HPE Private Cloud Enterprise

1. Service Description Overview

HPE Private Cloud Enterprise (the "Service") is a fully managed Infrastructure as a Service (IaaS) offering that delivers a self-service cloud experience to IT, application administrators and developers. This service relieves organizations from the burden of managing the lifecycle of hardware and software and allows them to instead focus their resources on activities that are core to their business while HPE takes care of the underlying platform. The Service enables customers to consume compute, storage, and networking resources, giving teams the ability to choose from bare metal, virtual machines (VMs), and/or Kubernetes clusters all deployed onto a common pool of cloud infrastructure.

The Service provides role-based access-controlled self-service, enabling the Customer's IT admins and developers to accelerate innovation. Backed by enterprise-grade availability SLAs, the Service is built to handle on-premises workloads ranging from legacy to cloud native

2. Core Service Features

2.1 Bare Metal

The Service provides Customers the ability to provision dedicated physical compute resources without a virtualization layer. Bare Metal instances are ideal for workloads that need direct access to the physical hardware or are sensitive to the performance overhead of virtualization. Customers can provision bare metal instances from any of the supported instance types that have been deployed at their selected location(s).

2.1.1 Key Features

- Dedicated Hardware: A bare metal instance ensures that all hardware resources are available to the workload.
- Performance: Without the overhead of a hypervisor, bare metal instances deliver the full potential of the underlying hardware to your workload. Bare metal instances are ideal for latency sensitive and compute intensive workloads.
- Configuration Flexibility: Choose from a set of hardware configurations that best meets the specific needs of the workload.
- Compute Groups: Create logical grouping and isolation of resources, and control compute, storage and networking consumption with quotas.
- Lifecycle Management: Manage the full lifecycle of compute, network and storage resources via the GUI, API and the HPE terraform provider (the "Terraform Provider"). Manage firmware updates, OS deployment and instance re-imaging across a fleet of bare metal instances.
- Networking Options: Create and attach bare metal instances to the right networks for your workload. Choose from public, private, shared, and hybrid (spanning bare metal/virtual machine/containers) networks.
- **Note**: HPE does not distribute OS images as part of HPE Private Cloud Enterprise. Customers are required to provide their own operating system images that have been hardened in accordance with their policies and use them to image their bare-metal instances. HPE provides documentation on how to build operating system images that are compatible with the Service. HPE also provides a list of supported operating systems and versions, which are updated periodically.

2.2 Virtual Machines

The Service allows Customers to provision VM instances that can be used to deploy and run HPE HVM hypervisor or VMware ESXi-based workloads. Customers can request multiple VM clusters that consist of different compute instance types and sizes allowing them to have optimized cost and performance for different virtual workloads. The Service uses NSX to provide advanced software-defined networking functions for ESXi clusters.

2.2.1 Key Features

- Create logical grouping and isolation of resources using groups
- Set compute, storage and networking quotas by type and quantity for groups
- Apply tags to VMs for billing, showback & chargeback purposes
- Provision and manage the lifecycle of compute, network and storage via the GUI, API and the Terraform Provider
- Support for public, private and shared networks for multi-tier applications that run on bare metal/virtual machines/containers
- Includes advanced software defined networking functions such as load balancers, firewalls and micro-segmentation that enable improved security and optimizing performance for ESXi clusters
- Includes standard VM sizes and supports creation of custom virtual machine t-shirt sizes
- Provides ability to create and publish application blueprints, application catalog that can be exposed as a click-to-deploy catalogue to the end users
- Carry out tasks and workflows that enable custom provisioning workflows with pre and post deployment tasks
- Policy-based auto-scaling
- Support for Terraform for Infrastructure as a Code, and integration with external automation tools like Ansible, Chef, and Puppet
- Option for HPE provided or Bring Your Own VMware licenses (HPE-specified versions only)
- Capable of integration with external backup solutions such as Commvault and Veeam[1]
- Compatible with cross-site highly available ESXi virtual machines to protect against site level failures[1],[2]

Note: HPE does not distribute OS images as part of HPE Private Cloud Enterprise. Customers can bring their operating system images that have been hardened as per their policies and use them to create virtual machines. The list of supported operating systems and versions are updated periodically in the user guide.

2.3 Kubernetes

The Service allows application teams to run their containerized workloads with industry recognized Kubernetes orchestration based on the HPE Kubernetes Service (HKS).

2.3.1 Key Features

- **Infrastructure Flexibility**: Application teams can choose the compute form factor that aligns with the needs of their application.
- **Version Flexibility**: Application teams can create clusters from multiple supported[3] versions of Kubernetes.
- **External Container Registry**: Integrate with external public and private repositories to securely store and manage your container images[4].

2.4 HPE Cloud Modules

Cloud modules are standardized components that provide workload-optimized compute instances, storage capacity, and network connectivity that allow Customers to meet their diverse workload requirements. The Service is enabled by these cloud modules and is designed to provide Customers with choice, automation, and faster time to value.

Each of the cloud modules supported by the Service manifests itself as a compute instance type or a storage capacity type that Customers can consume to run bare-metal workloads, virtualized workloads, and containerized workloads The Service supports multiple block volume storage capacity choices designed to meet the performance and availability requirements of a variety of enterprise workloads. Customers can choose one or more storage capacities based on their workload requirements.

---

[1] Requires HPE Services contract to setup and maintain the integration
[2] Requires HPE Services contract to setup and maintain the integration
[3] The list of supported versions is updated periodically and published to the user guide
[4] The list of supported image repositories is updated periodically and published to the user guide

The available instance types change over a period as new instances are made available and old instances are retired.

2.5 Identity and Access Management (IAM)

2.5.1 Key Features

- **Role Based Access Controls (RBAC)**: Assign roles and permissions to users and groups, enforcing that individuals have the correct level of access to compute, storage and network resources based on their responsibilities. Custom roles can be created when individuals access needs are different from predefined roles.
- **Granular Permissions**: Fine grained permissions cover the various operations within the Service, allowing for total control over the actions available to a user.
- **Single Sign On (SSO)**: Integrate with your current Identity Provider (IdP) to allow your users to access the Service seamlessly with their corporate credentials, subject to IdP being supported by HPE.
- **Multi-Factor Authentication (MFA)**: MFA mitigates credential phishing, password theft, and other threats by requiring multiple forms of identification (SMS code, hardware token, biometric identifier, and more) to confirm a user's identity.
- **Audit Logging**: Access an audit trail of all user activities within the Service, including who made what changes to *which* resources at *what* time and from *which* location.

2.6 UI, API & IaC

2.6.1 User interface (UI)

Customers can access and consume the Service through a rich and intuitive graphical user interface that is accessible through the hybrid cloud platform for HPE GreenLake cloud (the "platform") console. The graphical user interface is accessible from any location with an internet connection. The user interface is role-based access controlled, and customers can define the roles and permissions that govern the access associated with a user.

2.6.2 Application Programming Interface (API)

The Service provides a secure, standardized interface to provision, configure, and manage cloud infrastructure in their environments. These APIs allow customers to automate the consumption and lifecycle management of resources in the Service. HPE GreenLake APIs enforce the role-based access-control policies that have been defined.

2.6.3 Infrastructure as Code (IaC)

IaC functionality is offered by the HPE Terraform Provider to manage private cloud resources. The HPE Terraform Provider is published in the public terraform registry. The IaC framework provides a simplified, unifying experience in managing lifecycle of resources across bare metal, virtual machines, and container clusters

2.7 Integration with external clouds

To provide a hybrid cloud experience, The Service can be integrated with public clouds like Amazon Web Services, Microsoft Azure Cloud Services, Google Cloud Platform and pre-existing customer managed VMware infrastructure. The Service provides a cloud management platform, through which Customers can onboard and manage external clouds. Management of external cloud infrastructure is not included in The Service, and additional cloud management platform licenses are required to provision external workloads.

2.8 Consumption Analytics

The Service includes consumption analytics ("Consumption Analytics"). Consumption Analytics provides users with the ability to analyze cost and usage data. Consumption Analytics has capabilities for creating custom dashboards, cost and usage reports, cost and usage budgeting, and capacity usage reports. Consumption Analytics gives cloud or tenant admins visibility into private and hybrid cloud usage and cost data. The tools in Consumption Analytics deliver a unified view of historical cost and usage data for both Service resources and onboarded public cloud resources.

Consumption Analytics dashboards give the user an at-a-glance view of data included in reports. Reports provide detailed summaries of cost and usage data that can be exported in PDF format for distribution with charts and data, or in CSV format for importing into other tools.

Consumption Analytics budgets allow for the monitoring and control of cost and usage for both HPE Private Cloud Enterprise, and hybrid cloud. Users can define overall budgets, and category budgets as appropriate. The robust budgeting capabilities allow users to track usage against a budget and get notified when the tracked usage is expected to exceed the set budget. Budgets can be set against costs, usage, and a variety of custom reports.

Consumption Analytics capacity usage reports provided a detailed view of the resources in HPE Private Cloud Enterprise, and what is available for use. The information is presented for each service and includes historical charts for recognizing trends.

2.9 Service Implementation

HPE provides the physical implementation of the System at data centers (DCs) owned or managed by the Customer or at an HPE GreenLake contracted colocation facility. Implementation includes a fully installed and ready-to- consume environment.

Deployment management	HPE will assign a deployment specialist to coordinate the overall implementation of the Service and the handover to the operations phase. System setup begins with pre-integration of the System in the HPE factory. HPE contacts the Customer to gather the information required in the following areas: – onboard the Customer to the platform – preconfigure the System in the HPE factory – schedule the delivery of the System at the DC location and agree on the logistics of the on-site installation process. Working with the Customer, HPE will confirm and detail the specific site requirements, including connectivity and security, to enable a seamless System installation and operation of the Service.
Installation and startup	The deployment specialist contacts the Customer to validate site readiness prior to System shipping and coordinates the on-site installation at a mutually agreed upon time. An HPE field delivery specialist installs, powers on, and connects the pre-integrated and configured solution to the external peripherals network. Validation is performed to verify that there was no damage during shipping and that the solution is properly connected and functioning in the Customer's environment. – Connectivity validation is performed to ensure that the System is remotely reachable for ongoing monitoring and management. – HPE remote monitoring, support, and management tools are configured, activated, and tested. – Final solution configuration and validation is performed to help ensure the Service is functional and ready for ongoing operations.
Customer onboarding	HPE onboards the Customer per the user account details provided. This would provide Customers access to HPE GreenLake and other programmatic interfaces to interact with and consume the Service. As part of this process, HPE will provide a checklist confirming completion of the validation testing, Service consumption metering and billing is then enabled, and a notification of System readiness is sent to the Customer. An orientation session, delivered remotely, will be provided on the services and resources that help Customers to consume the Service, along with capacity measurement tools to electronically view their usage and understand the processes to contact HPE support

Table 1. Service implementation.

Note: The Service does not include cloud transformation services, network consultation services, identity or access management system integration, customer ITOM or ITSM system integration, workload migration, deployment, or customer workload performance monitoring services, customer-specific administrative or user configuration services, or other services not explicitly described herein. HPE provides additional professional and managed services that can be customized to meet the requirements of the customer environment.

2.10 Service Management

The Service includes comprehensive management of the following activities.

Proactive Monitoring
Incident Management
On-site repair and replacement of System hardware components
Remote troubleshooting and remediation of Solution software components
Lifecycle Management of Solution software and hardware components
Capacity Management

2.10.1 Relationship management

The purpose of relationship management is to govern the relationship between Customer and HPE with the aim of providing a smooth and swift collaboration between both parties. HPE will provide an assigned service relationship manager to be the Customer's advocate and focal point for Service governance.

Service Relationship Management	The Service Relationship Manager (SRM) is the Customer's primary point of contact within HPE for the Service and is responsible for coordinating Service delivery, leading a team of other HPE resources to deliver the services as described herein[5]. The SRM will remotely meet with the Customer for regular operational reviews of HPE's delivery of the Service and will provide advice and guidance regarding the routine delivery of the Customer's critical IT services. The SRM will also lead the change management process, where capacity or other Service scope changes are required.

Table 2. Relationship management.

2.10.2 Governance

Integral to making the service experience successful is a well-structured governance process, bringing together planned and unplanned activities and making sure the service is performing as expected.

A kickoff meeting between the Customer and the HPE services team is conducted to establish stakeholder contacts within HPE and the Customer and establish governance processes.

Cloud Service Support Plan	This document captures the expected service delivery activities during the term of the contract based on the standard HPE Private Cloud Enterprise services and any selected additional service options. Working with the Customer, HPE will document and maintain standard operating procedures specific to maintaining the System and documenting the service management processes and escalation protocols. The document will be reviewed remotely on a quarterly basis with Customer with any required changes being managed through the change management process.

[5] The scope of the SRM activities is limited to the Service and Systems described in the SOW and will not cover any other part of the Customer infrastructure.

Cloud Service Operational Review	The Customer and the HPE team review, on a quarterly basis, the services provided over the previous period and discuss trends, upcoming changes, and potential impacts. It provides an open communication forum to help ensure a common understanding of business and IT requirements. During these sessions, the HPE team may share HPE best practices and provide tailored advice.
Reporting	HPE will provide Customers access to tools such as Consumption Analytics, Capacity planning, etc. that allow Customers to generate reports and/or provide HPE generated reports covering the following areas: – Change Management – Customer-reported incidents – Capacity usage Reporting details will be communicated during the Service implementation period.

Table 3. Service Governance.

Event/incident management	HPE will proactively monitor the System to help ensure the System is operating correctly and to resolve any incidents that may arise. – Events requiring additional action will be logged as incidents or request for change (RFC) according to their nature. Where there is a potential impact on the Service or where Customer interaction is required, HPE will notify the Customer to agree on steps to resolve the issue. Where Customer interaction is required to resolve an incident, this will encompass communications and dialog with the Customer in a timely manner. – The incidents will be managed throughout their lifecycle through to closure. – Customers may also raise incidents as required. Regardless of coverage window, incidents can be reported to HPE through telephone, web portal, or as an automated equipment reporting event using HPE electronic remote support solution 24x7. Incidents should be reported by the Customer as a Service request, see section below.

Service feature	Coverage window
Enhanced phone response	Remote response 24x7; service 24x7 per week including HPE holidays
24x7 on-site coverage	On-site response 24x7; service 24x7 per week including HPE holidays

Table 4A. Service levels for remote support and on-site coverage.

Change management

HPE will implement a change management process relating to changes to be made to the System. The process will coordinate HPE's activities in relation to the implementation of those changes. HPE may implement changes periodically as part of standard operations without notice to the Customer for changes that are not expected to have an impact on the Service. If changes to the System impact the scope of the Service described in this service description, the changes will be subject to the change management process as detailed in the cloud service support plan.

HPE will publish any required changes that need to be made to the System and coordinate with the Customer for an agreed window to implement these changes based on their assigned priority.
Changes fall into two categories:

- Service improvement and restoration: Covers required changes to the System to resolve any underlying service issues or to enhance the overall performance of the Service. These changes will be managed based on their prioritization.
  - **Normal change**: Recommended changes to the System that are not urgent and can be scheduled at an agreed time or within sixty days.
  - **Critical change**: Urgent mandatory changes to the System to resolve a critical issue for which the normal change procedure does not meet the requirements. These changes are scheduled as soon as possible in agreement with the Customer or within seven days.
- Service expansion/reconfiguration: Covers expansion to the System to add additional capacity or changes to the use of the System such as reconfiguration of the Customer's workloads. These changes will be managed on a scheduled basis in cooperation with the Customer and are subject to the change management process as agreed upon and detailed in the cloud service support plan.

Service request management

Customers can raise service requests through the self-service portals made available to them as part of the Service. HPE will review and categorize the requests based on the nature and priority of the request and respond accordingly. HPE may request additional information from the Customer to effectively fulfill a service request. Customers should also log any Service-impacting incidents or events as service requests. Service requests will be assessed and prioritized by HPE and then addressed as per the following timelines. For clarity, these target timelines are not part of the SLA's set forth in section 5:

Priority	Description	Target Response Time	Target Resolution Time*
1	Critical	90% < 15 min	90% < 4 hours
2	High	90% < 1 hour	90% < 8 hours
3	Medium	90% < 4 hours	90% < 16 hours
4	Low	90% < 8 hours	90% < 24 hours

***Target Response and Resolution times are a best effort target. Resolution may include a temporary workaround**

Solution lifecycle management	HPE will maintain the System on an ongoing basis by updating, upgrading, or patching its various components. It is essential to maintain the System at the recommended levels to maintain the System availability/interoperability and to maintain the SLAs. – HPE will implement updates to the System on a periodic basis as outlined as part of Change management. – Customer is responsible to provide a schedule as necessary for implementing updates. • For updates classified by HPE as critical and requiring a scheduled maintenance window, Customer shall provide a schedule within seven days from the day HPE notifies the Customer of the requirement of a maintenance window. For updates classified by HPE as normal and require a scheduled maintenance window, Customer shall provide a schedule within sixty days from the day HPE notifies the Customer of the requirement of a maintenance window.
Capacity management	HPE will maintain a capacity plan relating to the System, based on Customer analysis of their capacity requirements in relation to the business demand. This will be documented and reviewed during the quarterly Cloud Service Operational Review meetings. Capacity management consists of two major elements: – Capacity utilization report within HPE's platform examining usage trends and used as input in the capacity planning process to forecast Service capacity requirements. – Capacity planning—A capacity planning meeting will occur at least quarterly with the Customer and the HPE team, or on an ad-hoc basis, when significant variations are detected by the HPE team. It can occur as well at the Customer's request. During the capacity planning process, the Customer will provide HPE with an outlook of future consumption needs. Any capacity changes will be made in accordance with the agreed contract change management process.

Table 4. Service Management.

2.11 System Operations and administration activities

The following tables show the specific HPE and Customer activities that will be performed as part of the Service.

Note for Tables 7 to 11: R—responsible, A—accountable, C—consulted, I—informed

Activities	Customer	HPE
Monitor health and availability statistics of HPE Private Cloud Enterprise System	I	A/R
Check log files on critical events/incidents	I	A/R
Stop and start HPE private cloud service capabilities	C	A/R
Add/remove/update tenant users, groups, and roles	A/R	-
Perform configuration backups of the System components managed by HPE	-	A/R
System patches, version upgrades, and maintenance	C	A/R
Address performance incidents within the scope of HPE's responsibilities	C	A/R
Address critical incidents within the scope of HPE responsibilities	I	A/R
Monitor running Services and changed the state of services	I	A/R
Respond to security events/incidents	C/I	A/R
Manage configuration changes of the System components managed by HPE	C/I	A/R

Manage HPE management NW changes	-	A/R
Manage Customer network configuration changes	A/R	C

Table 5. HPE Private Cloud Enterprise platform.

Note: In areas where the Customer is to be informed or consulted, HPE will use its discretion on the nature, time and mode of communication. Communication may be in the form of emails; information posted on the user interface portal or through the HPE specialists

Bare-metal instances: The following table shows the specific HPE and Customer activities that will be performed for Customers consuming bare-metal instances.

Activities	Customer	HPE
Bare metal orchestration platform management	I	A/R
Perform workload and application backup and restore	A/R	-
Install and update backup/antivirus agent	A/R	-
Provide and maintain operating system images and licenses	A/R	-

Table 6. HPE Private Cloud Enterprise—Bare Metal.

Virtual machine instances: The following table shows the specific HPE and Customer activities that will be performed for Customers consuming virtual machine instances

Activities	Customer	HPE
Virtualization platform management (hypervisor, SDN, CMP)	I	A/R
Perform workload and application backups	A/R	-
Install and update backup/antivirus agent	A/R	-
Backup and restore of customer virtual machines and associated data	A/R	-
Create, Delete, remove, suspend, power on, power off, resume, reset VMs	A/R	-
Deploy new or clone existing VM guest	A/R	-
Change VM guest flavor (size)	A/R	-
Reboot VM guest	A/R	-
Create VM guest snapshot	A/R	-
Provide and maintain guest operating system images and licenses	A/R	-

Table 7. HPE Private Cloud Enterprise—VMs.

Kubernetes clusters on virtual machine and bare-metal instances: The following table shows the specific HPE and Customer activities that will be performed for Customers deploying HPE Kubernetes (HKS) clusters.

Activities	Customer	HPE
Kubernetes platform management	I	A/R
Perform workload and application backups	A/R	-
Backup and restore of the Kubernetes control plane nodes and worker nodes	C	A/R
Delete Kubernetes control plane nodes (on Customer's request)	R	A

Delete Kubernetes worker nodes (scale down cluster)	A/R	-
Create, modify, or remove Kubernetes cluster	A/R	-
Increase or decrease the number of Kubernetes worker nodes	A/R	-
Manage Kubernetes cluster resource allocation (Kubernetes control plane and worker nodes)	A/R	-
Create, modify, or remove the Kubernetes platform add-ons	A/R	-
Upgrade platform extension service versions (if applicable)	I	A/R
Create, modify, or remove platform services (if applicable)	C/I	A/R
Create, modify, or remove namespaces and quotas	A/R	-
Create, modify, or remove Kubernetes pods (through kubectl, ERE console)	A/R	-
Container image upload to Docker repository	A/R	-
Remove/delete container image from Docker repository	A/R	-
Cross-service workload communication (VM application communicating to containerized application and vice versa)	A/R	C/I

Table 8. HPE Private Cloud Enterprise—Kubernetes.

External cloud integration with HPE Private Cloud Enterprise

Activities	Customer	HPE
Enable onboarding and integration of the supported external clouds with the cloud management platform	-	A/R
Support for provisioning and lifecycle management of the resources on the external clouds	-	A/R
Managing cloud subscriptions for external clouds and the resources within external clouds	A/R	-

Table 9. HPE Private Cloud Enterprise—external cloud integration.

2.12 Educational services

One-year access to pre-defined quantity of HPE Education Learning Credits is included with the Service. The Learning Credits can be used across multiple users and for multiple courses which may include (but not limited to) eLearning for various HPE technologies, eLearning for the Service etc. Third-party training courses or instructor-led training are excluded. See https://education.hpe.com/ww/en/training/portfolio/cloud.html for more information.

3. Minimum configurations

The Service allows Customers to create bare-metal hosts, VMs, and Kubernetes clusters on a common pool of infrastructure. Customers can determine the capacity to be allocated to support the different workload types at the time of initial System setup and make changes as necessary later.

Each HPE Private Cloud Enterprise deployment must have a minimum of 4 compute instances of the same instance type and at least one of the business critical or mission critical storage capacities. The first 4 compute instances of the same type are intended to create a virtualization cluster to support virtual machine workloads and must include at least 128 vCPUs per instance. Customers can determine the allocation of the remaining compute instances as per their requirements at any point in time.

The following table describes the conditions that govern the allocation/deallocation of bare-metal compute instances for the different workload types.

Bare metal	– All compute instances can support bare-metal workloads. – Customers can create bare-metal hosts using any compute instance that is available in the unallocated pool.
Virtual machines	– Minimum of four bare-metal compute instances are required per virtualization cluster and each cluster must consist of the same instance type. Two or three instance clusters can be requested but these will not be covered by the monthly uptime SLA for VM clusters. – VM clusters are configured with a default oversubscription value of 2:1 (vCPU to physical core) for VM services. Customer can opt for other oversubscription values (up to a maximum of 6:1 vCPU:physical core ratio) based on their workload requirements. – Customers can request the addition and/or deletion of capacity allocated to the virtualization clusters. HPE will review the request and fulfill it subject to the request satisfying technical limitations and availability of the necessary licenses and capacity. – Count of VMware licenses included in the solution is derived from virtual capacity (vCPU, memory) requirements projected by the Customer for their ESXi clusters during solution sizing and their associated CPU overcommit ratio. – Customers can bring their own licenses, as per HPE's specifications, if they have an enterprise license agreement with VMware.
Kubernetes	**Containers on VMs** – Minimum of four bare-metal compute instances are required per virtualization cluster that is needed to enable deploying containers on VMs, and each cluster must consist of the same instance type. – A single virtualization cluster can be shared to deploy virtual machines and containers on virtual machines.

Table 10. Workload-type support conditions.

4. Add-on Options

4.1 Customer Data Center Integration

The Service is delivered as a standalone private cloud within the Customer data center. Further integration steps may be required in order for the Service to operate within the existing data center framework. This integration may require additional contracted professional services to complete, which are not part of the Service unless they are agreed to in the SOW, including all required integrations and associated acceptance criteria. Start of Service metering and billing is not dependent on completion of these integration activities.

Additional integrations beyond the professional services agreed to in the SOW require additional service contracts. These integrations may include but are not limited to the following:

– Migration of workloads from Customer's existing IT systems.
– Identity, credentials and cypher management services
– IPAM and DNS service
– ITSM, monitoring, and logging services
– Automation, deployment, and build tooling
– Third-party container or Kubernetes services
– External cloud or customer data center infrastructure management
– Backup and disaster recovery services
– Integration with existing storage and networking infrastructure
– Localization of documentation, support, or software

4.2 Bring-Your-Own-License (BYOL) for VMware

Customers have the option to bring their own VMware licenses to the Service. The licenses are a mandatory component of the Service and should meet the version requirements, as supported by HPE. Following are VMware license type needed in HPE Private Cloud Enterprise:

VMware Cloud Foundation (contains vSphere, vCenter, and NSX Networking)

VMware Firewall (contains distributed and gateway firewall)

Please note, Customers must provide all the above licenses along with supported versions under the BYOL option. Customer must also maintain a valid support contract with the support level prescribed by HPE that is active for the entire duration of the contract for which the Service is active. Customers must also ensure that HPE is authorized to contact VMware on behalf of the Customer for product support.

Note: Customer cannot bring their own licenses for part of the HPE Private Cloud Enterprise deployment while requesting HPE to provide licenses for the remainder of them. Please refer to the SOW for the term and the quantity of licenses applicable for a given Service deployment.

4.3 Digital circuit breaker service

Digital circuit breaker is a separately billed service that allows customers to temporarily gain local access to HPE Private Cloud Enterprise, commonly referred to as a 'Break Glass' scenario, when network security threats are detected and the customer has disconnected from the internet. This ensures that customers can continue using the Service in an offline state for a limited time. Once the threat subsides and the internet connectivity is restored, the system securely reconnects when the circuit breaker is turned off. This approach supports business continuity while maintaining strong, adaptive protection.

4.3.1 Service implementation

HPE will enable direct access to the Service via a dedicated role-based customer administrative account and share the access with the customer for safekeeping. During implementation HPE and Customer will jointly agree and document the emergency access procedures to be followed, including but not limited to, the procedures and communications in the event of a break glass event or testing.

The service implementation will include a test of the digital circuit breaker functionality triggered by the Customer. The Customer will confirm successful completion of the test and return to the normal connected mode.

4.3.2 Service management and operation

As HPE Private Cloud Enterprise is a hybrid offering managed as a service by HPE personnel, the hardware and software are deployed in a hybrid model, meaning the workload-focused hardware is deployed within the customer's data centers and the control plane leverages HPE GreenLake cloud platform services.

When the digital circuit breaker is triggered, the on-premises workload servers continue to perform, while the connection to the cloud platform and its core functions are isolated and cannot be leveraged. The impact of the circuit breaker means that the ongoing use of the workload services continues, while the cloud platform functions (such as HPE monitoring and Consumption Analytics) are temporarily suspended.

While the local cloud management platform services will continue to run, no changes can be made to the underlying control and management systems including updates/upgrades, security patches, as the operational data normally sent to and collected by the HPE GreenLake cloud platform and HPE's connection to manage the on-prem systems are disabled. In the absence of active monitoring HPE will not be liable for any SLA breaches during the offline period.

In addition, all the System operations and administration activities that HPE is accountable and responsible for as defined in Section 2.11 will no longer be applicable. The System operations and administration activities that Customer is accountable and responsible for as defined in Section 2.11 will remain the same.

The Roles and Responsibilities are described in the following table:

Activities	Customer	HPE
Activate digital circuit breaker	A/R	I
Confirm with customer that digital circuit breaker has been activated and log event	C/I	A/R
Create tenant users' local access	A/R	
Inform tenant users' local access after activation	A/R	
Manage all workload-related activities as described in table 8,9,10	A/R	
Manually log any HPE Private Cloud Enterprise incidents	A/R	C/I

Respond to any raised incidents	C/I	A/R
Perform onsite parts replacement where needed	I	A/R
Reconnect HPE Private Cloud Enterprise to the internet	A/R	I
Deactivate digital circuit breaker	A/R	I
Inform tenant users' access is switched back to cloud login after deactivation	A/R	
Perform System test and confirm connectivity	I	A/R
Address any pending events	C/I	A/R
Perform system reconfiguration, as needed	C/I	A/R
Confirm return to normal mode of operations and close event	I	A/R

Table 11. HPE Private Cloud Enterprise – Digital Circuit Breaker.

Note: HPE will not provide any proactive remote monitoring during a digital circuit breaker event. Customer support will be limited to hardware break-fix support where no reconfiguration is required (e.g. disk failure) and must be initiated by the customer. Metering data will be collected and processed following the break glass event.

5. Service Level Agreement

The Service comes with the following monthly uptime SLAs.

– Monthly uptime SLA for bare-metal Instances
  - For each bare-metal Instance deployed in a single site, HPE will guarantee a bare-metal Instance monthly uptime percentage of at least 99%.

– Monthly uptime SLA for VM clusters
  - For each VM cluster deployed in single site cluster, HPE will guarantee a cluster monthly uptime percentage of at least 99.5%.
  - For each VM cluster deployed in a dual-site high availability (HA) stretched cluster of at least 8 nodes, HPE will guarantee a cluster monthly uptime percentage of at least 99.95%.

– Monthly uptime SLAs for Kubernetes clusters
  - For each Kubernetes cluster deployed in a single site, HPE will guarantee a cluster monthly uptime percentage of at least 99.9% for clusters deployed with three Kubernetes control plane nodes.

While maintaining unutilized capacity is not a prerequisite to SLAs and/or claim SLA Credits in the case of SLA breaches, HPE recommends that Customers maintain some unutilized capacity in each of their Service deployments to minimize potential workload downtime due to unforeseen incidents. It is recommended to maintain the higher of one node or 12.5% (rounded up for number of nodes) of the capacity needed for the workloads as additional capacity for improved fault tolerance. Such additional capacity may have to be maintained for each Instance type deployed.

5.1 Definitions

– **"Downtime"** is the total accumulated minutes that are part of minutes in the month that have no instance connectivity. Instance connectivity is defined as bidirectional traffic between an instance within the Service infrastructure and outside IP addresses over TCP/IP protocol where the instance is configured for allowed traffic.

– **"Instance"** is:
  - For bare metal equivalent to a bare-metal host
  - For VMs equivalent to a VM cluster
  - For Kubernetes equivalent to a Kubernetes cluster

– **"Minutes in the month"** is the total number of minutes in a given month.

- **"Monthly uptime percentage"** means the total number of minutes in a month, minus the number of minutes of downtime suffered from all downtime periods in a month, divided by the total number of minutes in a month, and converted to a percentage. Monthly uptime measurements exclude downtime resulting directly from any SLA exclusions listed in this service description.
- **"SLA"** means the service level agreement set forth in section 5 of this service description.
- **"SLA Credit"** means the compensation payable to Customer for any duly submitted and qualifying Downtime event as set forth in the SOW or the HPE GreenLake Terms for Select Solutions.

5.2 Eligibility for SLA Credits

To be eligible to claim any SLA Credits for an SLA event, Customer must meet the following requirements:

- Customer has satisfied all corresponding Customer responsibilities as identified in Section 7 of the HPE Private Cloud Enterprise Service Description.
- Customer provides the information requested by HPE to validate the claim.
- Customer has provided the necessary scheduled maintenance window to update and maintain the System as requested by HPE.
- For Bare Metal instances, Customer is required to install the HPE provided monitoring agent.

5.3 SLA exclusions

HPE will not be responsible for a failure to achieve an SLA to the extent such failure is caused by any of the following events or circumstances.

- Scheduled maintenance where Customer has been notified in advance of activities such as hardware maintenance, firmware updates, and such
- Force majeure, suspension, or cancellation events
- The acts or omissions of Customer or Customer affiliates, employees; subcontractors, representatives, agents, or third parties
- Failure of Customer’s or third-party equipment, environment, or services, including any failure thereof
- Customer’s failure to take corrective actions reasonably requested and identified by HPE in writing to Customer as essential to maintain service levels
- Any issues that are caused by events/incidents that are beyond HPE’s control
- Issues related to licenses lifecycle management (renewals, etc.) and access to OEM support in case of BYOL orders, where licenses are provided by Customer
- Misuse of the Service offering or a Service component by Customer
- Results from Customer’s software or hardware or third-party software or hardware or both, for example, guest OS and application-related downtime
- Any deviations to use the Service in a manner other than prescribed in this service description
- Any DC housing failures such as but not limited to (even in cases where co-location has been added as an add-on HPE service):
  - Power failures to racks in DC
  - Customer network failures
  - Cooling failures of racks in DC
- Customer has intentionally disconnected HPE Private Cloud Enterprise from the internet, including but not limited to activation of the digital circuit breaker or any other "break glass" scenario, until HPE has confirmed return to normal operation
- Failure to satisfy any of the Customer responsibilities identified in Section 8 of this document

5.4 SLA Claims

- To request an SLA Credit, a support request must be filed following the standard support request process within sixty (60) days from the day of the suspected SLA event.
- HPE, at its discretion, may request information from Customer, such as log files, to validate an SLA claim. Failure to provide the requested information will result in the SLA claim being denied.

6. General Provisions and Exclusions

- Customer's users will not be provided administrative access to the components deployed and managed by HPE to deliver the Service.
- Customers are not authorized to perform any changes to the Systems deployed at the Customer's premises.
- Customers are responsible for providing a physical or virtual quorum witness server and appropriate network connectivity for implementation of dual-site high availability stretched cluster deployments. Additional services may be required to complete the installation of this server.
- Termination of a System Term will terminate the Service with respect to the affected System.

7. General Terms and Definitions

License agreements that Customers agree to as part of HPE Private Cloud Enterprise.

VMware software license agreement	The Service includes VMware software components unless the Customer has opted for a bring-your-own-license (BYOL) model. As set forth in the HPE aaS Terms for Customers, Customer's use of any software included with the System is governed by the applicable license terms for such software. Accordingly, Customer's use of the VMware software included with the System is governed by the VMware End-User License Agreement (**"EULA"**). As part of the installation services provided pursuant to the statement of work (**"SOW"**), HPE will install the VMware software and Customer agrees to allow HPE to accept the terms of the VMware EULA, (collectively, the **"Shrink-Wrap Terms"**) on behalf of Customer, which may be in electronic format, embedded in the software, or contained within the software documentation. Customer acknowledges the Shrink-Wrap Terms govern Customer's use of the VMware software and Customer is responsible for reviewing such Shrink-Wrap Terms and hereby authorizes HPE to accept all Shrink-Wrap Terms on its behalf. The following link to the VMware EULA is for the Customer's reference: vmware.com/download/eula.html. For VMware software, the Customer will receive the VMware software activation codes from VMware directly and will work with HPE upon receipt of the codes as part of the installation process. Customer must notify HPE upon receipt of the codes in a timely manner and work with HPE as part of the installation process.
SUSE® Linux® Enterprise Server (SLES)	The Service includes SUSE software components. As set forth in the HPE aaS Terms for Customers, Customer's use of any software included with the System is governed by the applicable license terms for such software. Accordingly, Customer's use of the SUSE software included with the System is governed by the SUSE **EULA**. As part of the installation services provided pursuant to the SOW, HPE will install the SUSE software and Customer agrees to allow HPE to accept the terms of the SUSE EULA, (collectively, the **Shrink-Wrap Terms**) on behalf of Customer, which may be in electronic format, embedded in the software, or contained within the software documentation. Customer acknowledges the Shrink-Wrap Terms govern Customer's use of the SUSE software and Customer is responsible for reviewing such Shrink-Wrap Terms and hereby authorizes HPE to accept all Shrink-Wrap Terms on its behalf. The following link to the SUSE EULA is for the Customer's reference: suse.com/licensing/eula. For SUSE software, the Customer will receive the SUSE software activation codes from SUSE directly and will work with HPE upon receipt of the codes as part of the installation process. Customer must notify HPE upon receipt of the codes in a timely manner and work with HPE as part of the installation process.

8. Primary Customer Responsibilities

The following are the responsibilities of the Customer in relation to this Service.

8.1 General

- Customer provides the details as requested by HPE to enable factory integration and on-site deployment and configuration.
- Customer identifies primary and secondary point of contacts who are authorized to accept license terms on behalf of the Customer. HPE will engage the Customer point of contacts during the Service infrastructure build and configuration state to accept license agreements, as necessary.
- Customer to provide HPE with a contact list that contains at least one primary and one backup contact who will be the Customer’s point of contact during all operational support coverage hours as described in Tables 6A of this service description.
- Customer will provide the current network architecture and standards that will be used by HPE to build and set up the System.
- Customer will give HPE access to network services such as NTP, DNS, default gateways, routes, and remediation if needed.
- Customer will provide Active Directory credentials as needed for commissioning and integration of the solution.
- Customer is responsible for the security of their proprietary and confidential information, as well as properly sanitizing or removing data from products that may be replaced and returned to HPE as part of the repair process to ensure the safeguarding of Customer data.
- Customer must allow HPE VPN and/or other secure connectivity as determined by HPE to their network so that HPE can manage the Customer’s on-premises HPE GreenLake environment.
- Customer will make any modifications to the existing network that are required and identified during the planning stages of this Service, prior to arriving on-site to perform configuration and integration tasks.
- The agreement for the Service must be implemented by all parties.
- Customers are prohibited from moving or modifying Systems once deployed in the data center specified in the SOW.
- Customer ensures that site preparation (for example, power and cooling) has been completed at the location where the hardware will be installed in adherence with HPE specifications before the arrival of the Systems.
- Customer ensures that the access path can accommodate rack height and clearance requirements for delivery of the racked solution.
- In case of BYOL, Customer is responsible for providing the correct quantity and version of VMware licenses as prescribed by HPE.
- In case of BYOL, Customer will configure the VMware account accordingly to enable the HPE support team to contact VMware support on behalf of the Customer.
- Customer is responsible for removing all confidential, sensitive, and personal data and personally identifiable data when providing data to HPE in support of SLA claims, support tickets, and others.
- Customer must provide HPE with maintenance windows as requested by HPE to maintain the System.
- Customer must provide timely access to the Systems for service remediation activities.
- Customers are responsible for the host and guest operating system images and their licenses. The host operating system images need to be prepared following the bare-metal OS preparation guidelines published by HPE. The list of supported operating systems and versions are updated periodically in the user guide.

8.2 Service implementation

During System implementation, the Customer will:

- Provide HPE with physical access to site locations for initial installation and testing of remote connectivity software and/or hardware.
- Provide all equipment on Customer site relevant to the provision of the Services.

8.3 Digital Circuit Breaker (optional feature)

Customer is responsible for participating in the digital circuit breaker initial and periodic testing during the contract.

9. Applicable Terms and Conditions

Terms	Link
HPE Data Privacy and Security Addendum	https://www.hpe.com/psnow/doc/a50009396enw
Data processing & security measures	https://www.hpe.com/psnow/doc/a00046995enw
HPE's sub-processors for the purposes of this Service	https://www.hpe.com/psnow/doc/a50009358enw
HPE aaS Terms for Customers (unless otherwise stated in the Change Order Form)	https://www.hpe.com/psnow/doc/a50009054enw

a50009486ENW, V5

HEWLETT PACKARD ENTERPRISE
Hpe.com