foundational best practice, the 3-2-1-1-0 approach further improves resilience by incorporating immutable or air-gapped copy for ransomware protection, while ensuring backup integrity through regular validation and recovery testing

By following this approach, the solution ensures that production workloads are kept physically and logically distinct from the protection tiers. This separation enhances data security and resilience, reducing the risk of data loss resulting from hardware failure, cyber threats, or accidental deletion.

### Primary storage

HPE Alletra Storage MP B10000 presented as the shared iSCSI storage to HPE Morpheus Software-VM essentials cluster in HPE Private Cloud PC3000 serves as the primary workload storage by hosting production data which is the first copy in the 3-2-1 strategy. It is designed to support modern, traditional, and mixed workloads with enterprise-grade scale, availability, security, and performance.

**Note**

For HPE Morpheus Software-VM essentials environments, Commvault IntelliSnap integration is not yet supported with HPE Alletra Storage MP B10000 to accelerate backups and to reduce load on production systems.

### Primary backup tier

The following are the two primary backup storage tier options used to store the secondary copy of data backed up from the production HPE Morpheus Software-VM essentials cluster of PC3000.

1. HPE StoreOnce Catalyst: Used for deduplication-optimized, performance-efficient backups.
2. HPE Alletra Storage MP X10000 with Data Protection Acceleration Node: A scale-out, high-performance object storage platform designed for data-intensive and cloud-native workloads. When paired with the Data Protection Acceleration Node, it enables parallelized, high-throughput backup and recovery operations by offloading data movement and optimizing data paths.

### Secondary backup tier

Commvault extends data protection to secondary tiers through backup copy and tape archival workflows, creating isolated, long-term copies that are physically separated from primary and disk-based backup storage.

Following are the two secondary backup storage tiers which stores the data (third copy) sent as a backup copy either directly from Commvault or from primary storage tier such as HPE StoreOnce or HPE Alletra Storage MP X10000 with Data Protection Accelerator Nodes.

1. HPE Storage Tape:  Used for secure, long-term data archiving, ransomware defense, and cost-effective cold backups or infrequently accessed data.

2. HPE Cloud Bank: Used as an extension of HPE StoreOnce to move and store backup data in public or private cloud object storage.

**Comprehensive protection of data and configuration**

A robust data protection strategy must address both workload data and platform configuration, including Commvault configuration and underlying workload cluster i.e., HPE Morpheus Software-VM essentials on PC3000. This approach ensures comprehensive recoverability, enabling restoration of both data and infrastructure configuration in the event of system or site-level failures.

**Protection of workloads on PC3000 with HPE Morpheus Software-VM essentials**

This level of data protection focuses on safeguarding workload data, primarily through image level backup and restore of virtual machines running on PC3000 with HPE Morpheus Software-VM essentials. Backup data is stored across primary backup storage tiers such as HPE StoreOnce, or HPE Alletra Storage MP X10000, providing flexibility in performance and retention.

**Configuration protection**

To address system or site level failures, it is necessary to protect configuration of PC3000 workload clusters and backup server. In addition to backup of workload data, this includes backup of:

— PC3000 with HPE Morpheus Software-VM essentials cluster configuration and environment settings

Commvault control plane, Commvault configuration such as CommServe database, storage policies, schedules, and indexing metadata

**HPE Morpheus Software-VM essentials cluster configuration protection**

Protecting the workload cluster configuration ensures that cluster topology, resource definitions, and environment settings can be restored following infrastructure or site-level failures. This cluster level configuration backup enables rapid reconstitution of the workload platform reducing rebuild time and operational risk.

Refer to the following documentation to perform the configuration backup of HPE Morpheus Software-VM essentials cluster, Backing Up and Restoring HPE Morpheus Enterprise Appliance

### Backup recovery objectives (RPO / RTO)

The architecture can support different backup and recovery objectives based on the selected protection method and storage tier, enabling alignment with application criticality and business requirements.

**Table 1.** Recovery objectives alignment

| Protection Tier | Typical RPO | Typical RTO | Usage |
|---|---|---|---|
| Primary Backup Tier (StoreOnce / Alletra Storage MP X10000) | Minutes to Hours | Minutes to Hours | Standard enterprise workloads with defined recovery windows |
| Secondary / Object Storage Tier (HPE Storage Tape/ HPE Cloud Bank) | Hours to Days | Hours to Days | Long-term retention and cost-optimized recovery |
| Archive located off-site (Tape/ cloud object storage) | Hours to Days | Hours to Days | Compliance and disaster recovery scenarios |

Actual recovery objectives depend on workload characteristics, data size, infrastructure design, and operational processes. Table 1 provides baseline guidelines on RPO/RTO for different enterprise workloads, and these RPO/RTOs are highly dependent on solution implementation parameters such as backup data volume, available network bandwidth, deduplication strategy etc.

# Compatibility (firmware and software versions) *

The following table lists the hardware firmware and software versions that were validated as part of this solution. Using these versions helps ensure compatibility, interoperability, and consistent operation across the solution components.

### HPE Private Cloud PC3000

Refer to the PC3000 quick specs for more information on supported hardware and firmware compatibility, https://www.hpe.com/psnow/doc/a50004281enw.pdf**Commvault**

**Table 2.** Commvault Backup Infrastructure

| Type | Version | Image file |
|---|---|---|
| Commvault | 11.40.47 | Commvault_linux-x8664_Media_11_40.tar |
| Commvault Grid | 11.40.47 | sp40_13_hsx_prod_dvd_09152025_061956.iso |
| RHEL | 9.8 | RHEL-9.8.0-updates-20260511.3-x86_64-dvd1.iso |

**HPE hardware for backup infrastructure**

Drivers, firmware updates, and software downloads compatible with HPE hardware are available in the HPE Support Center under **Software & Drivers**.

**Table 3.** HPE Hardware for backup infrastructure

| Hardware | Firmware | Notes |
|---|---|---|
| HPE ProLiant DL3xx Gen11/Gen12 | 2026.03.00.00 | Recommended for bare metal deployment of Commvault components |
| HPE StoreOnce | 4.3.x<br>5.2.x | 4.x for Gen 4 appliances<br>5.x for newer Gen 5 appliances |
| HPE Alletra Storage MP X10000 | 10.5.x | |

*The version numbers provided are point-in-time references and intended solely for informational purposes. Please refer to official documentation or support channels for up-to-date recommendations and compatibility details.

# Integrated solution architecture

## Logical architecture – HPE Infrastructure

In this logical view, HPE Private Cloud PC3000 hosts an HPE Morpheus Software-VM essentials cluster that runs the production virtual machines. The cluster consists of hypervisor hosts running the HVM hypervisor, providing a highly available and balanced compute foundation. Virtual machines are distributed across these hosts and centrally managed by HPE Morpheus Manager, which handles lifecycle management, cluster operations, and integration with external systems. A Data Services Connector VM also runs on the HVM cluster, connecting the PC3000 environment to the HPE GreenLake Central data services cloud console.

Figure 1 illustrates a high-level logical architecture for a commvault based backup solution designed for HPE Morpheus Software-VM essentials workloads running on PC3000.

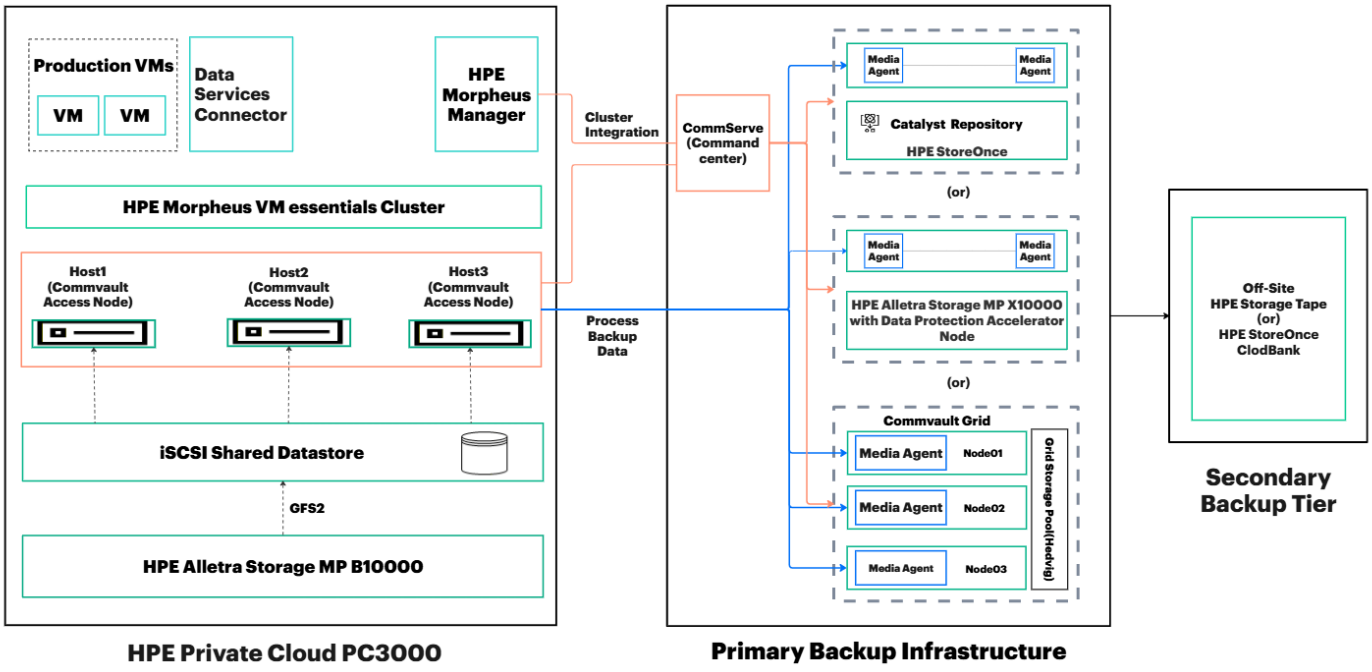



**Figure 1.** High-level logical architecture for a Commvault-based backup solution integrated with HPE Private Cloud PC3000

Workload data is stored on a shared iSCSI datastore, provisioned through the HPE Alletra Storage MP B10000 array of HPE Private Cloud PC3000. For the HVM cluster, datastores can be GFS2 clustered file system enabling concurrent access from multiple hosts and providing consistent, scalable storage across the cluster. This design allows all hypervisor nodes to read and write to a common storage pool, which is critical for workload mobility, failover, and backup consistency.

Backup and recovery operations are orchestrated by the Commvault CommServe, can be deployed on a Linux-based virtual machine or BareMetal server and provides the centralized control plane for data protection across the environment. It manages job scheduling, policy enforcement, and recovery workflows and is administered through the CommServe Command Center, which provides the interface for configuring and monitoring backup and restore operations. To enhance resiliency and security, the Commvault control plane and data plane are deployed in a separate fault domain outside the PC3000 environment, ensuring continued availability of the backup control plane in the event of cluster failures, storage array outages, or ransomware incidents.

Commvault Access Node acts as a gateway or data access server between Commvault and the HPE Morpheus Software-VM essentials workloads running on PC3000. It is deployed as a host-level package/service and act as proxies that read VM data from the shared storage. Its main job is to discover, read, and sometimes restore data from the source system. Commvault MediaAgent is installed on a dedicated physical or virtual server in solution rack and act as a data transmission manager in the CommCell environment. It receives data from clients or Access Nodes and writes backup data to the configured storage target, such as HPE StoreOnce. It also handles deduplication, compression, encryption, and restore operations. A repository is the actual storage location where backup data is stored. It may be HPE StoreOnce, Alletra Storage MP X10000 or cloud storage. The MediaAgent writes backup data into the repository.

The primary backup tier is implemented using disk-based or object storage repositories, which can be configured either as HPE StoreOnce or HPE Alletra Storage MP X10000 with Data Protection Accelerator nodes:

— HPE StoreOnce leveraging the Catalyst protocol for deduplication and efficient data transfer. HPE StoreOnce provides a purpose-built backup storage platform with high-performance ingestion, inline deduplication, and compression capabilities, significantly reducing storage consumption while maintaining efficient restore operations.

HPE StoreOnce Catalyst is a native integration between Commvault MediaAgents and HPE StoreOnce storage. Commvault writes backup data directly to a Catalyst Store, allowing StoreOnce to perform deduplication and storage optimization.

— HPE Alletra Storage MP X10000 with Data Protection Accelerator nodes, provides scalable, high-performance object-based backup storage. For S3-compatible object storage repositories, including HPE Alletra Storage MP X10000 platform. The Commvault MediaAgent integrates with HPE StoreOnce Catalyst technology and sends backup data through the Catalyst interface to the data protection accelerator nodes. The data protection accelerator nodes perform deduplication, Compression, Encryption, Data optimization before storage writes the optimized backup objects to the Alletra Storage MP X10000.

— To support extended retention and compliance-driven data protection strategies, HPE Storage Tape or HPE Cloud Bank may be deployed as a secondary backup tier managed by CommServe. Backup copy jobs are centrally orchestrated by CommServe, which moves protected backup data from the primary backup repository to these secondary targets, providing long-term retention, enhanced data resilience, and air-gapped protection.

**Note**

HPE Morpheus Software – VM essentials does not support Commvault IntelliSnap with HPE Alletra in a typical deployment. IntelliSnap depends on block-level array integration and direct LUN access, while HPE VM essentials support only Local/NFS/GFS2 datastores that don't expose those capabilities. Because of this, backups are usually done using image-level or in-guest agent-based methods instead of array-based snapshots.

# Connectivity and design decisions

## Integration of HPE Private Cloud PC3000 with Commvault

This section covers both layer 2 (L2) and layer 3 (L3) network integration designs of PC3000 rack with Commvault rack. The decision to chose either layer 2 or layer 3 is normally driven by scalability, resilience, and operational simplicity.

Layer 2 network integration provides the shortest path, lowest latency with simplified east west flow but will result in larger broadcast domain and may need setting of spanning tree protocols to prevent layer 2 loops. Layer 2 is usually suitable for small to moderate environments with one or two racks where same broadcast domain is needed across racks. Adaption of this L2 design for PC3000 integration with Commvault provides low operational complexity with no routing points and simpler firewall policy.

Layer 3 network provides cleaner segmentation and better scale but will introduce an extra hop with slightly higher latency compared to layer2. Layer 3 is suitable for large environments with multiple racks which requires better scaling and strong failure isolation with no complexity of spanning tree protocols. Adaption of this L3 design for PC3000 integration with Commvault provides better scaling and fault isolation with smaller failure domains.

**Layer 2 (L2) network Integration**

HPE Private Cloud PC3000, built on iSCSI-based HPE Alletra Storage MP B10000, supports a robust network architecture comprising one out-of-band management network, one in-band management network, and dual iSCSI networks to ensure storage path redundancy. The iLO interfaces, along with the management ports of the storage array and network switches, are connected to the out-of-band management network for secure and isolated administration. All HPE Morpheus Software-VM essentials hosts, the HPE Morpheus Manager, Data Services Connector VM, and other compute VMs reside on the PC3000 management network for operational connectivity.

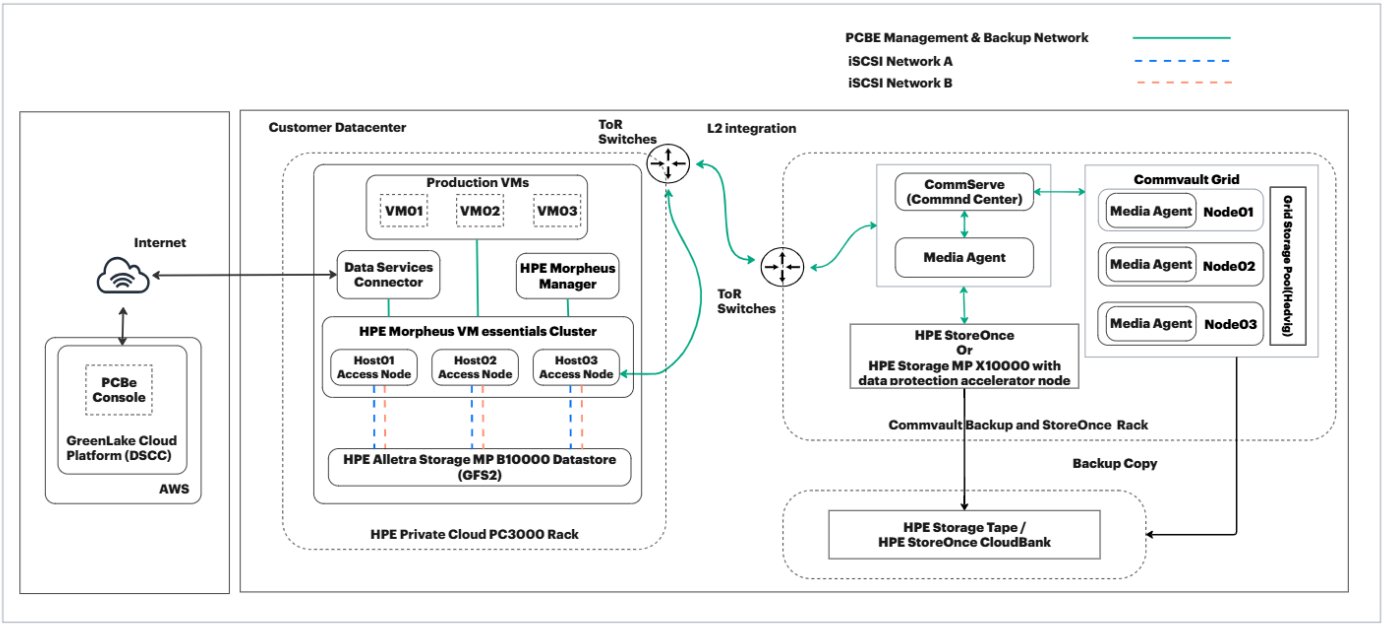



**Figure 2** Layer 2 integration of HPE Private Cloud PC3000 rack with Commvault components

Layer 2 integration is implemented by extending the PC3000 management VLAN across the ToR switches of both the PC3000 and Commvault backup racks, creating a shared connectivity domain that facilitates communication between Commvault control plane components and HPE StoreOnce.

**Note**

By default, PC3000 with HPE Morpheus Software-VM essentials cluster supports only management VLAN and iSCSI storage VLANs during deployment. In this integration, PC3000 management VLAN is also leveraged as the backup VLAN across both the PC3000 rack and the Commvault Backup Server rack.

If customer wants the backup network to be segregated from management network of PC3000, then additional network can be created with the assistance of HPE Support.

A multi-chassis link aggregation group (MC-LAG) carrying the PC3000 management/backup VLAN is configured between the ToR switches of both racks, enabling the backup VLAN to extend across racks. The Layer 2 extension simplifies deployment and reduces routing or firewall dependencies, which can make backup discovery, transport communication, and management easier and faster in moderate-sized environments. Because all backup components remain in the same subnet, the Commvault access nodes can directly communicate with the MediaAgent and backup infrastructure using simple IP adjacency and standard Ethernet forwarding.

### Layer 3 (L3) network integration

HPE Private Cloud PC3000, built on iSCSI-based HPE Alletra Storage MP B10000, supports a segmented network design with one out-of-band management network, one management network, and dual iSCSI networks for storage redundancy. iLO interfaces and management ports connect to the out-of-band network, while all HPE VM essentials hosts, Morpheus Manager, Data Services Connector VM, and other compute workloads operate on the PC3000 management network.

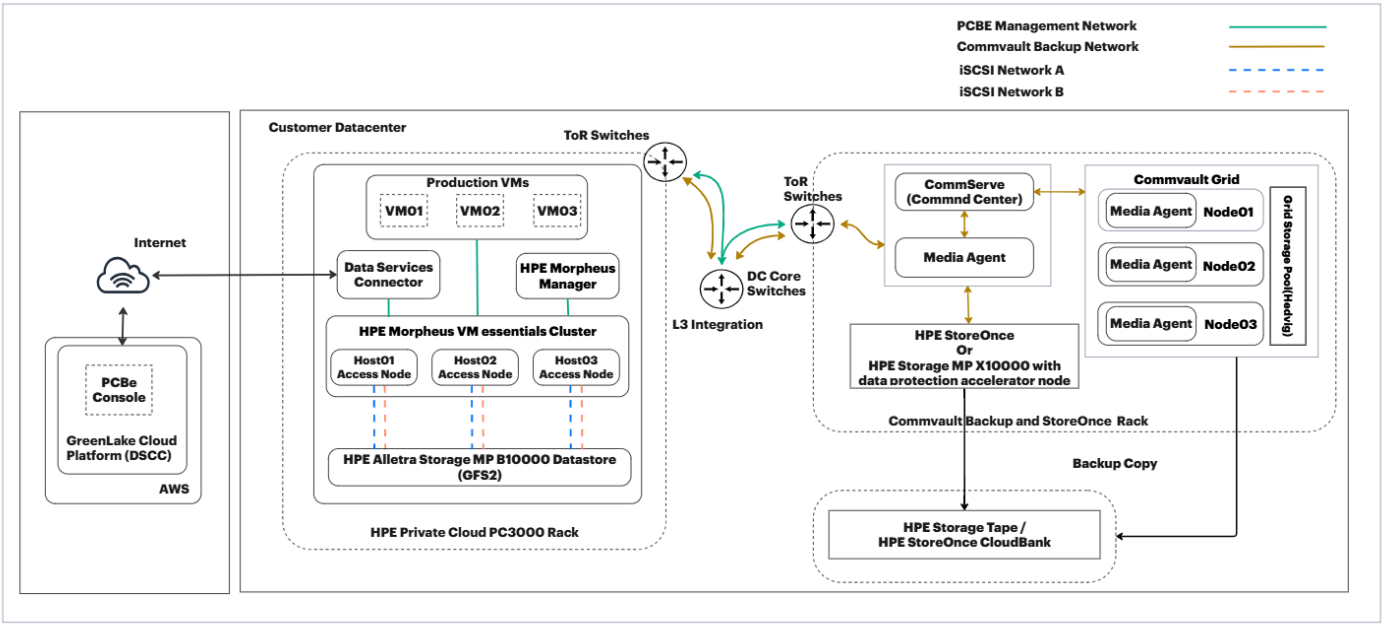



**Figure 3.** Layer 3 integration of HPE Private Cloud PC3000 rack with external Commvault

Layer 3 integration is implemented by routing backup traffic between the PC3000 rack and the dedicated Commvault backup rack through the DC Core switches. Separate subnets are used for the PC3000 management network and the Commvault backup network, allowing the backup infrastructure to operate in an isolated routed domain.

**Note**

By default, PC3000 with HPE Morpheus Software-VM essentials cluster supports only management VLAN and iSCSI storage VLANs during deployment. In this integration, PC3000 management VLAN is also leveraged as the backup VLAN in the PC3000 rack and routes to Commvault Backup VLAN in the Commvault rack.

If customer wants the backup network to be segregated from management network of PC3000, then additional network can be created with the assistance of HPE Support.

The ToR switches in both the racks uplink to the DC Core switches using routed interfaces or VLAN switch virtual interfaces, enabling IP-based forwarding between the Commvault access nodes, MediaAgents, and HPE StoreOnce components. Backup traffic generated by the Commvault Access nodes is routed through the Layer 3 core network to the Commvault MediaAgent and to the HPE StoreOnce appliance.

The routed design improves scalability and resiliency by reducing broadcast traffic, removing spanning tree dependencies, and enabling better security policy enforcement. This Layer 3 integration allows administrators to apply routing policies, ACLs, QoS, and firewall controls between the production virtualization environment and the backup infrastructure while maintaining efficient backup data transport.

## Commvault in the HPE Private Cloud PC3000 rack

If hosting Commvault in a separate rack outside of PC3000 is not an option, then Commvault components could be added to the PC3000 Rack itself outside of the PC3000 with HPE Morpheus Software-VM essentials cluster.

This placement protects Commvault components against cluster level failures but cannot be considered as a rack-level resiliency solution. Since switches and PDUs are always available in redundant pairs within a PC3000 rack,

this should still be a good option to isolate Commvault fault domain from the PC3000 with HPE Morpheus Software-VM essentials cluster.

**Note**

When the Commvault is deployed within the PC3000 rack, it is recommended to regularly back up the Commvault configuration to a location outside the rack. This ensures that the Commvault control plane can be restored in the event of a rack-level failure or complete site outage affecting the PC3000 infrastructure.

HPE Morpheus Software-VM essentials does not support SAN transport mode because it can not use block storage with direct LUN access like VMware vSphere environments. Instead, it relies on GFS2 or NFS datastores, where backups are performed over the network.

## HPE StoreOnce vs HPE Alletra Storage MP X10000 with data protection accelerator nodes

When choosing between HPE StoreOnce and HPE Alletra Storage MP X10000 for the primary backup target, the decision should be guided by the key evaluation criteria presented in the following Table 5.

**Table 4.**Primary Backup Tier Decision Criteria

| Feature | HPE StoreOnce (Catalyst) | HPE Alletra Storage MP X10000 with Data Protection Accelerator Node |
|---|---|---|
| Deployment Size | Better suited for small to medium-sized environments with moderate data volumes. | Better suited for large to extra-large environments with multi-petabyte scale. |
| Backup Throughput Requirement | Suitable when backup throughput requirements are moderate and within typical enterprise ranges. | Suitable when very high ingest throughput is required, including environments exceeding one hundred terabytes per hour. |
| Backup Window | Fits environments where standard backup windows are acceptable and can be met without aggressive performance requirements. | Ideal for environments where backup windows are highly constrained and rapid data ingestion is critical. |
| Cost Consideration | Preferred when cost efficiency and predictable investment are key priorities. | Preferred when performance and scalability requirements take precedence over cost considerations. |
| Architecture Model | Uses a tightly integrated appliance where data reduction and storage functions operate within the same system. | Uses a disaggregated architecture where data processing and storage functions are separated and independently scaled. |
| Scalability | Achieved through incremental expansion of appliance capacity and federation across systems. | Achieved independently by increasing processing nodes for performance and storage nodes for capacity. |
| Data Reduction | Handled within the platform using integrated deduplication and compression technologies. | Performed by dedicated data protection accelerator nodes before data is written to scalable object storage. |

| Feature | HPE StoreOnce (Catalyst) | HPE Alletra Storage MP X10000 with Data Protection Accelerator Node |
|---|---|---|
| Network Utilization | Network traffic is optimized through deduplication techniques that reduce the amount of data transferred. | Network utilization is optimized through parallel data reduction and high-throughput ingestion pipelines. |
| Restore Performance | Restore performance is reliable and consistent, typically aligned with disk-based system capabilities. | Restore performance is enhanced through flash-based storage and parallel processing, enabling faster recovery. |
| Workload Type | Works well for traditional workloads such as virtual machines, file systems, and enterprise applications. | Optimized for high-change-rate workloads, large databases, and data-intensive environments. |
| Growth Requirement | This option is suitable for environments with steady and predictable data growth. | This option is ideal for environments experiencing rapid data growth and requiring long-term scalability. |

# Deployment and configuration guidance

## HPE Private Cloud PC3000 (HPE Morpheus Software-VM essentials)

This section outlines best practices for deploying and configuring an HPE Private Cloud PC3000 environment based on HPE Morpheus Software-VM essentials clusters integrated with HPE Alletra Storage MP B10000. These recommendations are aligned with HPE validated configurations and deployment guidance intended to ensure high availability, consistency and optimal performance

**Compute**

— HPE Morpheus Software-VM essentials clusters in PC3000 require a minimum of three HPE ProLiant DL servers to support high availability, workload mobility, and cluster quorum.

— All servers within the cluster must belong to the same CPU family and maintain consistent hardware configurations to ensure compatibility and balanced workload distribution.

— PC3000 is typically shipped with preinstalled HPE Morpheus Software-VM essentials hypervisor on compute nodes and a Data Services Connector VM, and it is recommended to validate and update software versions using the HPE Private Cloud Installer before deployment.

**Network**

— PC3000 requires a minimum of two switches configured as a pair, particularly when leveraging network automation capabilities. Supported switches include HPE Aruba 8325 and Aruba 6300 models.

— Network traffic can be logically segmented into iLO interface, management, and iSCSI data networks. However, VLAN tagging is not supported for iSCSI and management traffic, and such traffic must remain untagged throughout the design. Dual network interfaces per server should be used to provide resilience across both switches.

— Link aggregation should be implemented for uplink connectivity to upstream or customer networks using LAG or MC-LAG configurations. Customer-side switches must also ensure that uplink ports are configured within a single aggregation group to maintain consistency and redundancy.

— Cabling must strictly follow HPE defined port assignments, where management and iSCSI networks are mapped to specific switch NIC ports. Incorrect cabling will result in failure of automated deployment. All servers and storage components should be connected to the same switch pair. Additionally, LLDP must be enabled, and

optional configuration of jumbo frames should be consistently applied across the network to avoid MTU mismatches.

**Storage**

— PC3000 deployments are integrated with HPE Alletra Storage MP B10000, which provides shared storage services across the HPE Morpheus Software-VM essentials cluster.

— The storage configuration requires two dedicated iSCSI data networks, which are mandatory to ensure storage network redundancy. These networks must be mapped consistently between servers and storage, with one subnet handling odd ports and the other handling even ports, ensuring proper traffic separation and redundancy.

— PC3000 automatically provisions a shared datastore for HPE Morpheus Software-VM essentials cluster, with a default size of 2 TB. This datastore is used for both virtual machine image storage and cluster heartbeat functions. It is critical to monitor datastore utilization regularly, as a fully consumed datastore can lead to cluster instability, including VM failures or service disruption.

**Deployment and automation guidance**

— IP address ranges must be clearly defined for management, iLO interface, and iSCSI networks to support automated assignment and scalability. Only static IP addressing scheme is supported during deployment.

— DNS and NTP configuration are mandatory, with at least two to three servers recommended for each service. All components within the PC3000 environment must use the same DNS and NTP configuration to ensure synchronization and operational consistency.

— Firewall rules should be configured to allow required communication over standard ports such as HTTPS, SSH, DNS, and NTP. Additionally, communication between servers, storage, and HPE GreenLake services must be permitted to ensure proper integration and management.

— Deployment should be performed using the HPE Private Cloud Installer, which provides automated validation of configuration parameters such as DNS, NTP, and IP addressing. The installer also simplifies deployment by enabling early detection of configuration issues and automating several setup steps, including hypervisor and management component initialization. For the latest supported version please follow the PC3000 deployment guide.

— Network automation can be leveraged to validate switch configuration and cabling, reducing the likelihood of misconfiguration and speeding up deployment.

## Commvault components

**CommServe**

The CommServe server acts as the central management component of the Commvault platform. It is responsible for orchestrating backup and restore operations, maintaining the backup catalog and metadata database, managing storage and retention policies, scheduling jobs, and coordinating communications between all Commvault components.

Deployment strategy

— Deploy CommServe with LiveSync enabled between two identical servers or virtual machines. This provides active–standby high availability by continuously replicating CommServe database, Logs and metadata.

— Linux (RHEL/Rocky) is recommended for CommServe deployment instead of windows for better performance and security.

— Isolate the disks required for operating system, database, and logs. Also host CommServe SQL database on high performance SSD/NVMe.

— Backup data processing should be offloaded to MediaAgents, CommServe should only orchestrate jobs and manage metadata.

— Ensure reliable and low-latency network connectivity from CommServe to Commvault MediaAgents and workload clusters.

— Network connectivity between two LiveSync CommServe nodes should be of high bandwidth and low latency (< 5ms).

**MediaAgents**

MediaAgents act as the data movement and processing layer in the Commvault architecture, transferring backup data between protected workloads and storage targets while performing deduplication, compression, and encryption. They also host indexing services that maintain backup metadata, enabling efficient search, fast recovery, and granular restore capabilities.

Deployment strategy:

— Linux (RHEL/Rocky) is recommended for Media Agent deployment instead of windows for better performance and security.

— Isolate the disks required for operating system, deduplication database, and logs. Also host deduplication database on high performance SSD/NVMe.

— Place the MediaAgents close to workload cluster hosts either same rack or on low latency networks to ensure optimal backup performance.

— Ensure redundant and low-latency network connectivity from virtual server agents on workload clusters to MediaAgents to backup storage targets (StoreOnce).

— Configure automatic load balancing when multiple MediaAgents are used to ensure horizontal scalability.

— Enable encryption for data in transit to prevent network sniffing and man-in-the-middle attacks.

— Encryption for data at rest can be enabled to protect the backup data when backup storage is compromised.

## Deploying Commvault Access node packages on PC3000 system

Since PC3000 is an engineered system, it enforces several guardrails around the stack components. Specifically, on the HVM hosts, root SSH login is disabled, and no root user account is exposed to customers.

---

**Note**

Customers cannot directly install Commvault packages on the HVM nodes.

---

For customers who require Commvault need to contact **HPE support**. Since the support team has mechanisms to access the system with root privileges, they handle the installation of **Commvault access packages** on behalf of the customer.

Deployment strategy:

— Access Nodes or VSAs should be deployed close to data source such as within the same workload cluster

— For better load balancing, deploy multiple access nodes or VSAs per cluster.

— HPE Morpheus Software--VM essentials cluster, the access node functionality is deployed as a host-level package/service with assistance of HPE Support.

— Do not co-locate access nodes with application workloads. This avoids resource contention since backup jobs can be I/O intensive.

— For workload hosts with local storage, access nodes should be deployed per host to maximize performance and minimize data movement across hosts. For workload hosts with shared storage, fewer access nodes may be sufficient, but deploying multiple access nodes is still recommended to ensure scalability, load distribution, and high availability.

— Network:

Ensure redundant and low-latency network connectivity from access nodes or virtual server agents on workload clusters to MediaAgents to backup storage targets (StoreOnce).

## HPE StoreOnce

**Backup target**

It is recommended to use HPE StoreOnce Catalyst (over TCP/IP or Fibre Channel) as the primary backup target with Commvault.

— Catalyst integration enables:

- Optimized data transfer using Commvault MediaAgent ( From Accessnode/proxy to MediaAgent and from MediaAgent to StoreOnce)
- Superior performance compared to SMB/NFS shares or VTL (Virtual Tape Libraries) targets
- Reduced bandwidth utilization and improved deduplication efficiency

— HPE StoreOnce Cloud Bank can be used as a secondary tier for long-term retention:

- Enables extension of Catalyst stores to low-cost object storage (on-prem or cloud)
- Can be integrated with Commvault backup copy jobs for tiering and archival

**Deduplication strategy**

— With Commvault and HPE StoreOnce Catalyst, the recommended approach is generally to leverage StoreOnce deduplication as the primary data reduction technology rather than performing excessive deduplication, compression, or encryption within Commvault. This approach reduces CPU and memory overhead on the client and MediaAgent, minimizes processing bottlenecks, and allows StoreOnce Catalyst to optimize data transfer and storage efficiency using its native deduplication capabilities.

**Network**

— Ensure low latency and high bandwidth connectivity between PC3000 with HPE Morpheus Software--VM essentials cluster, Commvault and HPE StoreOnce.

— Add redundant network paths for resilience

— For IP-based configurations, enable jumbo frames end-to-end where supported

## HPE Alletra Storage MP X10000 with data protection accelerator node

**Backup target**

— HPE Alletra Storage MP X10000 with Data Protection Accelerator Nodes is recommended as a primary backup storage tier for data-intensive and cloud-native workloads. On the Data Protection Accelerator Node, the Catalyst Cloud Bank Store is configured to map to the S3 buckets on X10000 with the “Service Provider” set to HPE Alletra Storage MP X10000.

— Separate object buckets are recommended for each workload type to provide granular retention and immutability, better security, and parallel data streams.

**Network**

High bandwidth and low latency network are recommended between PC3000 with HPE Morpheus Software--VM essentials cluster, Commvault and HPE Alletra Storage MP X10000 for faster backup and better restore performance.

**Security**

Enable the object lock on HPE Alletra Storage MP X10000 which provides immutability for stored objects. This is critical to ensure protection against ransomware and accidental deletion.

## Commvault Grid

**Backup target**

Commvault Grid cluster is recommended to use as a primary backup storage tier and should be built on identical server hardware, and a minimum of three servers are necessary to maintain the Grid cluster quorum and resiliency.

NVMe/SSD disks are recommended for metadata/cache tier and HDD for capacity tier of Grid cluster.

Network:

Deploy Commvault Grid cluster with isolated networks for management, data protection/backup, and storage.

Ensure redundant and low-latency network connectivity between workload cluster backup network and Commvault Grid data protection/backup network.

# Hardware architecture and Bill of Materials

## HPE Private Cloud PC3000

Refer to the PC3000 Quick Specs for more information on its bill of materials, https://www.hpe.com/psnow/doc/a50004281enw.pdf

**Table 5.**HPE Private Cloud PC3000 with Alletra Storage MP (Block)

| Component | Configuration |
|---|---|
| Storage | 1 x HPE GreenLake for Private Cloud Business Edition with Alletra Storage MP (Block) |
| Switches | 2 x HPE Aruba Networking CX 8325-32C |
| Compute | 3 x HPE ProLiant Compute DL360 Gen12 Configure-to-order Server for Private Cloud Business Edition |

## Compute tier (HPE ProLiant DL for Commvault CommServe and MediaAgent)

The HPE ProLiant DL320 Gen12 with 1 CPU, 1 to 4 32GB memory and 2 internal OS boot disks in RAID 1 mode can be used. Disk in RAID 1 mode will be selected for the operating system and all other disks available on server will be formatted as data disks automatically.

**Table 6.**HPE ProLiant DL for Commvault

| Component | Configuration |
|---|---|
| Server | HPE ProLiant DL320 Gen12 |
| CPU | One (16-core) |
| Memory | 4 x 32 GB |
| OS Boot | NS204i (2 x 960 GB) |
| Networking | 2 x 10/25 GbE 2- port Adapter |
| Storage | 2 x 1.6 TB NVMe |

# Backup target tier

### Primary backup HPE StoreOnce

**Table 7.** HPE StoreOnce as primary backup storage

| Model | HPE StoreOnce 3760 | HPE StoreOnce 5720 | HPE StoreOnce 5660 | HPE StoreOnce 7700 |
|---|---|---|---|---|
| Capacity expansion | 1x Disk Capacity Expansion kit | 3x HPE StoreOnce 5720 180TB Disk Upgrade kit | 8x HPE StoreOnce 5660 192TB Upgrade Kit | 6x HPE StoreOnce 7700 92TB Upgrade Kit |
| Yields usable capacity | 108 TB -216 TB | 144 TB - 576 TB | 1100 TB | 92 TB – 552 TB |
| Usable capacity with Cloud Bank | Up to 648 TB | Up to 2268 TB | Up to 3300 TB | 32.3 PB |
| Form Factor | 2U | 4U | Up to 18U | 2U |
| TB/Rack Unit | 108 | 144 | 61.11 | 92 |

### Primary backup HPE Alletra Storage MP X10000

**Table 8.**HPE Alletra Storage MP X10000 with the standard-density variant

| Hardware | Configuration |
|---|---|
| Controller nodes | 2 x Compute Enclosures (CBoxes) |
| Internal Fabric | 2 x 32 port Ethernet switches (100 GbE per port) |
| Storage (JBOF) | 2 x 1352 TB Storage Enclosure (DBoxes)<br>Yields 2.2 PB usable capacity<br>Provides aggregate throughput of up to<br>102 GB/sec read and 17 GB/sec write |

### Commvault Grid

Commvault Grid nodes are multi-role appliance nodes running multiple Commvault services.

Refer to the HPE Solutions with Commvault configuration guide for more information on its bill of materials, https://www.hpe.com/psnow/doc/a00060014enw.

**Note**

Refer to the “Reference Configuration” section of Reference Architecture for Data Protection with Commvault for detailed recommended hardware configuration.

# Security and governance

When HPE StoreOnce or HPE Alletra Storage MP X10000 is used as the backup storage tier with Commvault as the backup platform, each platforms deliver their own key security capabilities. Some capabilities are platform-specific, while others--such as encryption and immutability-can overlap between the platforms. Defining ownership of the security features early is essential for both security and operational efficiency. For example, applying encryption at both Commvault and StoreOnce can increase CPU utilization on the source workload and reduce StoreOnce deduplication efficiency. Therefore, clear security design boundaries between backup server and backup storage tier can help preserve performance and storage efficiency and strengthen the overall security architecture.

## Security design scenarios

The following scenarios demonstrate how Commvault and the backup storage tier can be configured to meet different security and protection requirements. These use cases highlight common backup deployment scenarios and the corresponding security considerations such as maximizing storage efficiency and ensuring data confidentiality.

**On-site backups requiring maximum deduplication efficiency**

In an on-site data center where backups are stored locally on HPE StoreOnce or HPE Alletra Storage MP X10000, backup data transferred over the secure data center network from the Commvault access node to the MediaAgent does not need to be encrypted before reaching the backup storage tier. In this design, encryption can be applied at the HPE StoreOnce layer before the data is written to disk.

Applying encryption only at HPE StoreOnce or HPE Alletra Storage MP X10000, rather than at the Commvault MediaAgent, improves deduplication efficiency. If required, IPsec tunnel functionality provided by the primary storage tier can be used to protect data in transit from Commvault to backup storage target.

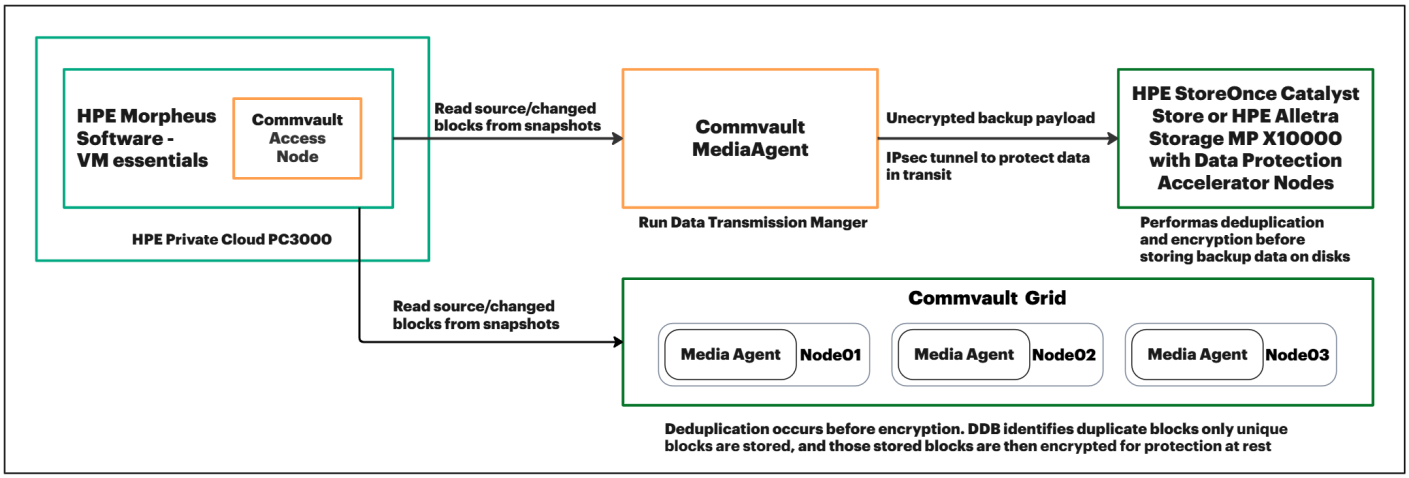



**Figure 4.** Backup workflow providing maximum deduplication efficiency

### Off-site backups requiring high security during transit

For off-site backups stored on HPE StoreOnce or HPE Alletra Storage MP X10000, it is best to encrypt the data locally with Commvault before it is transferred to the remote backup storage tier. This provides stronger protection while the backup data leaves the local network and traverses external links. After the data reaches the remote site, HPE StoreOnce or HPE Alletra Storage MP X10000 can perform deduplication before the data is written to disk.

Using encryption at the Commvault level can increase CPU utilization on the Commvault Backup Server and significantly reduce deduplication efficiency at the backup storage tier. Encryption effects deduplication efficiency since it converts structured, repeatable data into randomized, non-repetitive ciphertext, eliminating patterns required for block matching in deduplication. If required, TLS tunnel functionality provided by the Commvault can be used to protect data in transit from Commvault to backup storage target.

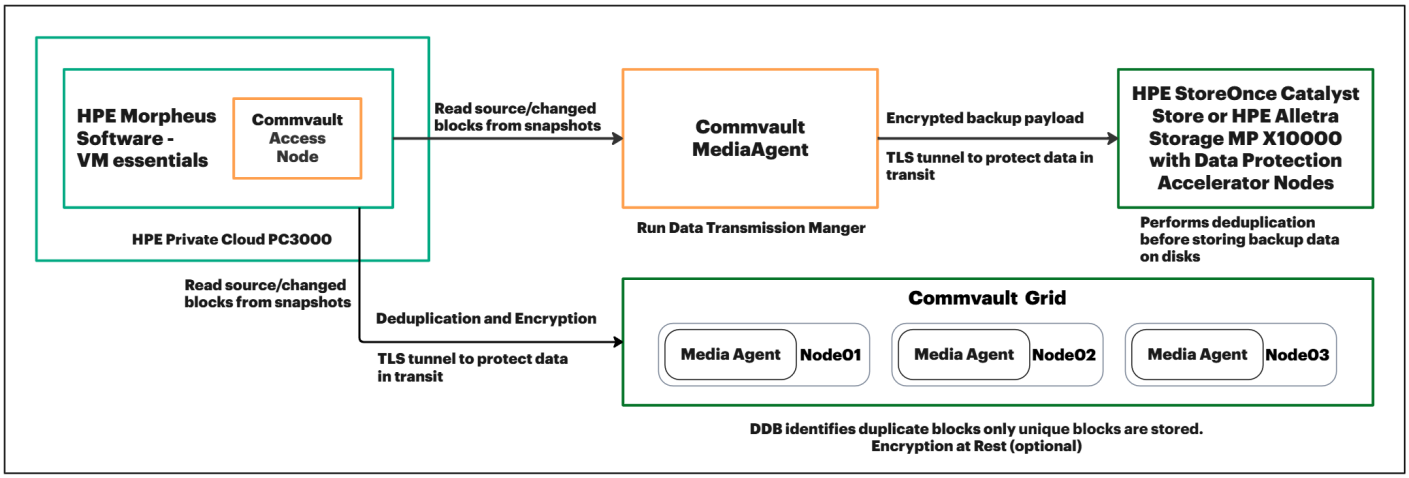



**Figure 5.** Backup workflow providing high security

## Security features of HPE Private Cloud PC3000 and backup infrastructure

The following sub sections capture the security capabilities available for PC3000 and proposed backup infrastructure.

### HPE Private Cloud PC3000

This describes the security and governance capabilities of HPE Private Cloud PC3000 based on features provided within the PC3000 platform and its integrated management services.

#### Role-Based Access Control (RBAC)

PC3000 implements built-in role-based access control (RBAC) to manage user permissions across infrastructure components and operations. The platform provides predefined roles such as:

— Private Cloud Business Edition Administrator

— Private Cloud Business Edition Operator

— Network Administrator

— Network Operator

These roles enforce granular access controls for operations such as cluster management, network configuration, and infrastructure changes.

**Credential and Secrets Management**

PC3000 uses a centralized secrets service to securely store and manage credentials across the platform. This includes credentials for:

— Server (iLO and host management)

— Hypervisor managers

— Storage systems

— Proxy and integration endpoints

Credentials are created, stored, and updated within the platform and are automatically synchronized with underlying components. Password complexity is enforced, requiring a mix of uppercase, lowercase, numeric, and special characters within defined length constraints.

A key governance control is that credential updates must be performed only through the PC3000 interface, as direct changes outside the system can result in authentication failures and loss of connectivity.

**Network Segmentation and Security Controls**

PC3000 provides network-level security through logical segmentation and controlled configuration of network resources during deployment. Network traffic is separated across:

— Management network

— iLO (out-of-band) network

— Data (iSCSI) networks

Network automation capabilities further validate switch configuration, cabling, and port assignments, helping prevent misconfiguration and ensuring consistent connectivity across the environment.

**Secure Integration and Management Services**

PC3000 integrates with cloud services through the Data Services Connector, which acts as a secure bridge between on-premises infrastructure and HPE Cloud services. Key capabilities include:

— Secure activation using one-time activation codes

— Controlled connectivity to management services

— Monitoring of data services connector health and status

— Support for remote diagnostics and support bundle generation

Remote support capabilities are enabled through controlled mechanisms, including explicit user actions and secure communication processes, ensuring secure interaction with support services.

**Commvault**

**Role-Based Access Control (RBAC) authentication**

Role-Based Access Control (RBAC) in Commvault should be implemented to enforce the principle of least privilege across the backup environment. This ensures that users and administrators have only the permissions required to perform their designated tasks.

Commvault RBAC is used to define granular permissions for:

— Backup configuration and policy management

— Restore and recovery operations

— Storage and data lifecycle administration

— Monitoring, reporting, and auditing

**Multi-Factor Authentication (MFA)**

To strengthen authentication security, Multi-Factor Authentication (MFA) should be enabled for all privileged and remote access to the Commvault environment. The use of MFA significantly reduces the risk of credential compromise, phishing attacks, and unauthorized access to backup and recovery functions.

You can use two-factor authentication (which is a form of multi-factor authentication) to add an extra level of security to the CommCell login requirements. Passwords alone might not provide enough security to protect your CommCell environment from unauthorized access.

When Two-Factor Authentication is activated, users must provide a 6-digit PIN (Personal Identification Number) along with their passwords in order to access the CommCell.

Commvault supports MFA through:

— Native MFA capabilities for CommCell Console and Command Center access.

— Integration with external identity providers (IdPs) supporting SAML 2.0 (e.g., Azure AD, Okta).

MFA is enforced for all administrative accounts and users with elevated privileges.

**Encryption (Data at rest and Data in transit)**

Encryption of Data in transit

All data movement within the backup environment should be protected using industry-standard encryption mechanisms (TLS 1.2t+). Encrypted communication paths include:

— HPE Morpheus VM essentials Clusters to Commvault MediaAgents

— MediaAgents to HPE StoreOnce (Catalyst protocol)

— MediaAgents to HPE Alletra Storage Server 4120 (Commvault Grid cluster)

TLS-based encryption in transit should be enforced for all backup, restore, replication, and management traffic to protect against interception and man-in-the-middle attacks.

Encryption of Data at rest

Backup data stored on HPE StoreOnce, HPE Alletra Storage Server 4120 (Commvault Grid), and HPE Alletra Storage MP X10000 is protected using hardware-based encryption at rest.

— Hardware-based encryption provides:

- Line-rate performance with no impact on backup or restore throughput
- Strong protection against physical media compromise
- Compliance with enterprise and regulatory security requirements

— Encryption is applied transparently at the storage layer, ensuring that all backup copies - primary and secondary - remain encrypted throughout their retention period.

— Encryption key management should align with enterprise security and compliance requirements, supporting centralized governance where applicable.

**Threat Scan**

Commvault Threat Scan delivers a unified solution that combines anomaly detection, threat scanning, and response actions to protect your backup data.

By leveraging AI-enabled threat intelligence, SOC analyst tools, and workload integrations, Threat Scan identifies and analyzes potential threats within backup environments. This approach helps organizations recover confidently to a clean state, while minimizing rollback and reducing operational risk.

Threat Scan offers the following features:

— Flexible scan modes: Supports scheduled scans, exception-based scans, post-restore scans, and on-demand scans.

— Comprehensive coverage: Works with VM backups, objects, NAS, and file-level data.

— Advanced threat detection: Includes HASH and YARA-based IOC scanning for precise threat identification.

— AI-powered assistance: Provides AI-driven insights and actionable recommendations.

— Cleanroom compatibility: Fully interoperable with Commvault cleanroom environments for secure analysis.

— Automated recovery: Enables synthetic recovery for clean, automated restoration.

— Cloud-native design: Offers full SaaS capabilities for scalability and ease of use.

### HPE StoreOnce

#### Access control and identity security

HPE StoreOnce provides identity and access controls that strengthen administrative security for the backup storage environment.

— Multi-factor authentication (MFA): StoreOnce supports MFA for console access by using an authenticator app to generate a temporary 6-digit one-time password (OTP) for user verification.

— Dual Authorization: StoreOnce requires approval from two authorized users for sensitive administrative actions, such as deleting a Catalyst store.

— Single Sign-On / directory integration: StoreOnce integrates with Microsoft Active Directory and other enterprise identity systems to provide centralized authentication and enforce least privilege access for users and service accounts.

#### Encryption

HPE StoreOnce provides encryption capabilities that protect backup data at rest and in transit using native or external key manager.

— Data at rest: StoreOnce protects backup data stored on disk using AES-256 encryption. This can be enabled for Catalyst stores, NAS shares, and virtual tape libraries (VTLs).

— Data in transit: StoreOnce protects data moving over the network using IPsec encryption.

— Key management: StoreOnce supports both a local key manager and integration with external key managers for encryption key control. For compliance-focused environments, it also supports cryptographic modules validated for FIPS 140-2.

---

**Note**

To preserve HPE StoreOnce deduplication efficiency, it is recommended to disable encryption at the source (Commvault) and enable it only on HPE StoreOnce. Double encryption can also increase CPU overhead and complicate key ownership.

---

#### Immutability

HPE StoreOnce provides immutable backups that makes backup files read-only for a defined retention period and prevents deletion or modification of backup files. This protects against ransomware attacks or accidental deletion of backups.

HPE StoreOnce supports two immutability modes:

— ISV-controlled immutability: The backup application, such as Commvault, sets retention for each backup.

— Server-controlled immutability: StoreOnce enforces a single retention period for the entire store.

#### HPE Alletra X10000 with Data Protection Accelerator Nodes

#### Access Control and Identity Security

HPE Alletra Storage MP X10000 provides identity and access controls that strengthen administrative security for the backup storage environment through:

— Multi-factor authentication (MFA): HPE Alletra Storage MP X10000 supports MFA for console access by using an authenticator app to generate a temporary 6-digit one-time password (OTP) for user verification.

— Single Sign-On / directory integration: HPE Alletra Storage MP X10000 integrates with Microsoft Active Directory and other enterprise identity systems to provide centralized authentication and enforce least-privilege access for users and service accounts.

#### Encryption

HPE Alletra Storage MP X10000 provides encryption capabilities that protect backup data at rest and in transit.

— Data at rest: HPE Alletra Storage MP X10000 protects backup data stored on disk using AES-256 encryption. This can be enabled for S3 object buckets created on the platform.

— Data in transit: HPE Alletra Storage MP X10000 protects data moving over the network using IPsec encryption.

#### Immutability

HPE Alletra Storage MP X10000 supports immutable backup storage to protect backup data from deletion or modification during the defined retention period. This helps defend against ransomware and accidental data loss.

For S3-compatible object storage repositories, immutability is enforced using Object Lock and Write Once Read Many (WORM) policies configured at the bucket level on HPE Alletra Storage MP X10000.

# Operations and monitoring

## Scalability

#### Scalability of HPE Private Cloud PC3000

PC3000 is a single-rack solution that includes HPE Alletra Storage MP, out-of-band management switches, top-of-rack switches, and HPE ProLiant DL360 or DL380 or DL325 Gen11/Gen12 servers. These HPE ProLiant DL servers can be used to deploy HPE Morpheus Software-VM essentials.

PC3000 can support up to 8 HPE Morpheus Software-VM essentials clusters and 16 servers per cluster. This cluster or node level scalability is decided based on rack units available in PC3000 for expansion.

### Scalability of Commvault components

The proposed data protection solution is architected to scale seamlessly in line with business growth, supporting both performance and capacity expansion without service disruption. Scalability is achieved through modular scale-up mechanisms across the data protection stack, including compute and storage tiers.

#### CommServe

The CommServe scales using a vertical (scale-up) model, as it functions as the centralized control plane responsible for orchestration, job scheduling, and configuration management rather than data movement. Its scalability is achieved by increasing CPU and memory in line with the number of protected workloads and concurrent jobs.

#### MediaAgent

— MediaAgent Servers in Commvault scale through a combination of vertical (per-node) and horizontal (multi-node) scaling, driven primarily by concurrency of tasks rather than just infrastructure size.

— Scaling up is achieved by increasing CPU and memory on each MediaAgent to support higher task concurrency, while scale-out is achieved by deploying additional MediaAgents to distribute the workload.

### Scalability of backup storage tier

#### HPE StoreOnce Scale-up

HPE StoreOnce systems span from an entry-level 18 TB model to an enterprise class model with over 1 PB that can be expanded over 3 PB usable capacity with Cloud Bank Storage. HPE StoreOnce deduplication can be extended to cloud and on-premises object storage to create a hybrid backup infrastructure to increase capacity and reduce the cost of backup data that requires extended retention times. HPE StoreOnce has no limit on objects in store; scales up to capacity of appliance; grows as needed.

#### HPE Alletra Storage MP X10000 Scale-out

HPE Alletra Storage MP X10000 uses a scale-out architecture, making it ideal for primary backup storage in growing environments. Capacity and performance are expanded by simply adding nodes to the cluster, without downtime or reconfiguration. Its disaggregated design allows independent scaling of data nodes to increase storage capacity and compute nodes (Data Protection Accelerator Nodes) to handle concurrent backup streams and S3 requests.

As nodes are added, the system automatically integrates them into a global namespace and redistributes data, delivering linear growth in throughput, capacity, and concurrency. This ensures consistent performance even as backup volumes and workloads increase. For backup use cases, this means HPE Alletra Storage MP X10000 can efficiently support parallel ingest from multiple backup jobs, scale to petabyte levels, and adapt to future growth-providing a cloud-like, elastically scalable backup repository on-premises.

## Monitoring

### HPE Private Cloud PC3000

PC3000 provides integrated monitoring and validation capabilities to ensure system health and compliance. The dashboard available on HPE GreenLake Data Services Cloud Console offers visibility into:

— System health, capacity, and utilization

— Virtual machine performance and resource consumption

— Infrastructure issues and alerts

Additionally, system configuration checks are executed automatically every 24 hours or can be triggered manually. These checks validate components such as:

— Hosts and clusters

— Datastores

— Network and connectivity

— Hypervisor managers

This continuous validation helps identify configuration drift, operational risks, and compliance issues proactively.

**Monitoring using HPE OpsRamp**

HPE OpsRamp provides a hybrid observability platform for integrating diverse organizational tools and applications, offering a single interface to view and monitor events across the IT infrastructure. HPE OpsRamp continuously collects and correlates metrics to provide real-time operational insights into system availability, storage latency and throughput, capacity thresholds, and component health i.e., CPU, memory, and storage utilization trends.

This enables operations teams to proactively address performance degradation before backup SLAs are impacted. HPE OpsRamp delivers end-to-end monitoring across all architectural layers including:

**HPE Storage Infrastructure**

— HPE StoreOnce

— HPE Alletra Storage MP X10000

**Commvault**

HPE OpsRamp integration with Commvault delivers visibility into and management of key resources, including CommServe, MediaAgent, and Backup repositories, leveraging CommServe.

The list of supported metrics for Commvault is available here: Commvault | OpsRamp Documentation.

# Support and maintenance

This section covers life cycle management of HPE Private Cloud PC3000 and backup infrastructure including Commvault, HPE StoreOnce, and HPE Alletra Storage MP X10000.

## Lifecycle management (firmware and software)

Lifecycle management follows a controlled, non-disruptive upgrade approach across all solution components.

**HPE Private Cloud PC3000**

PC3000 provides full stack lifecycle management and enforces governance through controlled lifecycle management and standardized update workflows. Software updates are delivered through validated catalogs that include:

— Storage operating system

— Hypervisor components

— Firmware and drivers

— Management services such as DSC and HPE Morpheus Manager

Before updates are applied, the platform requires a precheck validation, which verifies connectivity, system health, and readiness for upgrade. Updates proceed only after all blocking issues are resolved, ensuring system stability and compatibility. This approach provides controlled auditable updates, reduces operational risk, and maintains consistent software stack across infrastructure.

**Commvault Software**

Commvault software updates and feature upgrades are planned and executed in alignment with:

— Vendor support matrices

— Compatibility with HPE Morpheus Software-VM essentials

— Storage platform interoperability

The Commvault distributed architecture, consisting of the CommServe, MediaAgents, Access Nodes, and protected clients, supports phased software upgrades across the CommCell environment. Components can be upgraded individually or by server groups while maintaining compatibility between supported versions. This approach enables organizations to upgrade large-scale environments incrementally, reducing operational impact and minimizing disruption to backup and restore activities.

**Storage platforms**

— HPE StoreOnce and HPE Alletra Storage MP X10000 firmware updates need to be performed according to HPE recommended practices. HPE provides non-disruptive upgrade capabilities that minimize impact to ongoing backup and restore operations.

— Firmware lifecycle planning ensures continued vendor support, security patch compliance, and feature parity across storage tiers.

# Limitations and known issues

The following limitations and known issues should be considered when designing and deploying Commvault with HPE Private Cloud PC3000 and HPE Morpheus Software-VM essentials:

Since PC3000 is an engineered system, it enforces several guardrails around the stack components. Specifically, on the HVM hosts, root SSH login is disabled, and no root user account is exposed to customers. HPE support is needed to deploy Commvault access node packages on HVM nodes

PC3000 supports iSCSI protocol only for storage connectivity. FC and NVMeOF are not currently supported with PC3000.

PC3000 supports only management network and iSCSI storage networks by default for HPE Morpheus Software-VM essentials cluster and restricts user from adding additional networks during initial deployment. Any additional networks can be created with assistance of HPE Support.

HPE Alletra Peer Persistence is supported for PC3000 with only VMware vSphere platform.

Currently, only GFS2-backed shared datastores are supported for HVM clusters; HPE Alletra plugin-based direct-disk datastores are not supported.

# Summary

This reference architecture provides detailed design guidance for an on-premises enterprise data protection solution integrating Commvault with HPE Private Cloud PC3000, based on a modular and scalable architecture.

The solution supports tiered backup storage leveraging HPE StoreOnce, Alletra Storage MP platforms, and HPE Storage Tape, and includes network design considerations for performance and security. It also addresses cyber resilience capabilities, such as immutability and encryption, and outlines deployment and configuration best practices.

# Resources and additional links

HPE Reference Architectures
hpe.com/info/ra

HPE servers
hpe.com/servers

HPE Storage
hpe.com/storage

HPE Networking
hpe.com/networking

HPE Technology Consulting Services
hpe.com/us/en/services/consulting.html

Advisory and Professional Services
hpe.com/us/en/services/consulting.html

**Documentation feedback**
Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the Feedback button and icons (located at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (hpe.com/support/hpesc) to send any errors, suggestions, or comments. All document information is captured by the process.

Visit HPE.com

Chat now

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.
Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. All third-party marks are property of their respective owners.

a50016030enw

HEWLETT PACKARD ENTERPRISE

HPE.com