Infrastructure-as-a-Service (IAAS) Offer: Mozambique

Technical Specification Datasheet
Version 1.0.4, August 2024

COMMERCIAL IN CONFIDENCE

Terms and Conditions

This Datasheet is provided with accurate information at the time of publishing.

Bubble reserves the right to update or alter any technical specification of the service in question at any time, in which case an updated version of this technical specification will be published within 30 calendar days of such a change.

If any clarification is required about the technical capabilities of any part of this Service Offering, please contact your Bubble Account Manager, or the Bubble Sales team at: connect@bubble.co.mz.

Contents

Feature Set

This section describes the features available to a Customer once an IAAS Tenancy Agreement has been established.

Unless otherwise specified below,

- all features will be provided within a single, logically isolated customer tenant (private cloud) hosted by a single physical datacentre
- all features will be available to customer via self-service provisioning and configuration through a secure web portal
- The features will be subject to the resource limitations expressed in terms of compute, memory, networking and storage resources set out in the IAAS Tenancy Agreement.

This document is focused on describing technical and operational characteristics of the IAAS Offer, however where relevant it will highlight features which may incur an additional charge to the customer. For pricing information about any feature, please contact your Bubble Account Manager, or the Bubble Sales team at: connect@bubble.co.mz.

Administrative Access

Customer will be provided with a single superuser account to our web portal, which is based on VMWare Cloud Director technology.

- This account must be secured with **2FA**
- This account will have permissions to create additional administrative user accounts, using the predefined roles offered by VMWare Cloud Director
- The web portal is accessible via the secure HTTPS protocol

This web portal assumes that administrative users have an appropriate level of skill with the administration of virtual machines and associated compute, networking and storage services.

Content Library

Customer will have access to the portal to a content library, structured as a hierarchical filesystem.

Customer can upload ISO and other support files for provisioning VMs to this library.

The content library will also contain ISOs made available by Bubble for popular operating systems. Major versions N and N-1 will be available for the following operating systems.

- Linux:
  - Ubuntu Server 20.04: Latest Stable
  - Ubuntu Server 22.04: Latest Stable
- Windows:
  - Windows Server 2019: Latest Stable
  - Windows Server 2022: Latest Stable

Windows Licensing: customers who choose to install a Windows Operating System on a VM may choose between two licensing models:

- Bubble-provided Licensing: Bubble will provide a Product Key for each VM, and incorporate the appropriate license fee in the monthly service charge for the VM.
- Customer Licensing: subject to an approval process by Microsoft, customer may bring a previously-purchased license, using any of the purchasing models offered by Microsoft, and apply product key to the VM.

Virtual Machines (Compute Nodes)

The customer may create, provision, start, stop and destroy any number of Virtual Machines (VMs), within the following parameters:

- CPUs: between 1 and 32 virtual CPUs with the following specification:
  - Equivalent to or exceeding a single core of an Intel Xeon 3rd Generation 2.0Ghz Processor
- RAM memory: between 1 and 384 Gb, clock speed 3200 MHz or above
- Block device storage: 1 or more Gb of Directly-attached storage with the desired performance tier (see below) for OS and Application stack installation
- Additional storage may be provisioned and attached, based on any of the five performance tiers (see below)
- Network interfaces: 1-4 Network Interfaces with speed equivalent to Full Duplex Gigabit Ethernet
- Hypervisor: VMWare ESXI, 8.0 series

Machine Images/Templates

Customer may export any VM to a VMWare OVA file to be stored in the content repository. This file may be used to rapidly create and provision additional identical VMs.

VApps

Customer may group one or more VMs as a logical unit, using the VMWare VApps feature. This simplifies typical administration tasks such as startup/shutdown sequencing and resource management.

Networking

Basic Networking

The customer may define any number of local subnets with the following parameters:

- Network address and subnet mask
- Inter-subnet routing allowing complete control of isolation
- Firewall rules at the level of IP, TCP and UDP

Public Internet Connectivity

Customer may purchase one or more fixed public IPv4 addresses from Bubble, for exposing applications hosted on the tenant, to the public internet.

DHCP

DHCP-as-a-service is provided, with the following parameters:

- Allocated Address range

- Address reservation by host MAC address
- Lease expiry time
- DNS addresses for hosts
- Routing table for hosts

DNS

Customer VMs may perform DNS resolution via any of:

- a VM within the tenant on which customer installed an appropriate DNS service
- a DNS service within a customer datacentre, linked to the tenant via a VPN
- a DNS service on the public internet

Load-Balancing

Multiple load-balancing scenarios can be self-provisioned by the Customer, via the customer portal, using the NSX Advanced Load Balancer, which provides multiple advanced features:

- Web application load-balancing for HTTPS
- Other L4 and L7 load-balancing configurations
- Web Application Firewall with DDOS and Bot protection plus access to automated threat updates from VMWare Cloud Services
- Traffic monitoring and insights

This feature may require an additional monthly fee.

VPN

Bubble recommends that customer establish an IPSEC VPN from the tenant to customer's on-premise datacentre.

Performance

Scalability

Customer may increase physical resources available to any VM on-the-fly (no restart required), subject to the defined resource limits of their tenant and VMWare best practice.

Storage

Storage performance of the VMWare vSAN cluster which underlies the virtual storage devices provided to customer VMs is optimized for typical business application workloads.

The customer may contract for any volume of storage to be available for their tenant, and then attach this storage to Virtual Machines via the self-service portal. Storage is available in five performance tiers, each with a different charging structure.

- <u>Enterprise</u>: up to 10,000 I/O operations per second (IOPS), ideal for IO-intensive workloads, mission-critical applications and high-performance databases.
- <u>Performance</u>: up to 6,000 IOPS, for applications requiring consistent high performance. Provides reliable data access with moderate latency, suitable for demanding workloads such as real-time analytics, high-traffic websites, and online transaction processing.

- Standard: up to 2,500 IOPS, provides reliable data storage with moderate performance, making it suitable for a wide range of low and medium workload applications, including web hosting, content management systems, development environments and warm standbys.
- Capacity: up to 1,000 IOPS, providing cost-effective storage for read-rarely data such as images, scanned documents, archives and recent backups.
- Backup: unspecified IOPS, prioritises data retention and affordability, for long-term retention and disaster recovery and compliance purposes.

NOTE: the IOPS ranges given above are indicative. Performance measurements for specific customer applications should be simulated upon arrangement with Bubble customer service team.

Security

This section describes key aspects of the security provided by the IAAS Service. Unless otherwise specified, these security aspects apply to all features specified above.

Physical Locations

The service is provided from the following physical datacentre locations within Mozambique:

- MZ-SOUTH-1: iColo MPM-1 Facility, Maputo City: https://www.icolo.io/location/mpm1/

Data Sovereignty

All compute, storage and networking capability is physically located within Mozambique.

Customer should provide their own connectivity to Bubble datacentre's gateway router via one of the following options which ensure that all data transmission to and from our IAAS service takes place within Mozambique:

- Leased Line directly from Customer datacentre to MZ-SOUTH-1 datacentre
- VPN established over public internet, via a 3rd-party Internet Service Provider who confirms that they have a peering arrangement with iColo Maputo.

Management of the Bubble datacentre is performed by technical teams based in Mozambique and South Africa, using a secure access portal.

Access to a customer's compute resources and data hosted within the Bubble cloud will be provided to governmental authorities or other third parties subject to the following conditions:

- Upon written request by an entity with legal authority to supervise the customer's operations, subject to written authorization from the customer
- Upon receipt of a court order by a Mozambican tribunal

Data Security

Resource Availability

All CPU and RAM resources are provided from a unified pool of physical resources managed by a VMWare vSphere Management Cluster (Control Plane). The Management Cluster uses a High-Availability configuration based upon multiple physical nodes.

In the event of failure of any physical resources, customer VMs will be automatically migrated to alternative physical resources – this may imply a service interruption while the new VMs are provisioned and started.

All storage available to customer VMs is based upon a redundant configuration of physical media with characteristics equivalent to RAID-5.

All network connectivity to VMs is provided via redundant physical Network Interface Cards (NICs).

Bubble provides an overall availability guarantee of 99.9%, measured over each calendar year.

Integrity

Customer access to administration portal is subject to various security features offered by VMWare Cloud Director Tenant Portal, including:

- Predefined and custom role definitions
- Optional 2FA for individual users
- Organization-wide password policies

Customer may permit Bubble support team to access customer logical resources upon customer request, by defining a support account via customer portal, and providing credentials to Bubble support team.

All Bubble support team members access the cloud management console using accounts which are protected by IP Address Geolocation as well as 2FA.

Backup and Recovery

Bubble offers the following features to facilitate customer compliance implementation of backup routines for their VMs:

- Backup-as-a-service of entire VMs based on customer-defined intervals and retention periods
- Transactionality-aware interface for VMs hosting Databases: Oracle, SQL Server, PostgreSQL and MySQL supported.
- Point-in-time recovery of single files, multiple files, directory trees or entire VMs.
- Detailed feature set is shown below

Note: this service may require an additional fee.

Feature	**Description**
Ease of Use	Single pane of glass management.
Ransomware/Anomaly Detection and Diagnostics	Detect anomalies and encryption. Determine if the ransomed content contains any sensitive data.
Ransomware Protection	Backup data is not accessible over network. • Air gap • Immutable • Encryption
Scalability	Accommodate capacity growth through a distributed architecture for fast deployment.
Resiliency	Self-healing approach with distributed metadata, web scale file system and erasure coding.
Deduplication/Compression	Reduce total capacity required for data protection.
Reporting/Alert	Granular reporting and alerting capabilities.
API Integration with Automation Frameworks	Rest APIs can be integrated with automation frameworks.
Data Security & Immutability	Data is not written in native format. Once written it is inaccessible. Any incremental changes are written separately in non-native format.
Live Mount	Live Mount for recovery in negligible time.
Granular Recovery	Granular recovery for most workloads at file level.
Role Based Access Control	Provides object level access control, including MFA.
Cloud Tiering	Use of lifecycle management to move the data to a lower cost tier for long term storage.

Physical and Environmental Security

The physical datacentre which hosts the customer's cloud tenant provides the following features:

Access control

24/7 physical security including 24 x 7 on-site security team, CCTV with 24 x 7 monitoring, internal site security barriers.

Power supply

Site has secure permanent power supply with N+1 generator backup, providing 99.999% availability.

All physical hosts have redundant power supply with hot-swap capability.

Cooling

Temperature control with N+1 CRACS Redundancy.

Humidity control.

Fire prevention

Fire detection with automated suppression system, supported by manual backup.

Standards

The supplier which operates the MZ-SOUTH-1 datacentre is in the process of obtaining certifications against the following international standards related to information security, and anticipates completing the certification process in 2024:

- ISO/IEC 27001:2022
- PCI-DSS 4.0

Network Security

Gateway Firewall

VMs may be exposed to external networks (customer datacentres and/or the public internet) via VMWare NSX, a stateful L4–L7 firewall including:

- NAT and PAT
- Software L2 Bridging to Physical Environment
- VPN - L3 (IPsec VPN and SSL VPN)
- L7 application identification
- Source/destination address range restriction
- URL filtering for egress traffic
- Source reputation for ingress traffic
- Distributed Switching and Routing
- Stateful Gateway Firewall
- Dynamic Routing with ECMP (Active- Active)
- Virtual Routing & Forwarding (requires additional configuration by Bubble support team, and may be subject to an additional fee)

Monitoring and Reporting

Monitoring and Alerts

Bubble Support team will receive alerts when a customer VM or its associated resources approach resource limits or exhibits uncharacteristic behaviour.

Customer may configure similar alerts to be sent directly to their team members via email and SMS.

Reporting

Customer may access and download via portal, multiple reports about the behaviour, performance and resource consumptions of their VMS and associated resources.

Compliance and Regulations

Local Data Residency Requirements

Bubble Cloud supports adherence to the current regulatory requirement (*Bank of Mozambique's Aviso 04-GBM-03*) stipulating that commercial banks must physically situate their datacentres within Mozambican territory. We ensure that all data is stored and processed exclusively within the borders of the country, offering a fully compliant solution for financial institutions operating in Mozambique.

Information Technology Risk Regulation

Bubble Cloud is aware of the current regulatory requirement (*Bank of Mozambique's* A*VISO Nº.04/GBM/13 - Anexo II – Risco de Tecnologias de Informação*) and prepared to align with customer initiatives which comply with this regulation.

Future Regulatory Developments

As Mozambique's regulatory landscape evolves, Bubble is committed to supporting its clients' compliance efforts. We are actively monitoring regulatory developments and are prepared to align our services with any forthcoming detailed requirements, with particular regard to:

- Resolução 69/2021 of 31st December - *Política de Segurança Cibernética e Estratégia da sua Implementação*
- the anticipated Cyber Risk Management regulation, currently in preparation by the Bank of Mozambique (*cf. the consultation published in January 2023 Proposta de Aviso que Aprova as Directrizes de Gestão do Risco e Resiliência Cibernetica*)

Assistance with Regulatory Reporting

While there are currently no specific regulatory reporting requirements, Bubble is poised to assist clients in meeting any future obligations that may arise from upcoming regulations. Our team is dedicated to staying informed about the evolving regulatory framework, and we are ready to implement necessary measures to support our clients in fulfilling their regulatory reporting responsibilities.

Privacy Requirements regarding Personal Data

Mozambique has not yet approved specific legislation regarding personal data or privacy, however Bubble is prepared to work with customers who require specific features in order to comply with global corporate policies and all non-national standards such as the EU's General Data Protection Regulation (GDPR) or South Africa's Protection of Personal Information Act (POPIA).

Standards

Bubble's status with regards to compliance with relevant standards is as follows:

- ISO9001:2015 compliance pending, certification is anticipated by 2024.
- ISO27001: compliance pending, certification is anticipated by 2024.
- VMWare Cloud Verified: compliant

The cloud was built and is maintained by a VMWare Cloud Verified Partner, meaning that it uses an architecture and best practice recommended by VMWare. Certification status may be verified at https://cloud.vmware.com/providers/cloud-providers/strategix-technology-solutions-pty-ltd.

Further information about the VMWare Cloud Verified Programme is available at: https://www.vmware.com/vmware-cloud-verified.html

Data Ownership and Migration

Data Ownership

Customers retain full ownership of their data at all times. We act as custodians, ensuring the security, availability, and integrity of the data stored on our cloud platform. Our commitment to transparency is reflected in the comprehensive Master Services Agreement which customers enter into. The Data Ownership policy set out in this agreement clearly outlines the rights and responsibilities of Bubble and the Customer with regard to data ownership.

Migration away from Bubble Cloud

We define a straightforward process for clients wishing to retrieve or migrate their data. This includes transparent time limits for migration and any associated charges, if applicable. The goal is to facilitate a seamless transition for clients opting to switch providers, minimizing disruption to their operations.

For detailed information, please refer to our Master Services Agreement (MSA).

Service and Support

The cloud service is supported by a team with elements in Mozambique, South Africa and Europe, including a permanent on-the-ground presence in Maputo.

Accessing Support

Customer will have access to a web-based support portal which can be accessed via internet browser, mobile-phone or email, through which they can create and monitor support tickets.

Customer will provide primary and secondary technical contact points within their team who may be contacted by email or phone by Bubble support team when processing a support ticket.

Support Language

Customers may interact with our support team using either or both of the following languages:

- English (EN)
- Portuguese (PT)

Support Response Times

Once a ticket is created, first response times from the support team are as follows:

- Production system down: 1 hour

- Production system impaired: 2 hours
- Other system or component impaired: 3 hours
- General Guidance: 4 hours

Proactive Support

In the case of the Bubble Support Team detecting an incident with a customer VM which requires customer intervention to resolve, which is not resolved within 24 hours, Bubble Support Team will create a ticket and proactively contact customer to resolve.

In the case of security-related incidents, the Bubble Support Team may intervene immediately it detects an incident if warranted by the incident's severity level. In specific cases this may require limiting or deactivating a VMs access to network, compute or storage resources. In such cases the Bubble Support Team will immediately issue an initial written notification to the customer contact points and follow this up with a telephone call.

System Upgrades and Service Interruptions

System Upgrades

Bubble performs proactive updating of system software supporting the local cloud on a quarterly basis. These updates/upgrades may be required to resolve/enhance security risks, feature enhancements, and bug fixes.

During the execution of these updates, an orchestrated process is executed, leveraging features like VMware vMotion to seamlessly migrate VMs between physical resources, ensuring continuous operation. Additionally, load balancing mechanisms are implemented to distribute workloads optimally, preventing performance bottlenecks during the update process.

Security Upgrades

Security-related patches for CVE vulnerabilities rated as High (CVSS of 7.0 or above) will be applied within 48h of being made available by VMWare.

Incident Response

In the event of a major incident causing service interruptions for customer tenants, a comprehensive response protocol is enacted to swiftly address and mitigate the impact. This includes but is not limited to incidents such as cyber-attacks and provider power or network communication interruptions.

An incident response team is activated to assess the situation, initiate recovery procedures, and communicate transparently with affected parties. Contingency plans are implemented to restore services efficiently, with a focus on minimizing downtime and ensuring data integrity while regular updates are provided to customers throughout the resolution process.

Planned Downtime

The maintenance interventions described above will, in general, not impact service availability to customers.

If a maintenance intervention will impact service availability, this maintenance windows will be communicated to customers at least 2 weeks in advance, allowing them to plan accordingly. The only exception to this advance notice period will be Security Upgrades as defined above, in which case Bubble reserves the right to reduce the notice period to 1 calendar day.

Service Lifecycle and End-of-Life

In order to deliver 'As a Service' solutions which follow emerging industry technologies and best practice, we may sunset (also known as End-of-Life/EOL) a specific feature or service. In such cases, Customers will be provided with a minimum of 12 months' notice of the scheduled "end of life" for the service.

This notification will include an explanation of the reasons behind the decision, such as the age of the service and its diminishing relevance to evolving customer needs. The deprecation of a service is motivated by a need to offer a more advanced and feature-rich alternative.

By transitioning to an enhanced service, customers not only retain existing functionalities but also gain access to additional features that cater to their evolving requirements.

Environmental Sustainability

Bubble is committed to driving sustainability through our service offers. By consolidating and optimizing compute resources we achieve greater energy efficiency, reduced carbon footprint, and overall resource optimization.

Bubble cloud helps minimize unnecessary energy usage – and thus emissions of CO2 – at two levels:

- at the physical level, the underlying datacentre operates with modern, efficient manner, supported by an automated Building Management System that helps monitor and control various building parameters to ensure optimal conditions and energy efficiency.
- Processing hardware is latest generation Lenovo server hardware, which therefore benefits from Lenovo's approach to sustainability, including:
  - Use of appropriate materials and recycled content in product manufacture
  - a production approach which seeks to minimize air and water pollution
  - Multiple energy management features at the server level
- At the logical level, the VMWare ESXi cluster which underlies the Bubble IAAS offer, constantly optimizes compute resources in multiple ways to minimize the overall energy footprint of customer workloads. More information about this can be found at: https://blogs.vmware.com/vov/2023/08/14/how-vmware-it-is-increasing-its-sustainability-green-score/

Charging and Billing

Customer can access resource usage reports via the portal, in order to understand the actual historical resource usage by their VMs.

Customer can define alerts to be issued whenever predicted or actual monthly spend exceeds defined limits.