# Cloud Compute Services

## SERVICE DESCRIPTION

CloudCompute

# CONTENTS

These Product Specific Terms apply to the provision of the Cloud Compute Services and shall form part of and be incorporated into the General Terms.

## Summary

Vivio Cloud Compute Services deliver a number of Infrastructure as a Service (IaaS) products, notably Compute, Storage and associated network elements such as Firewalls and Load Balancers. Together, they are designed to provide SME customers with a fully functionally public cloud-based infrastructure to meet their application requirements. In addition, the service offers an optional 'Backup as a Service' application which customers can use to back-up their cloud data.

Whist the customer remains responsible for managing their own applications, the underlying infrastructure on which it runs is now part of a managed service as described within this document.

## Security

Vivio is responsible for the security of the Cloud Service and shall be solely responsible for the provision of appropriate technical expertise, knowledge and resources to correctly request the appropriate configuration of the firewall services required by the Client.

Vivio will use its reasonable endeavours to provide as secure a protection as possible but the Client acknowledges that no firewall is completely secure or proof against all external threats such as viruses, malware and other unauthorised intrusions.

Vivio shall have no liability to the Client for any direct or indirect costs suffered by the Client in the event of any penetration of the firewall by any third party or third-party software save in cases of fraud or negligence on the part of Vivio or an employee or sub-contractor of Vivio.

The Client also remains responsible for the security of:

- The Operating System
- Applications
- Data in transit
- Data at rest
- Data Stores

## Amazon Web Services / Microsoft Azure

Vivio's Cloud Compute services are primarily deployed on Amazon Web Services (AWS) or Microsoft Azure, platforms that are highly reliable, scalable and cost effective infrastructure platforms in the cloud that power hundreds of thousands of businesses in 190 countries around the world.

AWS and Azure are secure, durable technology platforms with industry-recognized certifications and audits: PCI DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 and SOC 2 audit reports. Their services and data centres have multiple layers of operational and physical security to ensure the integrity and safety of your customer's data.

## Core Product Set

In order to provide a complete functioning infrastructure, the following core product components are required to be created during the initial Client order: Compute (Virtual Servers), Storage and Networking.

## Compute Function – Servers

The servers are virtual machine instances which are built including an operating system chosen by the Client. The cost of the server includes the OS which will be pre-installed and ready to go. The current list of available operating systems are: -

- Windows Server 2012, 2012 R2, 2016 and 2019
- SUSE Linux Enterprise Server (Various)
- Red Hat Enterprise Linux (Various)
- Ubuntu Server (Various)
- Other operating systems may also be supported upon request or as they are added by AWS / Microsoft

***Note:*** *Vivio is not responsible for maintaining the OS and/or providing any updates or patches to the O/S.*

The service provides a range of virtual servers that are differentiated in terms of processing power (CPU), memory and IO capability.

Unless specifically arranged otherwise; all Virtual machines will be deployed using 64-bit architecture.

Each server has a specific number of processors and amount of memory allocated; if the Clients requirements change, the server can simply be replaced by a more suitable alternative with a minimum amount of downtime.

Naming convention – Whilst Vivio will use a pre-defined naming convention; the portal description and billing file will include both the product and Client defined name.

The servers are proactively monitored and are configured to automatically alarm if predefined thresholds are met. (see support section)

They are segmented as follows:

## Applications that can be Hosted

Almost all modern applications can be run within a virtualized environment hosted on Vivio's Cloud Compute service. Exception includes some applications that require a device driver (a form of integration with the OS) and 16-bit applications that need to run in shared memory space.

The Client remains responsible for confirming that their application is suitable for migrating to a virtualised environment.

## Moves, Adds and Changes

Following implementation, the following changes can be made subject to survey and additional charges:

## Change Server Type

The server can be replaced by an alternative specification model based on any suitable available combination of RAM and CPU. This activity is a scheduled event, booked within a 48hr window and subject to a 15 min downtime. The end user Client user login credentials remain unchanged. Unless specifically modified at the same time, all data volumes associated with the current server will be transferred to the 'new' server.

## Delete Server

Clients can delete servers (as opposed to changing models) following any minimum contract commitments.
Please note that any storage device attached to this server will be deleted unless requested to be re-attached to another available server prior to deletion. The Client should also be made aware that once deleted, the data will be lost and therefore offered the opportunity to save their data elsewhere prior to deletion. If the optional Backup as a Service (BaaS) feature is enabled on the server, this too will need to be removed before the server can be deleted.

## Increase existing Storage Size (increase drives)

The Client can request an increase on storage capacity (in 100GB increments up to a maximum of 16TB) associated with the server. This is a scheduled event within a 48hr window and requires a 30-minute downtime.

## Add Additional Storage Volumes (new drives)

The Client has the option to add additional storage volumes (drives) to the server. There is no downtime associated with this function.

## Add a Public IP

If the server exists within a Public IP subnet, the Client can request a Public IP to be attached to the server. If the server is not in a public subnet, contact Vivio for advice.

## Add/Remove Backup

The reseller can order the optional BaaS service to associate with the server and all of its associated storage volumes. The BaaS can also be removed, following confirmation that the user is aware of and has had opportunity of downloading any existing backup data.

The removal of any chargeable elements such as a servers are subject to minimum term charges as detailed in the Proposal and Order Form.

## Storage

All servers will have at least 1 storage device associated against it – these are high performance Solid State Drive storage devices and are available in 100GB increments up to a maximum of 16TB. The Client can create multiple volumes within a single storage device, noting that at least 50GB will be allocated to the operating system.

Each SSD device can support an aggregate transfer rate of up to 800MB/s and an IOPS of 48,000 and up to 160 MB/s and 10,000 IOPS per volume.

The Client will be responsible for creating and managing their own file systems across the deployed volumes. These are block storage devices with each storage device linked to a single server.

Each storage device is automatically replicated in order to protect it from component failure.

## Networking

The creation of each Client's server environment will include a Virtual Private Cloud (VPC) which is a logically isolated section of the cloud and provides the facility to deploy specific IP ranges, the creation of subnets, and configuration of routing tables and network gateways.

For example, Clients can have a public-facing subnet for their webservers with access to the Internet, and place their backend systems such as databases or application servers in a private-facing subnet with no direct connection to the internet for inbound access, outbound is still possible for general internet access.

Servers in a private subnet can access the Internet without exposing their private IP address by routing their traffic through a Network Address Translation (NAT) gateway in a public subnet.

In addition, Clients can choose to include a Virtual Private Network (VPN) connection between their own facilities and the VPC.

Each Client can be allocated up to 5 Public IP addresses; any additional requirements must be applied for separately.

The creation and configuration of the VPC is undertaken by Gamma on behalf of Vivio based on specific Client configuration requirements as captured by Vivio.

Note: The service uses IPv4 only.

The following elements constitute the VPC:

## Firewall

The service provides a Managed Firewall with a configuration based on a rule set provided by the Client. The outcome is an individual Firewall policy that is based on Port, Protocol and Source IP address rules.

The Firewall rules are based on security groups which are applied to individual servers and can therefore be tailored to the requirements of each server and their associated applications. Each server will be assigned to a single security group.

### Key Considerations:

- All servers on the same subnet will have unrestricted access to each other, an important consideration when deciding which subnet to place servers in. For example, good practice would exclude a publicly accessible web server from sharing the same subnet with a private application, database or development server.
- By default, no inbound traffic is allowed until you add inbound rules to the security group.
- The Firewall is not a web filtering Intrusion Detection (IDS) or Prevention (IPS) System. Customers that require this additional functionality must make their own provision for such functionality.
- Security groups are stateful — responses to allowed inbound traffic are allowed to flow

outbound regardless of outbound rules, and vice versa

You can allow specific ports/protocols for an IP or CIDR (Classless Inter-Domain Routing).

## Subnets

The creation of the Clients VPC allows for the introduction of subnets in order to isolate specific servers in a logical manner. The Client can specify the range of IP addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16

Please note:

The first four IP addresses and the last IP address in each subnet CIDR block available for you to use, and cannot be assigned to a server. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2: Reserved by AWS for mapping to the Amazon-provided DNS.
- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. Broadcast is not supported in a VPC, therefore address is reserved.

## Load Balancer

Load Balancing is an optional costed feature that automatically distributes incoming application traffic across multiple servers as defined by the user requirements. It enables greater levels of fault tolerance in applications, seamlessly providing the required amount of load balancing capacity needed to distribute application traffic.

When you define a load balancer in your configuration it will be in an internet-facing only configuration.

Load Balancing supports the ability to stick user sessions to specific servers using cookies. Traffic will be routed to the same instances as the user continues to access your application, it also scales its request handling capacity in response to incoming applications.

Applications using HTTP, HTTPS (Secure HTTP), SSL (Secure TCP) and TCP protocols are supported by the Load Balancer.

## Virtual Private Network (VPN)

The service provides a chargeable option to order an IPsec, VPN connection between your VPC and the Clients network.

The Client is responsible for configuring their gateway, which is the physical device or software application on the remote side of the VPN connection. They are also responsible for implementing redundancy and failover (if required).

The following customer gateway devices are known to work with VPN connections:

## Statically-routed VPN connections

- Cisco ASA 5500 Series version 8.2 (or later) software
- Cisco ISR running Cisco IOS 12.4 (or later) software
- Dell SonicWALL Next Generation Firewalls (TZ, NSA, SuperMassive Series) running SonicOS5.8 (or later)
- Juniper J-Series Service Router running JunOS 9.5 (or later) software
- Juniper SRX-Series Services Gateway running JunOS 9.5 (or later) software
- Juniper SSG running ScreenOS 6.1, or 6.2 (or later) software
- Juniper ISG running ScreenOS 6.1, or 6.2 (or later) software
- Microsoft Windows Server 2008 R2 (or later) software
- Yamaha RTX1200 router

If a VPN is required by the Client, a simple VPN form will be provided which will need to be completed with the following information:

- Tunnel Endpoint Device (Gateway)
- Tunnel Endpoint IP Address
- Networks to be tunneled

## Moves Adds and Changes

Vivio will on behalf of the Client, request configuration changes to be made to any of the networking elements of the design such including, Firewall rules, Subnets, Load Balancer and VPNs.

Such configuration changes are included within the managed service charge associated with the service.

The removal of any chargeable elements such as a VPN are subject to any minimum term charges as detailed in Proposal and Order Form.

## Security

## Server Passwords

Usernames and Passwords created for new servers will be emailed to the Client following successful creation on AWS or Azure. This is a once only communication and these details are not stored on any Vivio systems. Clients are strongly advised to change these passwords during the first login.

Note: Vivio are not able to retrieve or regenerate these details and it is therefore the Client's responsibility to safeguard these details.

## Service Account Root Credentials

The creation of service for each Client will automatically generate a unique username and password known as the root credentials. These details are securely stored with LastPass Enterprise Vault using AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes to ensure complete security in the cloud. They are not stored on Vivio systems or used for any subsequent interaction with the customer's service.

## Data Location

All Client servers, associated data and backup data (where applicable) are maintained within a single geographic region in the UK referred to as the EU (London) region. Resources and data will not be created or moved outside of this geographic region.

Please note: Within this region, there are multiple, isolated locations known as 'availability zones'. Servers are not replicated across regions unless specifically requested to do so.

Data storage devices are located within a single availability zone, whereas the backup service is located across multiple availability zones (again within the same EU (Ireland) region).

### Data Security

The AWS and Azure services deployed by Vivio are supported by the robust controls in place to maintain security and data protection in the cloud. All the relevant compliance features that are available from Amazon and Microsoft websites.

## Backup as a Service (BaaS)

The 'Backup Service' is an optional costed feature that can be ordered during the initial provisioning process or at a later date to an existing service.

It provides Clients with a simple to use application that can back-up their Cloud SSD storage devices to another logically and physically separate storage facility within the same region.

Specific configuration and user details can be found within the BaaS User Guide; noting that a backup software agent is required on the server.

### Highlights:

- Server agents support both Windows and Linux environments
- Source-based encryption and source-based global de-duplication
  Application-consistent backups of Windows Server tools
- Support for Active Directory, DFS, Exchange, SharePoint, SQL
- VSS (Volume Shadow Copy Service) integration enables application consistent backup and recovery with file-level granularity
- WAN-optimised protocols enable efficient and secure in-cloud and cross-cloud communication
- Incremental backup, globally de-duplicated and compressed
- Automatic resumption of interrupted backups

## Retention Period

Unless explicitly agreed otherwise, the following standard retention policy is applied:

- Quarterly Backup – 1-year retention
- 7 days of backups (daily)
- 5 weeks of backups (weekly)
- 3 months (monthly)
- 3 quarterly backups (quarterly)

### Security

The following security features are associated with this service and can be implemented by the Client:

- Source-based AES-256 encryption - Data is encrypted before it is sent to the cloud and remains encrypted as it is stored.
- SHA-1 Data Fingerprinting - Ensures data integrity as it travels between locations, prevents man-in-the-middle attacks and transfer errors.
- Private Encryption Key Management - Manage your own encryption keys or use personal passphrases per user to prevent privileged admins from accessing data.
- In-Transit TLS Encryption - In addition to data encryption, all WAN transfers use Transport Level Security (TLS) protocol over the WAN, preventing unauthorized interception of data transfers.
- Granular Event Logging - Monitor and log security events such as user access and failed logins, and integrate with SIEM systems via Syslog for 3rd party audit trail retention and reporting.
- Restricted Content Policies - Define rules based on file size, name, or type that deny or allow files to be shared externally or uploaded to your network.

## Support

Where an existing support contract is in place with the Client or is entered into at the same time as the order for Cloud Compute services, Vivio will work with the Client on their behalf to fulfill the responsibilities outlined above to complete the successful implementation of the new services.

Under this same support contract Vivio will provide the agreed level of support to the Client for the duration of the Cloud Compute agreement including any additional services stipulated under that support agreement.

## Service Level Agreement (SLA)

Vivio and Gamma provide a service level agreement as part of the Cloud Compute service; this SLA includes measurements for:

- Service Availability
- Fault Rectification
- Service Provisioning

## Service Availability

Service Availability is defined as the ability of a Service to perform its required function over a stated period of time. It is reported as the percentage of time that a Service is actually available for use by the Client within agreed Service Hours.

Availability is calculated as:

$$\frac{\text{Total number of minutes in the measurement period} - \text{Unplanned Downtime} \times 100}{\text{Total number of minutes in the measurement period}}$$

Note: If a Service is partially available then the Unplanned Downtime shall be calculated in equal proportion i.e. if a service is 50% available then the unplanned downtime will be calculated as 50% x elapsed period of the incident.

Availability Measurement Period: 1 Calendar month.

| Service Detail | Target Availability |
|---|---|
| Servers | 99.95% |
| Storage Drives (volumes) | 99.95% |
| Cloud Network (Firewall, Load Balancers, VPN) | 99.95% |
| Backup Service | 99.95% |

Service Credits:

Service credits will be applicable should the level of core service availability not meet the target monthly percentage, as per the table above. Service Credits applied to Monthly Service rental charges only. Service credits would need to be requested by the Client to Vivio, with evidence of services that you feel have been impacted. Any agreed service credits would be satisfied by the issue of a credit note to be deducted from the next scheduled payment to be made to Vivio.

| Service Detail | Target Availability | Service Credit |
|---|---|---|
| 99.95% | 99.90%-99.94% | 10% |
| 99.95% | 99.5% - 99.89% | 15% |
| 99.95% | <99.5% | 25% |

Unavailability means:

**For Cloud Servers** - When all of your running servers have no external connectivity.

**For Cloud Storage Drives** - When all of your attached volumes perform zero read write IO, with pending IO in the queue.

Please note the Service Availability and other measures with the SLA relate to the core Cloud Compute Service and does not include access or local CPE elements.

## Fault Rectification

Subject to the fault processes detailed in the product Service Description, the following definitions will be applied to faults raised on the Cloud Compute Service:

| Severity | Description | Time to Resolve |
|---|---|---|
| Priority 1 | Critical Fault - Loss of service - Multiple resellers/services affected | 5 Clock Hours |
| Priority 2 | High - Loss of service - single reseller or service | 7 Clock Hours |
| Priority 3 | Medium - Disrupted service - multiple or single reseller or service | 2 Working Days |
| Priority 4 | Non-critical operational impact that does not restrict user from performing key tasks. | 7 Working Days |

The Service Desk is available Monday – Friday 08:30 – 17:00 (Closed UK bank holidays). Out of Hours support is excluded from this SLA as best endeavours will apply.

Note: Service credits are not applicable against Fault Rectification performance metrics.

## Service Provisioning

The following performance indicators are applicable to in-life Cloud Compute Service Provision:

| Severity | Description | Time to Resolve |
|---|---|---|
| Standard Service Request | 3 Working Days | NA |
| Standard Change Request | 3 Working Day | NA |
| Non-Standard Change Request | 7 Working Days | NA |
| Emergency Change Request | 6 Clock Hours | NA |

### Standard Service Request:

A service request that does not require modification of any existing service.

### Standard Change Request:

A service request requires the modification or addition to an existing service. An example would be to increase a Client's storage capacity.

### Non-Standard Change Request:

A service request which requires further technical or commercial consideration and may be declined accordingly. An example would be the addition of an Amazon Web Service or Microsoft Azure feature not currently supported by Vivio.

### Emergency Change Request:

A request where significant impact is anticipated or immediate action to restore service is required. An example would be where a storage volume has reach capacity due to an error within the end user's application. The storage volume may need to be increased urgently to prevent the server from hanging.

Please note: Service credits are not applicable against Service Provisioning performance metrics.

## Billing and Invoicing

## Setup Charges

The service may include a one-off connection charge for the following elements where provisioned:

- Audit (per server - min 5 servers)
- Setup Per Server
- Network
- VPN
- BaaS Per Server
- Load Balancer
- Migration Infrastructure

## Re-occurring Fixed Fee

The fixed fee consists of the monthly subscription charge where the following elements are provisioned:

- Server
- SSD Storage
- Monitor & Support (per server)
- Managed Firewall
- Load Balancer Management
- Data Out (200GB/Month) Fair Use Policy
- VPN
- Load Balancer
- BaaS (per 100GB increments)

## Invoicing

The costs for the fixed fees plus the one-off setup charges shall be billed monthly, pro-rata if service started during the month.

There will be a minimum term for the services, details of which can be found on the Proposal and Order Form.