

Storage as a Service | blueAPACHE

Canonical: <https://www.blueapache.com/services/storage-as-a-service-private-s3>

Details:

Summary

Storage as a Service (Private S3) is our scalable, S3-compatible storage service for high-volume structured and unstructured data, with immutable storage options and a consumption-based commercial model. It was built with Hewlett Packard Enterprise, connects into emPOWER Cloud and the emPOWER Network, and in its case study holds health records across three data centres with fixed pricing and no ingress or egress charges. The service suits organisations replacing tape or legacy storage arrays, particularly where records must be retained for years and protected from alteration. The case study is undated and illustrative; confirm current inclusions, architecture and pricing in your proposal. The contractual summaries below describe General Terms v3.6, so confirm the version applicable to your order.

Key facts

Label	Value
Service	Storage as a Service (STaaS), Private S3, emPOWER Cloud pillar
Interface	S3-compatible object storage
Data types	High-volume structured and unstructured data
Immutability	Immutable storage option; in the pathology case study data cannot be deleted or changed unless an authorised user is physically at the registered device
Resilience (as deployed in the case study)	Data protected in real time across three data centres
Technology partner	Hewlett Packard Enterprise; we cited as HPE Service Provider of the Year 2021
Pricing	Consumption-based; case study states fixed, predictable pricing with no egress or ingress charges, lockable over multi-term contracts
Connectivity	Own core network fabric with connectivity to emPOWER Cloud and emPOWER Network, and to public and private clouds
Certification	emPOWER Cloud Services (IaaS) in scope of ISO/IEC 27001:2022 certificate 202507-118
Data residency	Our general sovereignty statement describes Australian storage and processing; confirm all

	relevant locations and access arrangements for your STaaS deployment
Default contract term in v3.6	36 months except Professional Services, unless the Service Description or Service Order specifies otherwise

What is included

The pathology provider case study is the detailed published description of the service in operation. Our STaaS, built with HPE, is described as cloud-agnostic and removes the need to store and retrieve data from tape. Data is stored with immutability, so records cannot be deleted or changed unless an authorised user is physically present at the registered device. Data is protected in real time across three data centres. Authorised users can access it from anywhere, unlike tape. The service has its own core network fabric providing high-speed, secure connectivity to public and private clouds, supports multi-cloud environments, and offers additional connectivity to emPOWER Cloud and emPOWER Network. The undated case study attributes fixed, predictable pricing and no ingress or egress charges to that solution's own core network connectivity. Confirm current pricing, usage limits and extraction charges for your proposed service.

What is not included

The case study and page do not state a retention period, a replication schedule, an object-count or capacity ceiling, or a separate uptime figure for the STaaS tier; the 100 per cent storage uptime figure is published for emPOWER Cloud's HPE Primera arrays, not specifically for STaaS. Immutability is an option to be configured per bucket or dataset, not a default the buyer should assume.

Storage capacity does not by itself establish a backup commitment. Read the express backup scope in the Service Order, Service Description and applicable Schedule together, including clauses 3.14 and 17.3 of General Terms v3.6. Clause 3.15 sets customer backup duties where the Services do not include backups. It is also not disaster recovery, which is emPOWER IT Continuity Services with an agreed Restore Time Objective. Responsibility for the lawfulness and record-keeping compliance of the stored data stays with the customer under clause 17.1, including obligations under taxation law, State Record Acts or Archives Acts; assistance with those obligations is available as a Professional Service.

Who it is for

The case study profile is a private pathology provider with hundreds of clinics that must, by law, keep sampling information and health records for at least 10 years and needed to integrate data from third-party suppliers. More generally the service suits organisations with large archives, long statutory retention, a need for tamper-proof storage, and a preference for fixed monthly cost over unpredictable tape logistics or public-cloud egress fees.

How it is delivered

Onboarding follows the Transition In Services in clause 8. Data migration from tape or legacy arrays is scoped per engagement; the case study does not quantify the volume migrated or the migration duration. Capacity is consumed through the S3 interface and expands with demand. Confirm the platform-management responsibilities and whether your deployment uses the shared blueAPACHE Environment. Where clause 5.1 applies, it permits specified software updates and replacement of

components with similar or superior components without prior consent; the service name alone does not establish that every deployment falls within that clause. Customers must provide 24x7 remote access to relevant components and keep their own software current and licensed (clause 7.1).

Commercial model

The case study adds that pricing is fixed and predictable, can be locked in over multi-term contracts, and carries no egress or ingress charges. Under clause 12, usage-based fees are invoiced monthly in arrears subject to any Minimum Spend, fixed fees monthly in advance, and usage may be rounded up to the nearest whole unit (the terms give 1.4GB rounded to 2GB as the example). Where pricing is in usage bands, the customer may request a band change, subject to any fee and the Minimum Spend (clause 12.3). Request the current capacity rate, minimum commitments and any retrieval or exit charges for your proposed service.

Support and service levels

Service Levels are only those stated under the "Service Level" heading in the Service Description, measured by our tools, and subject to the Reasonable Excuse carve-out; the general terms contain no service credit regime. Monthly performance reports arrive within five Business Days of month end. Clause 3.10 requires best efforts to carry out scheduled maintenance within the Schedule windows, or at other times with at least three Business Days' prior notice, and with minimum disruption to the customer's business. Emergency provisions are separate.

Related services

Offsite Backup, Private and Public SaaS Backup, Disaster Recovery, emPOWER Cloud, Core Network and Data Centre Interconnect, and Advanced Infrastructure Managed Services are related offerings. Confirm supported interfaces, backup targets, network paths and operational responsibilities in the solution design; listing these services does not establish interoperability or inclusion in every STaaS order.

Buying questions

Contract term and renewal. General Terms v3.6 provide a 36-month default Minimum Service Period from the Service Commencement Date, except Professional Services and where the Service Description or Service Order specifies otherwise. Confirm the version and negotiated terms applicable to your order. Clause 2.8 addresses written notice before the Service Period ends. Under clause 2.10, renewal may also be agreed by email or fax with or without a signature, or by continued use. If the customer gives no notice under clause 2.8 but continues to access or use services after the period ends, clause 2.9 extends all Services on that agreement for three months at the then-current full list price, with defined Service Levels not applying during that period. The undated case study describes pricing lock-in over multi-term contracts; confirm the current offer.

Termination. Customer: unremedied breach after 20 Business Days, blueAPACHE insolvency or ceasing business (clause 24.1). blueAPACHE: non-payment after five Business Days, specified breaches after 20 Business Days, insolvency, change of control (clause 24.2). Early Termination Payment under the Schedule and immediate payment of unmet Minimum Service Period or Minimum Spend (clause 25.2). We may also suspend or cancel a Service on end-of-life or upstream supplier grounds under clause 3.26 without a fixed notice period.

Exit. We delete Customer Data at the end of the Service Period at no cost and the customer must take their own copy first (clause 9.1). For a large archive, agree the exit window, export format and the network path for bulk extraction; confirm whether the case study's no-egress-charge position applies to your order, including bulk export at exit.

Data protection and residency. Our general data-sovereignty statement describes Australian storage and processing; confirm the location of data, replicas, logs and support access for your deployment. General Terms v3.6 impose mutual Privacy Act obligations and notification immediately, and in any event within 24 hours of discovery, of an eligible data breach involving the other party's Personal Information. Clause 18.3 records consent for specified overseas destinations where necessary or convenient to provide the Services, alongside its other conditions; this is not a statement that every deployment transfers data overseas. Clause 18.6 includes a customer warranty against providing GDPR-regulated personal data. Confirm the applicable agreement and any required variations.

Liability. Under General Terms v3.6, the general cap per Claim is the greater of amounts paid under the Service Agreement in the three months before the Claim first arose and \$25,000, subject to clauses 19.1, 19.2 and 19.4 and applicable law. Clause 19.4(a) addresses liability for loss of or damage to Customer Data: it excludes that liability where no relevant backup or disaster recovery obligation exists, and where such an obligation exists and is breached limits it to the specified restoration cost. Read it with clauses 19.1 and 19.2, applicable law and the complete agreement.

Defining retention and retrieval together

Identify data, applications and retention and deletion rules. Where immutability is part of the design, establish how retention is set and administered. Storage durability, backup and application restoration are different outcomes. Agree retrieval and exit alongside storage, including the format and access a replacement system needs. The pathology example's retention and commercial terms should not be assumed for every storage customer.

Which document defines the commitment

The published General Terms v3.6 give the Service Order precedence over the General Terms, followed by the Schedules and then the Acceptable Use Policy (clause 2.3). Record the agreed scope, exclusions and negotiated departures in that document set. Keep the versions supplied at signing with the executed order and signed variations. Two offers with the same service name can cover different systems, operating hours or responsibilities.

Confidential information and access

Clause 16 provides mutual confidentiality protection. It covers information marked confidential, information identified orally and confirmed in writing within 30 days, and information that should reasonably be understood to be confidential. Customer Data, Customer Records and Customer Software are included; our agreement and fees are also confidential. Permitted disclosures include appropriately bound personnel on a need-to-know basis and specified professional advisers, with other exceptions in the clause. Identify who may receive operational reports, configuration details and commercial information. Access to information to deliver the service is not a general permission to circulate it.

Customer content and take-down requests

Clause 14 distinguishes operating the service from responsibility for the customer's content. It requires the customer to notify us promptly of relevant take-down notices or directions and comply with them.

The terms also reserve rights for us to restrict or remove Customer Data in specified circumstances, including suspected agreement breaches or exposure to harm or liability. These rights are separate from routine availability commitments. Agree who receives regulatory notices and who can authorise operational action, and retain the notice and decision record. The full clause, including its discretion and good-faith wording, is explained in the terms guide.

Responsibility across the delivery chain

The published terms allow us to subcontract all or part of the Service Agreement without customer consent or a notification requirement. Clause 27.5 nevertheless makes us liable for our subcontractors' acts and omissions to the same extent as for our employees. This differs from a third-party supplier contracted directly by the customer. Identify which arrangement applies to each dependency in the design. Where supplier identity, delivery location or change notification matters, request a documented supplier list and put any agreed notification or approval requirement in the Service Order; the general clause does not supply that visibility automatically.

Continuity when an external event interrupts service

Clause 23 addresses force majeure separately from normal incident management. Performance is suspended to the extent a qualifying event causes delay or failure. The definition includes specified events outside reasonable control; it is not a blanket classification of every outage. If the delay exceeds 20 Business Days, the other party may terminate by written notice. The clause also requires payment for services to termination and the applicable Early Termination Payment. A continuity plan should cover operational recovery and the commercial consequences of prolonged interruption. Confirm the Schedule's exit calculation rather than assuming an externally caused outage creates a cost-free exit.

Related

Cloud pillar hub

emPOWER Cloud

Offsite Backup as a Service

Private and Public SaaS Backup

Disaster Recovery as a Service

emPOWER Core Network and Data Centre Interconnect

Advanced Infrastructure Managed Services

Case study: blueAPACHE on HPE GreenLake

Industry: Healthcare and aged care

Industry: Government and public sector

Partners

Service Agreement terms

Support

Contact blueAPACHE

What is S3-compatible storage?

Object storage that speaks the Amazon S3 API, so applications, backup tools and archiving systems written for S3 can use it without change. Our service provides this on private infrastructure it manages,

rather than on a public cloud.

Is the storage immutable?

Immutable storage is an option. In the pathology case study, health records and sampling data are stored so that they cannot be deleted or changed unless an authorised user is physically at the registered device, which is the control that makes the archive tamper-resistant.

Where is the data held and how is it protected?

In Australian-based data centres under Australian legal jurisdiction, per our data sovereignty statement. In the case study deployment, data is protected in real time across three data centres.

Are there egress or ingress charges?

The undated pathology case study describes no ingress or egress charges, fixed and predictable pricing and multi-term pricing options for that solution. Confirm current charges and any conditions in your Service Order, including bulk extraction at exit.

Who is the technology partner?

The undated pathology case study describes the STaaS solution as built by blueAPACHE with Hewlett Packard Enterprise. Confirm the infrastructure proposed for your deployment.

Does putting data in STaaS mean it is backed up?

Storage and backup are distinct capabilities. Check the express backup duties across the Service Order, Service Description and applicable Schedule, including clauses 3.14 and 17.3 of General Terms v3.6. Where backup is not included, clause 3.15 imposes customer backup duties. Data-loss liability must be read with clauses 19.1, 19.2 and 19.4, applicable law and the complete agreement.

What uptime applies to the storage?

The STaaS case study and page do not state a separate figure, so the contractual Service Level for STaaS is whatever is written under the "Service Level" heading in the Service Description.

How is it priced?

On consumption, with capacity expanding as needed. Usage fees are invoiced monthly in arrears subject to any Minimum Spend, usage may be rounded up to the nearest unit, and usage bands can be adjusted on request.

Can the storage connect to public clouds?

The undated pathology case study describes connectivity to public and private clouds, multi-cloud support and connectivity to emPOWER Cloud and emPOWER Network. Confirm supported destinations, interfaces and paths for your design.

What is the minimum term and what happens at the end?

General Terms v3.6 provide a 36-month default Minimum Service Period from the Service Commencement Date, except Professional Services and where the Service Description or Service Order specifies otherwise. Confirm the version and negotiated terms applicable to your order. The exit provisions require the customer to take copies of Customer Data before the Service Period ends and provide for deletion from the blueAPACHE Environment at no cost, alongside other return duties. Agree the export plan for a large archive before exit.

Who is responsible for the legality of what is stored?

The customer, under clause 17.1, including record-keeping obligations under taxation, State Record and Archives legislation. We can help with those obligations as a chargeable Professional Service.

What is your Storage as a Service (Private S3)?

Our Storage as a Service (Private S3) is a scalable private S3-compatible storage solution for high-volume structured and unstructured data, offering immutable storage options and a consumption-based service model. It provides private S3-compatible capacity, resilience, and managed infrastructure.

Does your Storage as a Service offer immutable storage?

The service offers immutable storage options. The undated pathology case study describes health records and sampling data that could not be deleted or changed unless an authorised user was physically at the registered device. Confirm the immutability controls and retention settings for your deployment.

What pricing model do you use for Storage as a Service?

The service is described as consumption-based. The undated pathology case study reports fixed, predictable pricing without ingress or egress charges for that solution. Confirm current rates, minimum commitments, usage conditions and exit charges in your quote.

What data protection features does your Storage-as-a-Service provide?

The undated pathology case study describes real-time protection across three data centres and multi-cloud archiving. These are attributed deployment details; confirm redundancy, replication, recovery objectives and supported cloud integrations for your proposed service.

What compliance standard does your Storage-as-a-Service adhere to?

The undated pathology case study describes its multi-cloud archiving solution as complying with ISO27001. That statement does not establish the current certification scope of every Storage-as-a-Service deployment. Request the current certificate and confirm the applicable service, platform and facilities.

How does your Storage-as-a-Service integrate with its other cloud services?

The pathology case study describes a core network fabric connecting public and private clouds and additional connectivity to emPOWER Cloud and emPOWER Network. Confirm the paths, interfaces and integrations included in your design.

What service category do you classify this offering under?

The page categorizes Storage as a Service (Private S3) under the 'Cloud' category, with a service type of 'Cloud, backup and recovery', and it is offered in Australia.