Hosted Private Cloud (HPC) – Service Description

SEPT 2025

Table of Contents

Hosted Private Cloud Overview

Hosted Private Cloud (HPC) is the packaging and positioning of EMS products to offer a managed, single-tenant infrastructure service delivered and managed by Equinix Managed Solutions (EMS) and hosted in secure, resilient Equinix IBX® data centers to enable private cloud, hybrid cloud and multi-cloud solutions.

This offering provides enterprises with dedicated, high-performance selected choice of server, storage and networking infrastructure—physically provisioned, logically configured, maintained, and supported by EMS, while customers retain administrative control of their guest virtual machines and operating systems according to the solution design.

HPC is designed for enterprises that need private, high-performance infrastructure without the operational burden of owning, deploying, or managing physical infrastructure. It eliminates the need for enterprises to build or manage their own data centers while preserving full control over system-level software and security.

Many global organizations face challenges such as:

- Rising costs and operational complexity of maintaining on-prem infrastructure
- Inadequate performance, compliance, or data residency control in public cloud
- The need for deterministic performance for legacy or latency-sensitive applications
- Long, labor intensive procurement and project cycles for infrastructure refreshes

HPC addresses these challenges by providing dedicated, enterprise-class hardware with lifecycle management, located in strategically placed IBX facilities and supported 24x7 by EMS.

By combining EMS operational expertise with vendors proven platforms, hardware reference architecture, HPC delivers a scalable, private cloud foundation ready to support a wide range of mission-critical enterprise workloads.

Hosted Private Cloud powered by Dell

Hosted Private Cloud with Dell is a joint and certified solution designed and certified by both partners following the expertise and standards to guarantee the best solution for customers' requirements. This is tailored for mid-to-large multinational enterprises that require:

- Dell Technologies
- Dedicated physical infrastructure managed up to virtualization layer
- Integration with hybrid or multi-cloud environments
- Compliance with data sovereignty, security, and uptime requirements

Standard Service

Hosted Private Cloud with Dell includes:

- Fully racked and cabled Dell PowerEdge servers and optional vSAN-ready storage nodes.
- Customer choice of Intel or AMD processor platforms to match workload needs.
- Customer choice of select network appliances
- High-performance, high-memory configurations available.
- Rack and stack, including cabling and power setup
- EMS provides complete hardware lifecycle support for all elements within EMS sole administrative control
- EMS provides complete management of the infrastructure up to hypervisor layer, leaving guest VM management to the customer
- Firmware updates
- Hardware diagnostics and replacement within Equinix IBX
- Incident support and remote hands

Equinix management framework includes:

- Monitor availability, capacity and performance, trying to anticipate and avoid any service disruptions
- Fast response support, allowing customers to open issue tickets or service requests based on our service catalog

- Periodic maintenance activities, such as critical patching updates, capacity analysis, high availability tests, hardening configuration and even vulnerability analysis
- Change Management to help customer to apply changes mitigating service impact
- Availability SLA for the managed items

For more details on Digital Infrastructure Management (DIM), see the additional service descriptions for those offerings.

Vmware Management

When the customer chooses EMS to manage the hypervisor, Equinix operates the VMware Cloud Foundation management domain—including physical infrastructure, network, storage, NSX, vSAN, SDDC Manager, and vCenter platform services. A dedicated workload domain is provisioned for the customer, who receives vSphere access to create and manage their own clusters, virtual machines, guest operating systems, and application workloads. Equinix maintains lifecycle management, platform health, compliance, and availability of the management domain, while the customer is responsible for all configuration and operations inside their workload domain

A similar division of responsibilities applies if another enterprise hypervisor is used: EMS manages the underlying infrastructure and its management domain, while the customer controls and operates their own dedicated workload domain.

Key Deliverables

From Equinix (Management Domain):

- Guarantee platform resilience and availability under agreed SLAs.
- Provide regular capacity, health, and vulnerability reports for the managed vSphere platform.
- Perform infrastructure monitoring, patching, and change management for the management-domain components.
- Deliver proactive recommendations and compliance evidence in periodic reports.

From Customer (Workload Domain):

- Provide timely access, data, and instructions required to enable services.
- Review, approve, and collaborate on requested changes and compliance actions.
- Ensure the integrity, legality, and governance of all data and applications deployed on their virtual machines.
- Maintain proper access controls, software licensing, and secure connectivity for all workloads.

Hosted Private Cloud Compute Cluster and hosts best practices

The HPC cluster includes a combination of hosts sized according to the required compute capacity, the availability and SLA characteristics of the service.

A certified HPC environment includes a cluster configuration considering the use of spares according to the expected SLA (N + 1, N + 2 principle) considering the capacity of the spare server(s) to ensure availability. Spare nodes can’t be utilized while all active nodes remain operational, therefore the capacity they provide is not included in the calculated available capacity. See other recommendations below:

- Customer can choose multiple hosts and clusters that match the resource request.
- Multiple guarantees of vCPU can be mixed in one cluster by adding an extra Virtual Data Center (VDC).
- There is no maximum size of a VM for the use of compute resources HPC, within the limits of the host. But there are recommendations for the best performance of a VM. Adding more compute resources to a VM above the recommended size does not always lead to performance improvements.
- The recommended virtual disk size per VM is between 40 GB and 8 TB.

Hypervisor license

Based on the customer's solution requirements, HPC deployments optionally include the hypervisor license in accordance with the software vendor's best practices and use rights. See Software Licensing Service Description for more details.

If the customer chooses to bring their own software licenses (BYOL, Bring Your Own License) instead of procuring the Software Licensing service from Equinix, then the customer must observe the software vendor's license terms and conditions. Refer to the Equinix Software Licensing Policy Guide for more information about Software Licensing service from Equinix terms and conditions. For clarity, all BYOL scenarios, the customer is responsible for ensuring compliance with the software vendor's requirements.

Equinix is compliant with strategic and market leading vendors BYOL programs and can accept customer-provided licenses and deliver support as part of our managed services based on the customer's solution requirements.

Connectivity

Connectivity is offered using Equinix Fabric (Virtual Circuits). To make HPC an integral part of customers (multi) cloud architecture, it can be easily connected to the following:

- Equinix Colocation
- Equinix Network Edge
- WAN Providers
- Cloud Service Providers (CSP)
- Other EMS platforms environment in same or another Metro
- Equinix Internet Access (EIA) via Equinix Fabric

Customers can choose to bring and install their own:

- Operating Systems (Linux, Windows, etc.)
- Virtualization platforms (e.g. VCF Bundle, Nutanix AHV, Red Hat Virtualization [RHV], etc.)
- Container platforms (Kubernetes, OpenShift, etc.)
- No embedded software stack is assumed or enforced.
- Back-up & Restore resources can be provided through the Managed Private Backup Service (ordered separately).

Service Options

Dell & Intel-Based HPC Nodes

- Ideal for applications with high per-core performance requirements
- Supports enterprise databases (e.g., Oracle, SQL Server), SAP HANA, ERP systems
- Suitable for legacy workloads and licensing models that favor low core counts

Dell & AMD-Based HPC Nodes

- Optimized for multi-threaded or compute-dense workloads
- High VM density for Kubernetes clusters, CI/CD pipelines, and microservices
- Great for big data analytics, AI/ML training, and high-throughput environments

Dell vSAN Ready Node Clusters

- Purpose-built for hyperconverged infrastructure (HCI)
- Ideal for virtual desktop infrastructure (VDI), ROBO, backup/DR sites
- Simplifies storage/compute scaling in business-critical environments

Hypervisor Licensing

- Access to a dedicated instance of vSphere through VMware Cloud Foundations (VCF) bundle.
- Monthly Technical Support hours for EMS to provide incident management of VCF elements.
- Enablement Services for initial installation and configuration

Microsoft Licensing

- Access to Microsoft Windows Data Center edition.

For more details on Private Hardware, Software License, Enablement Services and Digital Infrastructure Management, see the additional service descriptions for those offerings.

Service Demarcation & Enabling Services

Service demarcation defines the clear boundary of responsibilities between Equinix Managed Solutions (EMS) and the customer within the Hosted Private Cloud (HPC) environment. This delineation ensures mutual understanding of operational responsibilities, support expectations, and integration points.

For VMware deployments, EMS manages the physical infrastructure and the entire VMware Cloud Foundation management domain—including vCenter, NSX, vSAN, and SDDC Manager—while the customer manages their dedicated vSphere workload domain, including virtual machines, guest operating systems, and network configurations.

EMS (Equinix) Responsibilities:

EMS is responsible for the lifecycle management of the physical infrastructure, which includes:

- Hardware provisioning:
  - Rack and stack of Dell servers (Intel, AMD, vSAN-ready)
  - Power and network cabling inside Equinix IBX
  - BIOS and firmware compliance with industry best practices
- Ongoing operations:
  - Hardware diagnostics and remote troubleshooting
  - Firmware patching and upgrades as required
  - Proactive replacement of failed components (disks, PSUs, NICs, etc.)
  - Monitoring all managed components
  - Acting on incident and change management according to ITIL framework
  - Monitoring of out-of-band interfaces (e.g., iDRAC)
- Colocation infrastructure:
  - Power feeds and circuits
  - Cooling and environmental monitoring
  - Cross-connects or Fabric ports for network egress
- Virtualization:
  - Choice and installation of hypervisors (e.g., VMware VCF, AHV, Hyper-V)
  - Configuration and management up to hypervisor layer to deliver the private cloud solution

Customer Responsibilities:

Barring the utilization of Software Licensing Product or Monthly Technical Support, the customer retains full ownership and control of all software and logical configuration on the hosted infrastructure, including:

- Operating system and middleware:
  - Installation, licensing, patching, and hardening of the OS
  - Configuration of drivers and security agents
- Additional virtualization or container orchestration (if applicable):
  - Choice and installation of hypervisors (e.g., VMware, AHV, Hyper-V) or bare-metal Kubernetes
  - Management of virtual machines, pods, or services
- Application layer:
  - Deployment, licensing, and support of business applications
  - Backup and recovery policies for workloads
- Networking beyond the handoff point:
  - Configuration of logical networks, firewalls, and routing inside the OS or hypervisor
  - Management of cloud VPNs or direct Fabric connections into customer cloud VPCs
- Security, compliance, and access control:

- Managing user access to OS, apps, and remote tools
- Encryption, auditing, and compliance certifications

This demarcation enables customers to maintain full control of their software environments while offloading the operational burden of physical infrastructure management to EMS. It also ensures that support tickets are routed to the correct owner, minimizing delays and confusion during incident resolution

Roles & Responsibilities

ACTIVITIES	EMS	CUSTOMER
Hardware ownership (title holder of physical assets)	R/A	CI
Hardware procurement	R/A	CI
Hardware OEM Maintenance & Support	R/A	CI
Hardware lifecycle management	R/A	CI
Scaling compute and storage infrastructure	R/A	CI
Physical access to hardware	R/A	CI
Hardware and firmware administration and updates	R/A	CI
Monitoring of all managed components	R/A	CI
Registering and acting on monitoring alerts as part of management	R/A	CI
Virtualization license titleholder*	OPTIONAL	DEFAULT
Virtualization licensing compliance and platform administration*	R/A	CI
Virtualization platform lifecycle management and upgrades**	R/A	CI
Virtualized resources within tenancy (Guest & In-Guest)	N/A	RA
O/S, middleware, database and application management	N/A	RA

*See Software Licensing Service Description.
**See Monthly Technical Support Service Description

Onboarding

The onboarding process ensures a smooth transition from contract signature to operational readiness. EMS facilitates the end-to-end setup of the physical infrastructure and hands over management access so the customer can install and configure their desired software stack (OS, hypervisor, apps).

Onboarding Phases

Phase 1: Pre-Deployment Planning

Objective: Define scope, validate infrastructure plan, schedule logistics

STEP	ACTIVITY	OWNER	DELIVERABLES
1.1	Kickoff Meeting	EMS + Customer	Roles, contacts, communication plan
1.2	Review Design & BOM	EMS + Customer	Validated configuration, location, power, ETI
1.3	IBX & Rack Assignment	EMS	Confirm IBX, cabinet, power circuit
1.4	Interconnect Planning	Customer + EMS	Network design (Fabric or cross-connects)

Phase 2: Hardware Delivery & Installation

Objective: Physically install and test infrastructure

STEP	ACTIVITY	OWNER	DELIVERABLES
2.1	Hardware delivery to IBX	Dell / Logistics	Asset receipt confirmation

STEP	ACTIVITY	OWNER	DELIVERABLES
2.2	Rack & cable Dell infrastructure	EMS	Completed installation log
2.3	Power-up & test	EMS	Boot verification, indicator check
2.4	BIOS & firmware compliance	EMS	Confirm baseline image versions
2.5	Network setup	EMS + Customer	Fabric ports or cross-connect
2.6	Out-of-band management (OOBM)	EMS	iDRAC or BMC interface configured

Phase 3: Private Cloud Implementation

Objective: Hypervisor deployment, management configuration and testing

STEP	ACTIVITY	OWNER	DELIVERABLES
2.1	Installation of hypervisor and delivery of the workload domain(s) in accordance with design	Equinix	Completed installation log
2.2	Installation of monitoring and management agents and configurations	Equinix	Completed installation log
2.3	Configuration of the workload domain(s) in accordance with design	Equinix	Completed installation log
2.4	Configuration of agreed storage capacity in accordance with design	Equinix	Completed installation log
2.5	Configuration of connectivity in accordance in accordance with design	Equinix	Completed installation log
2.6	Delivery of the Managed Virtual Circuits in accordance with the order	Equinix	Completed installation log
2.7	Delivery of the Equinix Internet Access in accordance with the order	Equinix	Completed installation log
2.8	Delivery of the hypervisor operational console and access	Equinix	Completed installation log
2.9	Delivery of the Admin account for the Operational Console	Equinix	Completed installation log

Acceptance Into Service

Customer Access & Validation

Objective: Enable secure customer access to begin OS/hypervisor installation

STEP	ACTIVITY	OWNER	DELIVERABLES
3.1	iDRAC access confirmation	EMS	OOBM credentials & IP schema
3.2	Remote console access tested	Customer	Confirmation from IT lead
3.3	Walkthrough of Docs.Equinix.com	EMS + Customer	Live session for questions
3.4	Project close	Customer	Acceptance Into Service milestone

Transition Phase

Following the delivery of Hosted Private Cloud, the transition phase begins for the Equinix team responsible for managing the environment to review the initial documentation and establish execution of all routines and activities necessary to ensure the availability of the Customer's environment. Also, at this stage the necessary activities are carried out to maintain the SLA agreed to with the customer.

Some activities performed during the transition phase are:

- List risks and their severity for the Client
- Technical review of security policies
- Definition of plans for incident management

- Environment/Client escalation list definition
- Review of monitoring and consequent actions

The transition phase is expected to a maximum of 90 days and the goal is to allow both Equinix and customer to align on expectations, check environment implementation standards. Once the transition phase is complete, the Equinix team interacts with the Customer to formalize the validity of the Service Level Objective (SLO) for each defined environment. During the transition period no penalties for SLA disruption are applied.

Operational

RACI (Responsible, Accountable, Consulted, Informed) matrix for the HPC, showing clear ownership across EMS, the Customer, and Dell (as hardware supplier)

TASK / RESPONSIBILITY	EMS	CUSTOMER	DELL
Hardware provisioning (rack, cable, power)	R/A	I	C
BIOS/firmware versioning and compliance	R/A	I	C
iDRAC / OOBM setup and delivery	R/A	C	I
Hardware health monitoring (fans, PSU, drives)	R	I	I
Physical component replacement (e.g., failed drive)	R/A	I	C
Server diagnostics and log retrieval	R	C	I
Network handoff (cross-connect/Fabric setup)	R/A	C	I
Hypervisor installation and configuration	R/A	C	I
Operating System installation	I	R/A	I
Software patching and updates	I	R/A	I
Logical network / security config (inside OS or VM)	I	R/A	I
Application deployment and tuning	I	R/A	I
Integration with external cloud/SaaS	I	R/A	C
Infrastructure expansion (additional nodes)	R	A	C
Performance diagnostics (hardware-level)	R	C	C
Remote console and access verification	R	A	I
Initial onboarding coordination	R/A	C	I
Delivery and BOM validation	C	I	R/A
Incident management (hardware-related)	R/A	I	C
Incident management (software or OS-related)	I	R/A	I
24/7 Monitoring and alerting (hardware health)	R/A	I	I
Service request handling (adds, removals)	R/A	C	C
Proactive maintenance scheduling (firmware/hardware)	R/A	C	C
Access management to workload domain	R	A	I
Asset tagging and labeling	R	I	C
Compliance with physical security and IBX standards	A	I	I
Capacity Consulting	R/A	C	I

RACI Legend:

- R = Responsible: Executes the task
- A = Accountable: Ultimately owns the task's success/failure
- C = Consulted: Provides input or technical/operational support
- I = Informed: Needs awareness but does not act

Service Requests

There are two types of service requests available:

- **INCLUDED**: These Service Requests fall within the scope of the managed infrastructure and are covered under the standard service contract.
- **ADDITIONAL**: Service Requests which are out of scope of the Service and therefore are *best effort* and additional charges apply.

REQUEST NAME	EXAMPLE	INCLUDED/ADDITIONAL
Extended Remote Hands	Console-based OS installation assistance; Media mounting (virtual ISO or USB); BIOS or RAID configuration at customer request	Additional
Software-Layer Assistance	Troubleshooting customer-installed software; In-guest performance diagnostics	Additional
Network Configuration	Additional IP planning, VLAN creation, or Layer 3 routing (beyond handoff)	Additional
Custom Installations	Adding non-standard components (e.g., PCIe cards, USB dongles); Device firmware flashing outside EMS baseline	Additional
Capacity Consulting	Architecture reviews, scaling strategies, cloud integration mapping	Included
Project-Based Tasks	Migration support, DR configuration, multicloud setup	Additional
Emergency Off-Hours Work	After-hours tasks not related to an active P1 incident	Additional
Hardware Support	Disk, PSU, NIC, or fan replacements due to failure; iDRAC or OOBM connectivity troubleshooting; Physical diagnostics and health checks; Response to critical hardware alarms	Included
Basic Access Support	Credential resets for iDRAC or Fabric ports; Verification of cross-connects or power feeds	Included
Environmental Maintenance	Visual inspection (Smart Hands) for LED, cabling, labels	Included
Basic Remote Hands	Reboot or power cycle request (within EMS support hours)	Included
Administration	Updating customer contact list or access control entries	Included
Create a DC Group	Create a DC Group over multiple workload domain(s)	Additional
Change workload domain access	Change external access workload domain(s) API	Additional
Add/remove a user	Add a user for the workload domain(s)	Included
Change permissions	Change permissions for a user	Included

Note: Included means the request is part of the service and has no additional implementation cost. Additional means the service request has additional cost and its execution requires an approval in the EMS self-service portal.

All changes not listed in the table above can be requested by the customer by selecting “change” at the service request module. Equinix will perform an impact analysis to determine whether the change can be implemented and to determine associated costs and lead time.

Any charges related to Service Requests will be deducted from the Premier Support Plan Balance (See the Service Description for Premier Support for more details), or in case of insufficient balance invoiced in arrears based on the prevailing rate.

Changes in the baseline capacity, amount ordered or any other change that will have an impact on the monthly service fee should be requested via the Sales team.

Reporting

Upon customer request the following reports can be provided up to once per calendar month at no additional charge:

USE CASE	REPORT TYPE
Hardware Asset Audit	OME inventory + iDRAC exports
Pre-maintenance Planning	Firmware compliance & thermal reports
RCA (Root Cause Analysis)	iDRAC system logs & event histories
Risk Mitigation	Warranty expiration & power anomaly alerts
SLA Verification	Dell Infrastructure Uptime and power/thermal event logs

Service Levels

The purpose of this Service Level Agreement (SLA) is to define the measurable performance levels associated with the service and specify remedies available to Customer if Equinix fails to achieve these levels.

Incident Management

Incident management is included in service support. All incidents are handled based on priority. Priority is determined after the failure has been reported and assessed by Equinix based on the provided information.

Support

The SLA on support applies to the incident registration and resolution (see section Rapid Response of this document).

PRIORITY	RESPONSE TIME	RESOLUTION TIME	EXECUTION OF WORK	SLA
P1	< 30 min	< 4 hours	24 x 7	95 %
P2	< 60 min	< 24 hours	24 x 7	95 %
P3	< 120 min	< 5 days	24 x 7	95 %

Note:

- Response time is from submitting the Trouble tickets and an Equinix Managed Solutions specialist sending a formal response.
- Resolution time of a case is from registering to closing or cancelling the Trouble Ticket in the ITSM Tool or the hand over to customer.
- SLA applies to the support response time, details on the SLA can be found in the Product Policy.

PRIORITY	IMPACT/URGENCY	DESCRIPTION
P1 High	Unforeseen unavailability of a service / environment delivered and managed by Equinix, in accordance with service description due to a disruption. The user cannot fulfill its obligations towards its users. The user suffers direct demonstrable damage due to the unavailability of this functionality.	The service must be restored immediately; the production environment(s) is/ are unavailable, with platform-wide disruptions.
P2 Medium	The service does not offer full functionality or has partial functionality or a reduced performance, because of which the users are impacted. The user suffers direct demonstrable damage due to unavailability of the functionality. The service may be impacted due to limited availability of this functionality.	The service must be repaired the same working day; the management environment is not available.
P3 Low	The service functions with limited availability for one or more users and there is a workaround in place.	The moment of repair of the service is determined in consultation with the reporting person.

Availability

The availability level of the HPC service is shown in the table below and refers to the availability of a single OVDC considering the observance of certified blueprints and Digital Infrastructure Management pre-requirements. The HPC service is considered “Unavailable” when a failure in the infrastructure managed by Equinix means that the OVDC operating on it is in an error status and there is an interruption to the customer’s services caused directly by that error.

Availability SLA per month	Type of Environment	Infrastructure Resilience
99,95%	Production	Environment has full High Availability solution in place - When the management target has a HA or cluster solution in place
99%	Production	Environment has no High Availability solution in place - When the management target has no HA or cluster solution in place, so Equinix will need to act on repairing as soon as new item is in place

90%	Production	Equinix has limited access to environment - If for some reason any configuration, tooling or access has been limited or removed, Equinix is not able to deliver proactive services
85%	Non-production	Environment is used for nonproduction workloads - If the environment is not used for Production workloads, then Equinix will provide a lower SLA
No SLA applicable	N/A	Equinix access to environment was removed - If Equinix has no access to environment, partially or totally, will not be able to provide management or repairing activities

- A Service credit regime is available on the availability SLA, this is described in the Product Policy.
- If management target is customer owned, then customer is responsible to replace it if fails, and the SLA is calculated only during the period that Equinix team is working on repair.
- If management target is Equinix owned, then Equinix team will take necessary steps to replace it and repair it.
- If the customer execute changes on the environment without follows Equinix Change Management process, SLA may not apply.
- SLA applies to the availability, details on the SLA can be found in the Product Policy.

The availability of HPC does not include the restore of the data. Customers are responsible for restoring the data. When you have contracted Managed Private Backup, you can restore the data by using Self Service in the Managed Private Backup Operational Console or by asking as additional support. See Managed Private Backup Service Description for more details.

Other documentations

Where to find more documentation?

You will find the most up to date documentation on docs.equinix.com website.

Where to find EMS policy?

You will find it on our website.

Where to find official [manufacturer] documentation?

You will find it on https://docs.vmware.com [example]

How to ask for help

Please make sure to open a ticket every time you need help. This is your guarantee that the right team has received your request and will work on that under the expected SLAs.

