Reference Architecture for HPE Morpheus Software—VM Essentials based HPE Private Cloud PC3000 Data Protection with Veeam

Contents

Executive summary 5

Target audience 6

Solution overview 6

- Solution portfolio 7
  - HPE Private Cloud PC3000 7
  - Veeam Backup Server core components 7
  - Primary backup storage 8
  - Secondary and archive storage 9
  - Network switches 10

Design principles and requirements 10

- Solution scope (in scope / out of scope) 10
- Data protection strategy 11
  - Adherence to 3:2:1 backup strategy 11
  - Comprehensive protection of data and configuration 12
  - Backup recovery objectives (RPO / RTO) 13

Compatibility (firmware and software versions) * 13

Integrated solution architecture 14

Connectivity and design decisions 16

- Integration of HPE Private Cloud PC3000 with Veeam Backup Server 16
  - Layer 2 (L2) network Integration 17
  - Layer 3 (L3) network integration 18
- Veeam Backup Server in the HPE Private Cloud PC3000 rack 19
- Veeam transport modes 19
- HPE StoreOnce vs HPE Alletra Storage MP X10000 with data protection accelerator nodes 19

Deployment and configuration guidance 20

- HPE Private Cloud PC3000 (HPE Morpheus Software—VM essentials) 20
  - Compute 21
  - Network 21
  - Storage 21
  - Deployment and automation guidance 21
- Veeam Backup Server Components 22
  - Veeam Backup Server 22
  - Veeam backup proxies / worker VMs 23

Gateway servers 23
Mount server 24
HPE StoreOnce 24
HPE Alletra X10000 25
RPO and RTO reference guidelines 26
Hardware Architecture and Bill of Materials 26
HPE Private Cloud PC3000 26
Compute tier (HPE ProLiant DL for Veeam Backup Server) 27
Backup target tier 27
Primary backup HPE StoreOnce 27
Primary backup HPE Alletra Storage MP X10000 27
Security and governance 28
Security design scenarios 28
On-site backups requiring maximum deduplication efficiency 28
Off-site backups requiring high security during transit 29
On-site or off-site backups requiring protection against ransomware and insider threats 29
Security features of HPE Private Cloud PC3000 and backup infrastructure 30
HPE Private Cloud PC3000 30
Veeam 31
HPE StoreOnce 32
HPE Alletra X10000 with Data Protection Accelerator Nodes 33
Operations and monitoring 33
Scalability 33
Scalability of HPE Private Cloud PC3000 33
Scalability of Veeam Backup Server components 33
Scalability of backup storage tier 34
Monitoring 35
HPE Private Cloud PC3000 35
Monitoring using HPE OpsRamp 35
Support and maintenance 36
Lifecycle management (firmware and software) 36
HPE Private Cloud PC3000 36
Veeam Backup Server 36
Storage platforms 36
Limitations and known issues 37

Summary 37
Resources and additional links 38

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 HPE 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 primarily available through an OpEx based HPE GreenLake Flex consumption model, helping organizations avoid significant upfront capital costs.

This reference architecture describes a data protection solution for **HPE Private Cloud PC3000** built with **Veeam Backup Server (Veeam Software Appliance)** as part of the **Veeam Data Platform**. Veeam Backup Server serves as the central data protection platform that orchestrates backup, recovery, replication, and retention policies across virtual, physical, cloud, and application workloads. In this solution, Veeam 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 StoreEver 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.

Veeam Backup Server provides the centralized control plane that governs job orchestration, policy enforcement, configuration, and metadata handling, while other Veeam core components including backup proxies, gateway servers, and mount servers —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 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 Veeam Backup Server 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 **Veeam Backup Server** 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 Veeam Backup Server is deployed externally to the PC3000 rack using an advanced deployment model, 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 Veeam components—including worker VMs, gateways, and mount VMs—enabling independent scaling to sustain performance and operational flexibility as workloads grow. Veeam's host-based protection provides agentless, image-level backups for workloads running on PC3000, specifically within 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 Veeam Software Appliance. 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 **Veeam Backup Server** 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 Veeam, HPE StoreOnce, and HPE Alletra 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 Veeam's 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, Veeam Backup Server and its components, HPE Storage platforms such as HPE StoreOnce, HPE Alletra 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 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 Private Cloud 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.

Veeam Backup Server core components

This section describes the core components of the Veeam Backup Server, 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.

Veeam Backup Server

Veeam Backup server can be deployed either as a hardened Linux based Veeam Software Appliance or as a Veeam Backup and Replication server on Windows.

This reference architecture uses Veeam Software Appliance which is delivered as a preconfigured Linux-based software appliance using the Veeam-supplied ISO. It serves as the central control plane for backup and restore operations. This Linux based appliance combines operating system, security hardening, and application services in a single stack and aligns well with environments that prioritize security consistency, operational standardization, and reduced maintenance complexity.

Veeam Backup Windows Console

The Veeam Backup Windows Console is the administrative client used to manage and monitor the Veeam environment. It is installed on a local Windows machine and connects remotely to the Veeam Backup Server, allowing administrators to configure backup and recovery jobs, manage repositories, and perform restore operations.

Note

For HPE Morpheus Software—VM essentials, the Veeam Web UI does not support backup job creation or management, and these operations must be performed using the Veeam Backup Windows Console.

For more details refer to the link: https://helpcenter.veeam.com/docs/vbr/userguide/web_ui_limitations.html.

Veeam Plug-in for HPE Morpheus Software—VM essentials

The Veeam Plug-in for HPE Morpheus Software—VM essentials provides integration between Veeam Backup Server and the HPE Morpheus Software—VM essentials. This plug-in enables Veeam to communicate directly with the HPE Morpheus Manager to help synchronize application-consistent checkpoints and supervises the execution of backup and restore workflows.

Backup proxy / worker

Workers are Linux-based lightweight proxy VMs that process backup workloads when transferring data to and from backup repositories. Workers are installed on the HPE Morpheus Software—VM essentials cluster and are bought online only for the duration of a backup or restore operation and can handle data-plane operations, including Changed Block Tracking (CBT), inline deduplication, and compression.

Gateway Server

Gateway Server is a backup infrastructure component that hosts the Veeam Data Mover service used to facilitate data movement between backup proxies/workers and backup repository targets. It acts as a transport bridge for backup and restore operations and can also be used to connect source and target backup repositories for backup copy workflows.

A gateway Server is usually deployed when integrating with systems like HPE StoreOnce Catalyst or other repositories that require an intermediary system for data handling since they cannot host the Veeam data mover locally.

Mount Server

Mount Server is responsible for enabling advanced recovery capabilities required for guest OS files and application items and is typically positioned close to the backup storage tier to ensure low-latency access to backup data.

To access files or applications stored in a backup file, Veeam Backup server mounts the content of the backup to the mount server. Only after the content is mounted, Veeam can access the files or applications and copy them to the restore destination.

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:** HPE StoreOnce performs high-efficiency, target-side deduplication and compression, storing only unique data blocks.

— **Veeam Gateway-based integration:** Backup data from Veeam backup proxies is sent to HPE StoreOnce through a Gateway Server, which is required because HPE StoreOnce cannot host Veeam Data Movers directly.

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

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

During backup operations, Veeam connects the Data Mover on the proxy to the Data Mover on the Gateway to enable efficient backup data transfer. Together, these components provide a secure, high-performance, and storage-efficient backup architecture for large and performance-sensitive environments.

HPE Alletra Storage MP X10000 with Data Protection Accelerator Nodes

HPE Alletra Storage MP X10000 serves as an object-based primary backup storage tier and by using its native S3-compatible interface, it provides scalable, high-performance, all-flash object storage for modern data protection environments.

Key design characteristics

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

— **Flexible data transfer:** Veeam Backup proxies / Worker nodes can send data either directly to object storage or through a gateway server using Veeam Data Movers for transport.

— **Veeam-managed repository behavior:** The object storage repository must fully support S3 API operations and is managed exclusively by Veeam for retention and lifecycle policies. External lifecycle changes can create backup and restore inconsistencies.

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

During backup operations, Veeam connects the Data Mover on the proxy/worker to HPE Alletra Storage MP X10000 object storage repositories directly or through the Data Mover on the Gateway to enable efficient and high throughput backup data transfer.

Secondary and archive storage

HPE Storage Tape

HPE Storage Tape (StoreEver) is integrated with Veeam as a secondary backup tier, providing a cost-effective and secure solution for long-term retention. Veeam 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. Veeam 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, Veeam Backup Server components, and primary backup storage tier.

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

Design principles and requirements

This section outlines the foundational design principles governing the backup architecture leveraging HPE Infrastructure and Veeam Backup Server.

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 Veeam
2. On-site Layer 2 / Layer 3 network integration of HPE Private Cloud PC3000 with the Veeam Backup Server
3. Position HPE storage platforms (HPE Alletra and HPE StoreOnce) to deliver production workload storage and backup repository tiers within the Veeam architecture
4. Hardware architecture and Bill of Materials (BOM)
5. Deployment and configuration best practices for integrating Veeam Backup Server with HPE Private Cloud PC3000 and HPE storage platforms
6. Monitoring Veeam 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 Veeam 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)

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 copies and recovery validation to mitigate modern cyber threats.

— As part of an offline or air-gapped backup, HPE Storage Tape or HPE Cloud Bank can be used to maintain an offline/immutable secondary copy of backup data.

— To ensure zero restore errors, backup recovery validation should be done in regular intervals using Veeam features like Instant VM Recovery.

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, Veeam does not support storage snapshot integration 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

Veeam 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 Veeam Backup Server or from primary storage tier such as HPE StoreOnce or HPE Alletra Storage MP X10000.

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 Veeam Backup Server 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

— Veeam Backup Server configuration

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

Veeam configuration and metadata protection

Veeam Backup Server protects its configuration through a built-in configuration backup mechanism, which captures data from the Veeam configuration database and stores it as a backup file (in BCO format) in one of the chosen repositories configured on Veeam. This ensures that the backup system itself can be fully restored in the event of backup infrastructure failure, corruption or loss.

This configuration backup creates a consistent point-in-time snapshot of the Veeam configuration database and includes all critical components required to rebuild the Veeam environment:

— Backup infrastructure components such as backup servers, proxies/workers, gateways, and mount servers

— Backup jobs, backup copies, replicas, and policies

— Session history and operational data

— Tape configuration, libraries, media pools and catalogues

— Credentials and access control settings.

Note

Veeam configuration backups must be stored on a separate repository, independent of the Veeam Backup Server, to eliminate single points of failure. HPE StoreOnce catalyst can be leveraged as the target repository to store Veeam configuration since it provides secure and centralized storage integrated with enterprise backup policies.

Even though the configuration backups of Linux-based Veeam Backup Servers can be sent to HPE StoreOnce repositories via the Catalyst protocol, StoreOnce do not support configuration restore by direct file-level access of backup files (such as *.bco) from Veeam Linux Management UI. Therefore, for Linux-based Veeam Backup Server, it is recommended to store Veeam configuration backups on a standard, easily accessible storage location such as an SMB/NFS share or local directory, rather than on deduplicating storage like HPE StoreOnce.

For more information on creating configuration backups for Veeam refer to the link: https://helpcenter.veeam.com/docs/vbr/userguide/export_vbr_config.html?ver=13

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) *

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

Veeam Backup Server

Table 2. Veeam Backup Infrastructure

Type	Version	Image file
Veeam Backup Server	13.0.2.29	VeeamSoftwareAppliance_13.0.2.29_20260523.iso
Veeam Plug-in HPE Morpheus Software—VM essentials Build	13.1.1.10	veeam-platform-service-hpemorpheusvme-13.1.1.10-0.el9.x86_64.bndl
Veeam Backup Windows Console	13.0.2.29	VeeamBackup&ReplicationConsole_13.0.2.29.exe

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 Veeam Backup Server
HPE StoreOnce	4.3.x 5.2.x	4.x for Gen 4 appliances 5.x for newer Gen 5 appliances
HPE Alletra Storage MP X10000	10.5.x	

Hypervisors for backup infrastructure

Table 4. Virtualization platform supported with Veeam Backup Server

Component	Supported Version	Recommended Version	Notes
HPE Morpheus Software—VM essentials	8.0.13 or later	8.1 or later	Recommended for virtual form factor deployment of Veeam Backup Server and its core components.

*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

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 Veeam based backup solution designed for HPE Morpheus Software—VM essentials workloads running on PC3000.

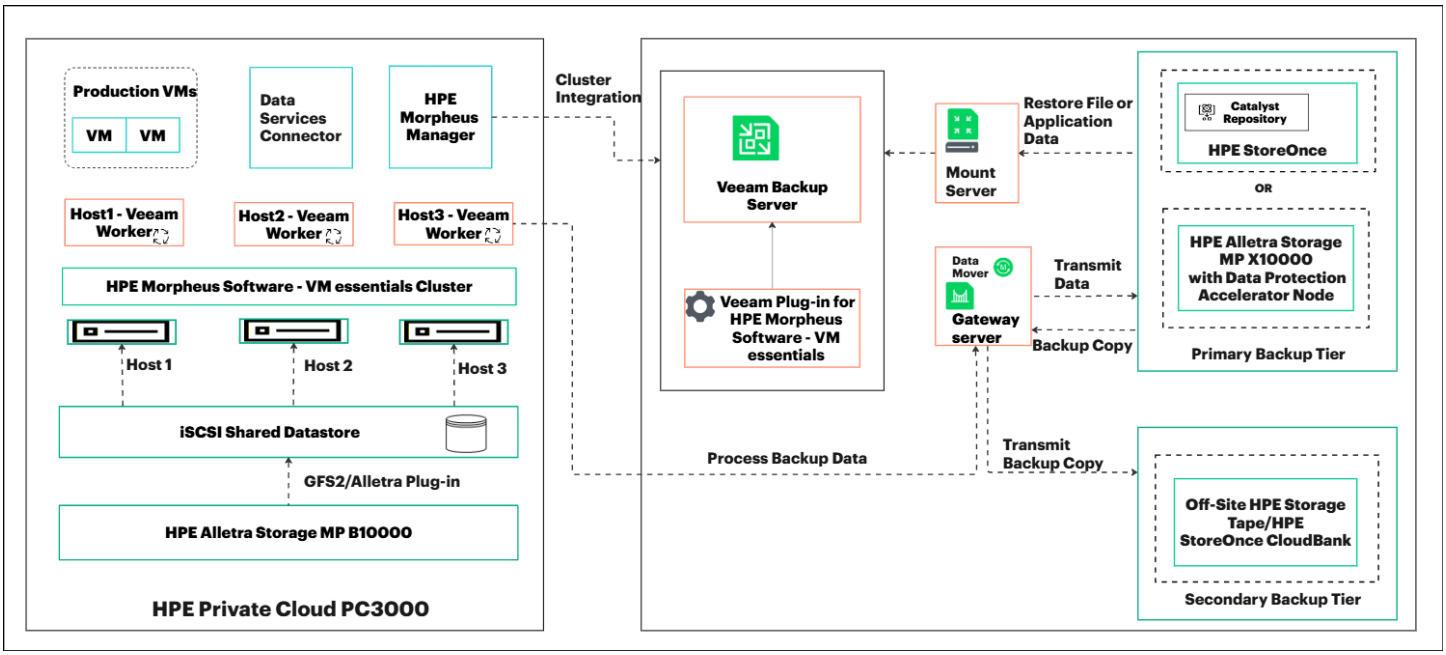


Figure 1. High-level logical architecture for a Veeam-based backup solution integrated with HPE Private Cloud PC3000

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 the datastores can be GFS2 or HPE Alletra Plugin based that enable concurrent access from multiple hosts, ensuring consistent and 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 Veeam Backup Server, deployed as a Linux-based software appliance that 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 Veeam Backup Windows Console, which provides the interface for configuring and monitoring backup and restore operations. To enhance resiliency and security, the Backup Server is 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.

The Veeam Plug-in for HPE Morpheus Software—VM essentials integrates Veeam with the virtualization layer by enabling direct communication with HPE Morpheus Manager. This integration gives Veeam visibility into managed resources and supports policy-driven protection for virtual machines running in the PC3000 environment.

Veeam Worker VMs handle backup and restore data movement. These Linux-based virtual machines run within the HPE Morpheus Software—VM essentials cluster and act as proxies that read VM data from the shared datastore, process it, and transfer it to the backup repository via Gateway server. In case of low bandwidth/high latency connectivity (Ex: WAN) between Veeam gateway and backup storage tier, Veeam gateway server can be hosted close to Veeam worker VM and in case of high bandwidth/low latency connectivity between Veeam Gateway and backup storage tier, Veeam gateway server can be hosted close to the backup storage tier. File level and application level restore requires a mount server to mount the content of the back up data before it can be restored by the Veeam Backup Server. The backup and restore data path are handled by the Veeam worker VMs,

Gateway Server, and Mount Server which collectively manages data transport, optimizes communication with backup storage tiers, and enables recovery operations.

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.

  For HPE StoreOnce Catalyst integration, the gateway server is a must to host the data movers to manage communication with the StoreOnce appliance, as StoreOnce cannot host Veeam data movers on its own. The gateway performs the target-side data movement, enabling backup proxies/workers to transfer data to StoreOnce, while handling session management and protocol translation between Veeam components and StoreOnce catalyst repository.

— 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 use of a gateway server is optional. To transfer data to S3-compatible object storage, Veeam Backup Server supports two modes:

  - Direct mode: Backup proxies send data directly to object storage (preferred for simplicity and performance when target object storage repository is located locally to backup data source)
  - Gateway mode: A gateway server is used to transfer data from proxies/workers to object storage, acting as an intermediary for data movement

For extended retention and compliance use cases, HPE Storage Tape or HPE Cloud Bank can be added as a secondary backup tier to Veeam Backup Server. Backup copy jobs are orchestrated through Veeam Backup Server to transmit already protected data from the primary backup tier to these secondary backup targets for long-term retention and air-gapped protection.

Note

By default, HPE Private Cloud PC3000 has a 2TB GFS2 datastore created for monitoring cluster heartbeat and storing Virtual machine images. It is recommended to create a another GFS2 datastore on PC3000 to store the temporary snapshots created by Veeam Backup Server during backup operations as HPE Alletra Block Storage datastore type is not yet supported for storing VM snapshots. To ensure GFS2 datastore has sufficient space for snapshot creation, it should be sized considering the number of backup jobs that can run concurrently along with the size of all the VMs that will be part of the backup job.

Connectivity and design decisions

Integration of HPE Private Cloud PC3000 with Veeam Backup Server

This section covers both layer 2 (L2) and layer 3 (L3) network integration designs of PC3000 rack with **Veeam Backup Server** 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 Veeam Backup Server 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 Veeam Backup Server 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.

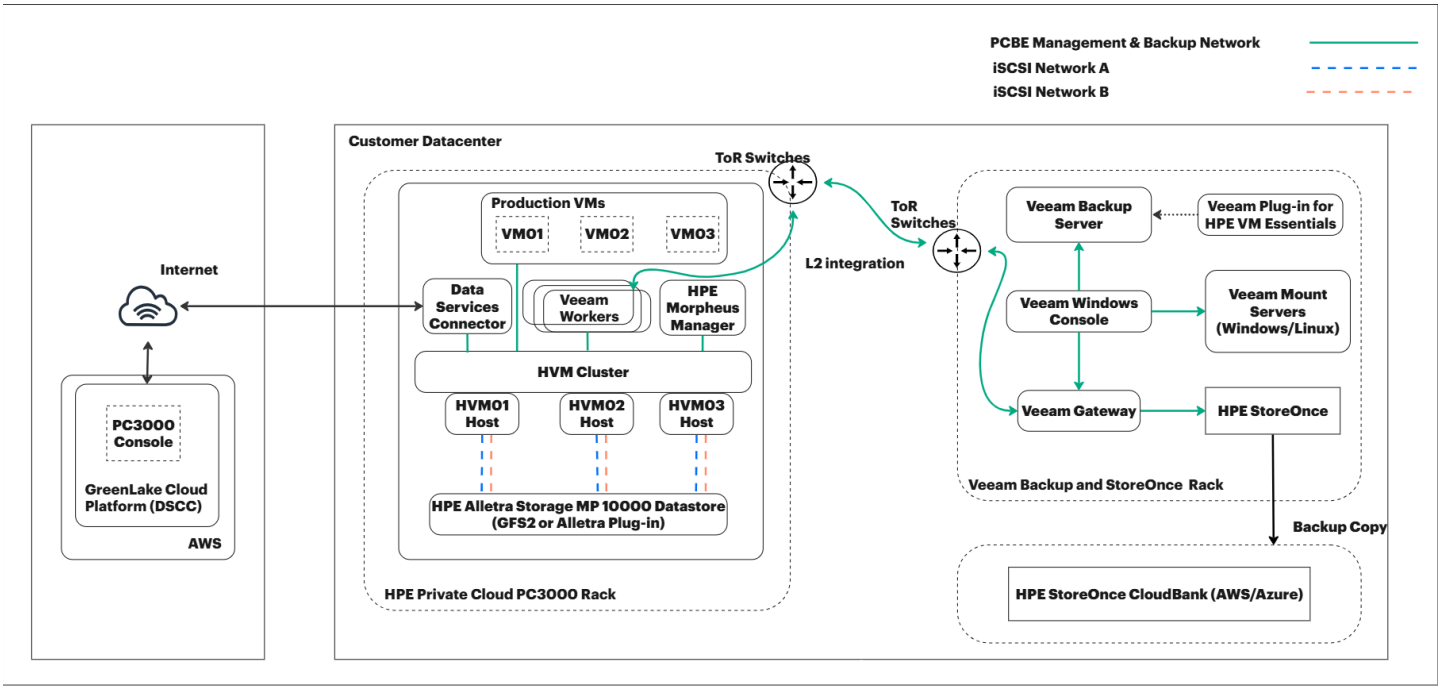


Figure 2 Layer 2 integration of HPE Private Cloud PC3000 rack with external Veeam Backup Server

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

Note

By default, PC3000 with HPE Morpheus Software—VM essentials cluster supports only management VLAN and ICSI storage VLANs during deployment. In this integration, PC3000 management VLAN is also leveraged as the backup VLAN across both the PC3000 rack and the Veeam 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 Veeam Workers can directly communicate with the Gateway 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.

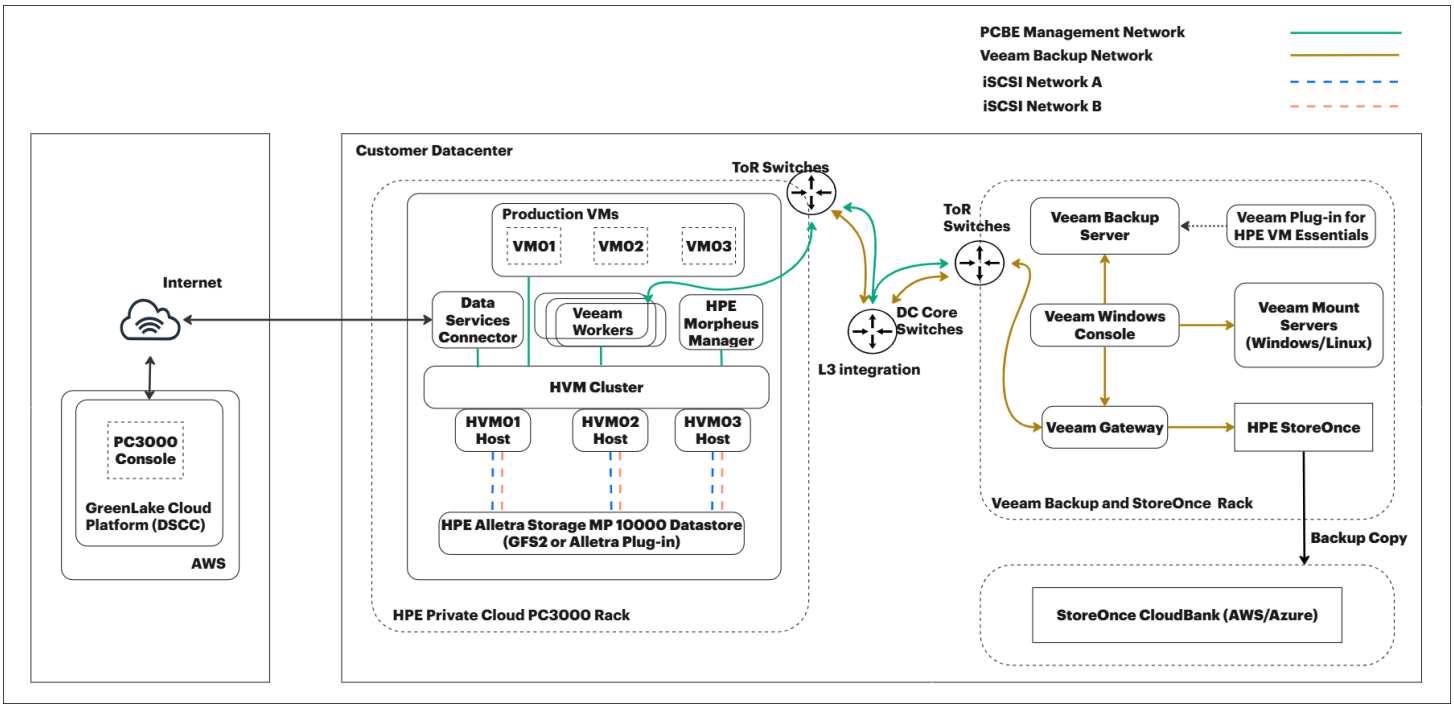


Figure 3. Layer 3 integration of HPE Private Cloud PC3000 rack with external Veeam Backup Server

Layer 3 integration is implemented by routing backup traffic between the PC3000 rack and the dedicated Veeam backup rack through the DC Core switches. Separate subnets are used for the PC3000 management network and the Veeam 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 ICSI storage VLANs during deployment. In this integration, PC3000 management VLAN is also leveraged as the backup VLAN in the PC3000 rack and routes to Veeam Backup VLAN in the Veeam 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.

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 Veeam Workers, Gateway, and HPE StoreOnce components. Backup traffic generated by the Veeam Workers is routed through the Layer 3 core network to the Veeam Gateway 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.

Veeam Backup Server in the HPE Private Cloud PC3000 rack

If hosting Veeam Backup Server in a separate rack outside of PC3000 is not an option, then Veeam Backup Server could be added to the PC3000 Rack itself (either as a bare metal server or a virtual machine) outside of the PC3000 with HPE Morpheus Software—VM essentials cluster.

This placement protects Veeam Backup Server 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 Veeam fault domain from the PC3000 with HPE Morpheus Software—VM essentials cluster.

Note

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

Veeam transport modes

Veeam supports two transport modes with HPE Morpheus Software—VM essentials:

1. Network Block Device (NBD) mode: In NBD mode, backup data is transferred over the LAN network from the hypervisor host to the Veeam worker VMs. It is generally preferred for its simplicity which does not require direct storage access.
2. HotAdd mode: In HotAdd mode, source VM disks temporarily attach to the Veeam worker VM allowing direct access to backup data. This mode requires Veeam workers to have access to the same storage as the protected VMs and typically delivers higher performance than NBD mode.

Note

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 5. 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.
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. Depending on when PC3000 servers are shipped, it supports PC Installer version 2.0.4.1 or earlier and 2.0.7.1 or later versions.

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

Veeam Backup Server Components

Veeam Backup Server

— Deploy the Veeam Backup Server outside the PC3000 with HPE Morpheus Software—VM essentials cluster it protects to maintain clear separation between backup management functions and production workloads.

— Choose the appropriate deployment form factor for the Veeam Backup Server:

- **Physical**: Recommended for large to extra-large environments with high backup throughput requirements or where compliance constraints limit the use of virtualization platforms. To ensure resilience and operational continuity, High Availability (HA) must be implemented at the backup server level, eliminating single points of failure within the backup infrastructure.
- **Virtual**: Best suited for small to large environments where backup operations are not highly latency sensitive. This model is generally preferred due to its operational simplicity and ease of maintenance. High Availability is achieved by leveraging the underlying hypervisor platform's native HA capabilities to ensure continuous availability of the backup server.

— While Veeam simple deployment model may be adequate for smaller environments and PoC validation purposes, it is not recommended for production environments. Veeam advanced deployment model should be adopted, as it supports both scale-up and scale-out growth strategies, ensures better task concurrency, and mitigates the risk of performance bottlenecks as workload demands increase.

— Enable and encrypt Veeam configuration backups, store configuration backup copies offsite to protect the Veeam server and its database to ensure full recovery capability in case of failure.

— For optimal performance, the Veeam Backup Server should be positioned to ensure:

- low-latency access to the PC3000 HPE Morpheus Manager and the worker VMs.
- low latency and high bandwidth connections to HPE StoreOnce catalyst repositories or HPE Alletra Storage MP X10000 object storage.

Note

For virtual machines that require application-consistent backups, QEMU Guest Agent must be installed on protected virtual machines before enabling Veeam Plug-in for HPE Morpheus Software—VM essentials quiescence functionality in the backup job.

Veeam Backup Server High Availability

Veeam Backup Server High Availability (HA) refers to a design approach that ensures Veeam backup services remain continuously available even if the underlying infrastructure fails. It is generally recommended to implement high availability when the Veeam Backup Server is deployed on a physical server, as a single physical instance

represents a single point of failure. When deployed as a virtual machine on a virtualization platform, cluster-level HA mechanisms typically ensure the availability of the Veeam Backup Server.

— Two physical servers are required to implement Veeam high availability in an active standby mode. Both servers participating in HA must run the same Veeam Backup Server version.

— Same DNS suffix and DNS settings should be configured on both servers.

— Veeam local disk repositories are not supported in the Veeam HA cluster and should be deleted before configuring HA. External shared backup repository should be added to both servers.

— Veeam HA cluster should be managed using cluster virtual IP and not using individual server IP.

Note:

Veeam HPE Morpheus VME Service is not properly managed for High Availability. Ensure to stop and start the service manually when creating a Veeam High Availability cluster and during switch and failover scenarios.

To know more about limitations of Veeam high availability, refer https://helpcenter.veeam.com/docs/vbr/userguide/high_availability_limitations.html

---

Veeam backup proxies / worker VMs

— Deploy dedicated backup proxy/worker VM on each node of the hypervisor cluster to improve overall backup performance.

— Place backup proxies / workers close to the data source (hypervisor and primary production storage) to minimize latency and optimize data transfer.

— Ensure backup proxies / workers have proper access to required datastores and limit access to only relevant storage to reduce scan time for Change Block Tracking.

— Configure appropriate concurrency (tasks per proxy) based on CPU and memory resources to maximize throughput without overloading the proxy

— Prioritize high-speed network (10 GbE or higher) for source connectivity.

- Source-to-proxy / worker path carries uncompressed data (100% of data size)
- Proxy / worker-to-repository sends optimized data (~50%)

— Avoid any manual changes to worker VM in HPE Morpheus Software—VM essentials cluster, this can lead to instability or failures

— Choose optimal transport mode:

- **HotAdd**: Preferred for virtualized environments
- **Direct Storage Access (SAN)**: Provides highest performance when available
- **NBD**: can be a fallback option if HotAdd or SAN mode are not supported.

Gateway servers

— Gateway servers are mandatory when leveraging HPE StoreOnce as backup storage tier, since StoreOnce cannot host Veeam Data Movers on its own and therefore requires a gateway to act as the target data mover.

— Deploy multiple gateway servers and enable automatic selection for gateways on Veeam Console,

- Selecting gateway servers deployed close to the backup storage tier help reduce processing overhead on backup servers and improves restore performance

- Selecting gateway servers deployed near to the backup proxies/workers help reduce network load with faster backup windows and makes data transfer more efficient.

— Ensure high-bandwidth and low-latency connectivity between:

- Proxies/workers and gateway
- Gateway and backup storage tier

— Dedicated gateway servers (Windows or Linux) should be configured for scalability and performance in larger environments.

— Enable automatic selection for gateway servers through Veeam console, this dynamically assigns best suitable gateway for data transfer and supports multiple gateways for parallel task processing, with built-in failover to alternate gateway servers to ensure continuity.

Mount server

— Mount servers should be deployed close to the backup storage tier to minimize network traffic and improve restore performance

— Scale mount servers horizontally for large environments and assign one mount server per Veeam backup repository to ensure optimal restore performance and scalability

— Use platform-appropriate mount servers:

- Windows mount server for Windows workloads.
- Linux mount server for Linux /object / file workloads.

— Ensure high-bandwidth and low-latency connectivity between:

- Mount server and backup storage tier
- Mount Server and restore target

— Ensure Veeam mount servers are sized with adequate CPU, memory, and disk I/O capacity, especially for:

- Instant Recovery
- SureBackup
- File-level and application restore

Note

Veeam Backup Server automatically creates firewall rules for the ports required to allow communication between the HPE Morpheus Manager, worker VMs and the Veeam Backup Server, refer this link to know more on firewall port requirements of Veeam Backup Server,
https://helpcenter.veeam.com/docs/vbr/userguide/hpe_used_ports.html

---

HPE StoreOnce

Backup target types

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

— Catalyst integration enables:

- Optimized data transfer using Veeam Data Movers (proxy → gateway → StoreOnce)
- Superior performance compared to SMB/NFS shares or VTL 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 Veeam backup copy jobs for tiering and archival

Deduplication strategy

— With Veeam, deduplication is split across source side (proxy / worker VM) and target side (StoreOnce appliance)

— For low bandwidth / high latency environments:

- Use source side deduplication that allows Veeam Data Movers (proxy/gateway) to optimize data before transmission
- Use Catalyst over IP with optimized compression/dedupe settings
- Minimizes WAN bandwidth usage while preserving performance

— For high bandwidth / low latency environments:

- Use StoreOnce target-side deduplication to maximize global deduplication efficiency.
- Tune Veeam settings (compression, inline dedupe) to avoid over-processing

— Use separate Catalyst stores per workload type:

- Improves deduplication ratios
- Enables independent retention policies
- Optimize performance and parallel ingest streams

Network

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

— Add redundant network paths for resilience

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

HPE Alletra X10000

Backup target

— HPE Alletra Storage MP X10000 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, Veeam Backup Server 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.

RPO and RTO reference guidelines

Recovery Point Objective defines the maximum amount of data loss that is acceptable after a failure, measured in time. While Recovery Time Objective defines the maximum acceptable downtime before a service must be restored. RPO is affected by how often recoverable copies are created and protected and unlike RTO, it is not directly affected by restore performance.

The following are the factors that influence RPO targets:

1. Backup frequency decides whether RPO will be in days, hours, or minutes.
2. Backup window duration that completes the backup within the next scheduled window.
3. Network bandwidth that helps keep the backup duration within scheduled window.
4. Number of concurrent backup jobs running should be within the backup infrastructure supported limit.

The following are the factors that influence RTO targets:

1. Performance of backup storage tier including factors such as concurrent restores supported, ingest rates, deduplication overhead etc.
2. Placement of gateway servers effect latency. Ensure low bandwidth and high latency connectivity between ‘gateways and backup storage tier’ and ‘gateways and worker VMs’.
3. When possible, use dedicated backup VLAN to provide more predictable backup performance.
4. Physical proximity of backup storage tier to recovery infrastructure.
5. Multiple gateways and worker VMs help process concurrent backup jobs and avoids over subscription.
6. Target datastores influence the restore speed with HDDs providing lower speeds compared to SSDs and NVMe drives.
7. Regularly test recovery workflows and connectivity.
8. Bare-metal deployment of backup infrastructure can improve RTO by providing direct access to hardware resources and by eliminating virtualization overhead.

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 6. HPE Private Cloud PC3000 with Alletra Storage MP (Block)

Component	Configuration
Storage	1 x HPE GreenLake for Private Cloud Business Edition w/Alletra STG MP Block OS Base Configuration
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 Veeam Backup Server)

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 7. HPE ProLiant DL for Veeam Backup Server

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

Hardware	Configuration
Controller nodes	4 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) Yields 2.2 PB usable capacity Provides aggregate throughput of up to 102 GB/sec read and 17 GB/sec write

Note

Refer to the "Reference Configuration" section of Veeam Standalone reference architecture from HPE 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 Veeam 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 Veeam 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 Veeam 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, ensuring data confidentiality and resilience against ransomware and insider threats.

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 Veeam worker VM to the Veeam Gateway 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 Veeam Backup Server, improves deduplication efficiency. If required, IPsec tunnel functionality provided by the primary storage tier can be used to protect data in transit from Veeam to backup storage target.

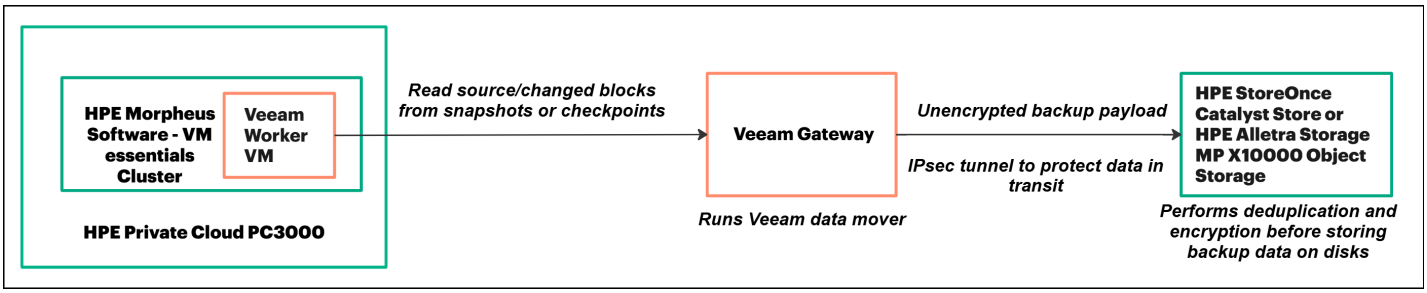


Figure 4. Backup workflow providing maximum deduplication efficiency

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 Veeam 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 Veeam Backup Server level can increase CPU utilization on the Veeam Backup Server and 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 Veeam can be used to protect data in transit from Veeam to backup storage target.

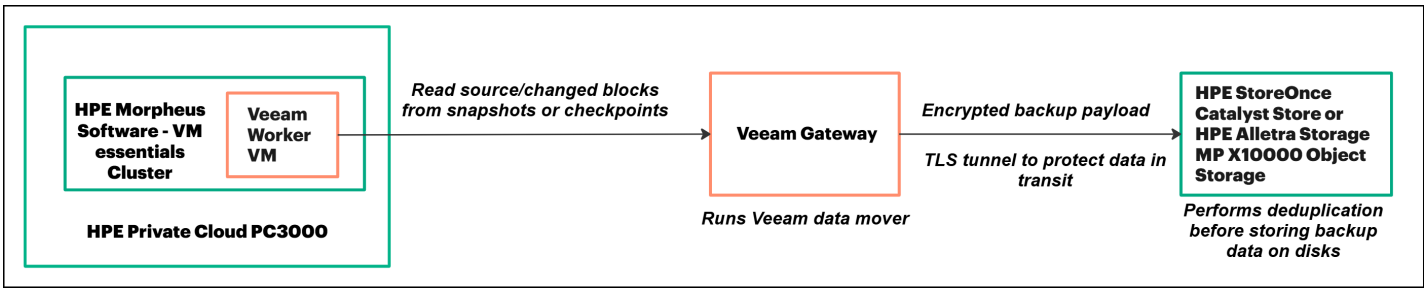


Figure 5. Backup workflow providing high security

Note

For HPE Morpheus Software—VM essentials, Veeam Backup Server does not provide a job-level backup encryption option. Instead, backup encryption can be enabled at the backup repository level.

On-site or off-site backups requiring protection against ransomware and insider threats

When the backup data compliance requires protecting the backup data against ransomware or accidental deletion or insider threats, immutability must be configured to prevent deletion or modification of backup data.

Immutability prevents backup data from being deleted or modified during the defined retention period. Immutability is enforced by the backup storage layer through StoreOnce Catalyst Store Security Lock or Alletra Storage MP X10000 Object Lock feature. This prevents backup data from being modified or deleted before the configured retention period expires, regardless of actions taken from the backup application.

When a backup retention period expires, Veeam initiates the deletion process by requesting the configured backup storage tier to remove the corresponding restore point. The backup storage tier then independently verifies whether any active immutability retention period remains in effect before allowing the deletion. As a result,

in the event of ransomware attacks, or accidental deletion attempts, immutability prevents the removal of backup data until the configured retention period has elapsed, ensuring that backups remain recoverable.

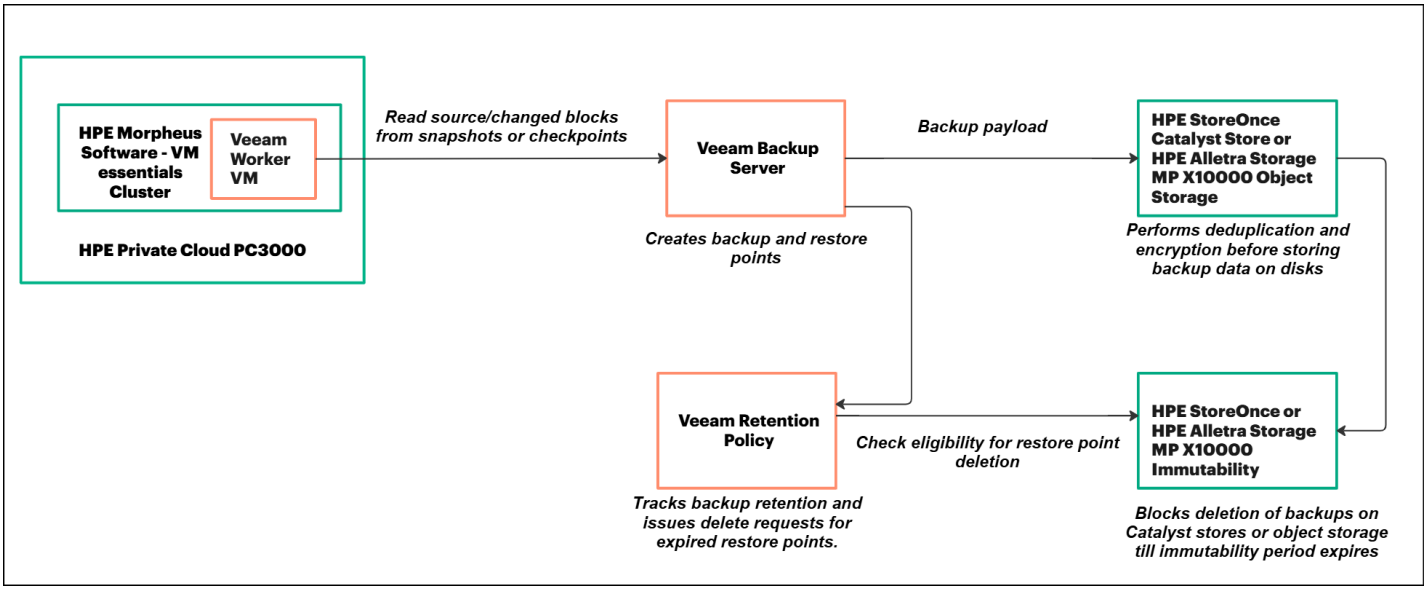


Figure 6. Backup workflow showcasing immutability

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.

Veeam

Access Control and Identity Security

Veeam supports identity and access controls that strengthen administrative security for the backup environment.

— Multi-factor authentication (MFA): Veeam 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: Veeam 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

Veeam uses AES-based encryption to protect backup data before it leaves the backup server. Encryption can be enabled when backup jobs are created, and encrypted data cannot be read without the encryption password or key managed by Veeam or an external key manager.

Threat Detection and Recovery Verification

Veeam inline malware detection scans backup streams for suspicious behavior and recovery verification with Veeam Sure Backup boots VM from backup, verifies it starts and can run integrity tests. This verifies if backups are recoverable after an incident.

Note:

Veeam Backup Server provides a built-in tool named 'security and compliance analyzer' to ensure the backup server configuration follows security best practices for Veeam backup infrastructure components based on Microsoft Windows Server and Linux operating systems. Adhering to all security checks provided in this tool helps maintain a better security posture of Veeam Backup Server. The list of all compliance checks can be accessed here, https://helpcenter.veeam.com/docs/vbr/userguide/best_practices_analyzer.html

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 (Veeam) 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 Veeam, 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 Veeam Backup Server 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.

Veeam Backup Server

The Veeam Backup Server 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, with Veeam recommending additional memory allocation per job and sufficient compute resources for job processing. In larger environments, it is recommended that the configuration database should

be externalized and independently scaled to avoid bottlenecks, while all data-path functions are offloaded to backup proxies, and gateway servers.

Note

. When deploying a Linux-based Veeam Software Appliance, ensure sufficient storage is allocated upfront, since disk expansion after deployment is not supported.

Veeam worker VM and gateway servers

— Worker VMs / Proxies and Gateway Servers in Veeam 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 worker or gateway VM to support higher task concurrency, while scale-out is achieved by deploying additional worker or gateway VMs to distribute the workload.

— Veeam processes backup workloads as discrete tasks (typically one task per VM disk), and both workers and gateways must be sized based on the number of concurrent tasks they are expected to handle; official guidance recommends allocating approximately 1 vCPU and 2 GB RAM per concurrent task for workers, while gateway VMs (including object or deduplication appliance gateways) require base resources plus additional memory per concurrent task (for example ~4 GB RAM per task).

— From a design perspective, Veeam recommends controlling and tuning maximum concurrent tasks per component to match available CPU and memory, ensuring stable and predictable performance. In HPE Morpheus Software—VM essentials environments with increasing workload servers or clusters, a minimum design guideline is to deploy at least one worker VM and one gateway VM per workload node to ensure locality and avoid bottlenecks, with additional nodes introduced as concurrency and throughput requirements grow.

— Adding more worker or gateway VMs does not necessarily improve backup throughput, as overall backup performance also depends on the available backup storage tier and network bandwidth. Ensure that both the backup storage and network infrastructure are sized to sustain the aggregate throughput of all data-path components.

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

Veeam Backup Server

HPE OpsRamp integration with Veeam delivers visibility into and management of key resources, including Veeam Enterprise Manager, Veeam Backup Servers, and Backup repositories, leveraging Veeam Backup Server, Enterprise Manager, and Service Provider Console REST APIs.

The list of supported metrics for Veeam is available here: https://docs.opsramp.com/integrations/backup-and-recovery/veeam/supported-metrics-and-default-monitoring-configuration/ .

Note

The real time monitoring of job schedules, backup status or automated alerts for failures or any jobs running on HPE Morpheus Software—VM essentials are not tracked by HPE OpsRamp. This is because Veeam does not expose APIs for collecting job information related to backup and restore jobs for HPE Morpheus Software—VM essentials workloads.

The steps required to configure observability for Veeam are divided into the following sections:

Integration Setup: This section covers the steps to set up the monitoring integration available in HPE OpsRamp to monitor the Veeam resources. (OpsRamp reference link: https://docs.opsramp.com/integrations/backup-and-recovery/veeam/working-with-veeam-backup/#configure-veeam-backup)

View Discovered Resources and Dashboard: This section covers the steps to view the discovered resources and navigate to the Veeam Dashboard to view the components and their Alerts. (OpsRamp reference link: https://docs.opsramp.com/integrations/backup-and-recovery/veeam/working-with-veeam-backup/#discover-resources-in-veeam-backup)

Support and maintenance

This section covers life cycle management of HPE Private Cloud PC3000 and backup infrastructure including Veeam Backup Server, 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.

Veeam Backup Server

Veeam Backup software updates and feature upgrades need to be planned and executed in alignment with:

— Vendor support matrices and Veeam release lifecycle policies

— Compatibility with HPE Morpheus Software—VM essentials

— Interoperability with target storage platforms such as HPE StoreOnce and HPE Alletra Storage MP X10000

The advanced Veeam architecture, comprising backup server, proxies, repositories, and gateway servers, supports phased (rolling) upgrades, enabling components to be upgraded sequentially with minimal disruption to backup and restore operations.

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 Veeam with HPE Private Cloud PC3000 and HPE Morpheus Software—VM essentials:

1. PC3000 supports iSCSI protocol only for storage connectivity. FC and NVMeOF are not currently supported with PC3000.
2. 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.
3. HPE Alletra Peer Persistence is supported for PC3000 with only VMware vSphere platform.
4. Veeam Backup Server does not yet support HPE Alletra based storage snapshots backup and recovery with HPE Morpheus Software—VM essentials.
5. Veeam Plug-in for HPE Morpheus Software—VM essentials does not support the multitenant configuration.
6. Veeam Plug-in for HPE Morpheus Software—VM essentials does not support the IPV6 protocol.
7. Veeam Plug-in for HPE Morpheus Software—VM essentials does not support backup of the HPE Morpheus Manager.
8. Veeam Plug-in for HPE Morpheus Software—VM essentials does not support backup of VMs deployed manually using Libvirt scripts.
9. Veeam Plug-in for HPE Morpheus Software—VM essentials does not support storing backups in HPE Cloud Bank Storage repositories directly. However, it supports storing copies of backups in HPE Cloud Bank Storage.

Summary

This reference architecture provides detailed design guidance for an on-premises enterprise data protection solution integrating Veeam Backup Server 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. VMware vSAN, VMware vSphere, VMware Cloud Foundation, and VMware are registered trademarks or trademarks of Broadcom, Inc. and its subsidiaries in the United States and other jurisdictions. All third-party marks are property of their respective owners.

a50015902enw

HEWLETT PACKARD ENTERPRISE

HPE.com