IBM G-Cloud
Apache Web Server as a Service

Service Definition
1. Summary

1.1 Service Description
This offering is provided by IBM Global Business Services and provides an Open Source Apache Web server capability.

The Apache HTTP Server is an open-source HTTP server for modern operating systems including UNIX, Microsoft Windows, Mac OS/X and Netware. Apache is intended to provide a secure, efficient and extensible server that provides HTTP services observing the current HTTP standards. Apache has been the most popular web server on the Internet since April of 1996. The following link provides more detail about Apache.


The service provides as standard a single non-clustered Apache web server. This can be subsequently configured using the standard features provided within Apache.

The service provides:

• Proactive monitoring of the service from 8am-6pm Mon-Fri and 9am-5pm Sat/Sun
• Initial response to system alerts – e.g. restart of failed process or node using procedures provided by the client
• Escalation of any issues which are not resolved to the individual or organisation nominated by the client

This offering is designed to provide a Web Server which comes deployed on an IL0, IL2 or IL3 accredited cloud. An established and mature team will build and monitor your Web Server and will provide an initial response to an alert, along with a mechanism to get the client team involved should the issue be more complex.

1.2 Service Characteristics

<table>
<thead>
<tr>
<th>Lot</th>
<th>Cloud Infrastructure and Hosting (Platform as a service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicability</td>
<td>Any organisation which requires a Web Server platform at IL0, IL2 or IL3</td>
</tr>
<tr>
<td>Contract Duration</td>
<td>Flexible – to be agreed in the Call-Off Order</td>
</tr>
<tr>
<td>Contract Price</td>
<td>As per G-Cloud order.</td>
</tr>
<tr>
<td>Lead time to start</td>
<td>2 weeks</td>
</tr>
<tr>
<td>Related Lot(s) /Offering(s)</td>
<td></td>
</tr>
</tbody>
</table>
1.3 Why IBM

- Proven track record of delivery to multiple Government departments
- Leading Cloud services
- Leading server and software technology to deliver Cloud services

1.4 Contact

<table>
<thead>
<tr>
<th>Contact Name</th>
<th>Steve Cliff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>IBM UK Cloud Alliances Executive</td>
</tr>
<tr>
<td>Address</td>
<td>PO Box 41</td>
</tr>
<tr>
<td></td>
<td>North Harbour</td>
</tr>
<tr>
<td></td>
<td>Portsmouth</td>
</tr>
<tr>
<td></td>
<td>Hants, PO6 3AU</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Email</th>
<th><a href="mailto:gcloud@uk.ibm.com">gcloud@uk.ibm.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Phone</td>
<td>07710 035877</td>
</tr>
</tbody>
</table>

2. The Detail

2.1 Context
Most modern systems are built around a Web Server capability. This offering provides a managed Web Server for integration into a larger system. The offering can operate at IL0, IL2 or IL3 and is hosted within a secure pan-government accredited cloud.

2.2 The Cloud Infrastructure
This offering includes the following:

- Apache Web Server capability built on a fully accredited, Network, Compute and Storage Platform
- Private Government “Community Cloud”
- Pay as you go compute model
- Flexible environments
- Number of pre sized machine offerings available
- Additional customised sizing options available upon request
- Option to provide Burst and Elastic capabilities for CPU, Memory and Storage
- Fully GPG 13 Compliant (DETER) Virtual Machine
- Ability to connect via the Internet the GCF and the PSN Government Networks.
- Guest level back up each evening, with a standard 10 day retention period (limited to the boot partition) included.
- Disaster Recovery and Dual Site option providing two levels of compute availability
- Built upon industry standard components and services

The offering is hosted within SCC’s Secure Multi-Tenant Cloud (SMTC) platform which provides a secure, robust, Infrastructure as a Service offering across multiple Business Impact Levels.

There are 5 standard size variations available. These are as follows:

<table>
<thead>
<tr>
<th></th>
<th>Memory (GB)</th>
<th>vCPU</th>
<th>Storage – Boot Partition Size (GB)</th>
<th>Storage – Page File (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mini</td>
<td>2</td>
<td>1</td>
<td>90</td>
<td>10</td>
</tr>
<tr>
<td>Small</td>
<td>4</td>
<td>2</td>
<td>90</td>
<td>10</td>
</tr>
<tr>
<td>Medium</td>
<td>8</td>
<td>2</td>
<td>90</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Memory (GB)</td>
<td>vCPU</td>
<td>Storage – Boot Partition Size (GB)</td>
<td>Storage – Page File (GB)</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>------</td>
<td>-----------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Large</td>
<td>16</td>
<td>4</td>
<td>90</td>
<td>16</td>
</tr>
<tr>
<td>Very Large</td>
<td>32</td>
<td>8</td>
<td>90</td>
<td>32</td>
</tr>
</tbody>
</table>

Additional infrastructure capacity can be added to each of the standard sizes available. This can be either via allocating dedicated resource to the virtual machine or to provide the virtual machine with the ability to burst its resources only when required, utilising the shared resources of the cloud platform and ensuring a true utility based compute model.

Options available for expanding the offerings are as follows:

### Service Component
- 1GB Memory Increment – Elastic
- 100MHz Core Increment – Burst
- 100MHz Core Increment – Elastic
- 100GB Tier 1 Storage
- 100GB Tier 2 Storage
- 100GB Tier 3 Storage
- 1GB Backup to Disk
- 1GB Backup to Disk and Tape
- Internet per MB
- GSI/GCF per MB

### Storage
Storage at IL0, IL2 and IL3 Secure is provided as follows:
- On a per 100GB per month basis.
- Comprising 3 tiered options:
  - Tier 1 performance is 20,000 IOPS
  - Tier 2 performance is 10,000 IOPS
  - Tier 3 performance is 5,000 IOPS.
- Providing both Burst and Elastic capabilities.
- Including a guaranteed set of resources that can be defined at purchase.
- With backup from our Secure Backup Service available as an additional Service.
- Service will be delivered at Impact Level IL0, IL2 or IL3 as appropriate

This Service shall deliver a Secure Storage platform. The Supplier shall provide tiered disk appropriate to Customer data needs, within a fully monitored and managed SAN environment.

Customer data shall be loaded on to the secure storage Service by the Supplier’s accredited and security cleared staff who shall be responsible for all on-boarding activities associated with the delivery of this Service.
The secure storage Service shall be fully managed by the Supplier’s security cleared staff, including:

- To ascertain availability of the Storage Service Infrastructure.
- To measure the percentage of Storage Service capacity being used (this information will also be available via the Supplier’s customer portal)

Requests for additional storage requirements shall be made, either via the Supplier’s customer portal or via the Service change request process.

**Backup**

The Virtual Machines will be backed up to disk each day and backups will be retained for 10 days as part of the core service offering.

This backup shall be limited to the standard boot partition of the virtual machine and will not include additional Persistent (Data) storage connected to the service.

Backup of additional “Application” data is provided under our Secure Backup Service options.

Backup will be to disk only. Backup of the OS to tape is offered as an additional, separate option.

Recovery of a VM Image from backup shall be actioned within 4 Hours from the point of request by The Customer through the Service Desk. The time taken to recover a Virtual Machine will be dependent upon the size and the complexity of the restore process for the specific machine.

**Availability**

The cloud platform is housed within its Tier 3+ Datacentre and provides resiliency at all levels of the infrastructure, providing a stable, reliable infrastructure platform. In order to provide additional levels of availability and redundancy, there is an option for a dual site implementation, utilising a secondary Data Centre as a cold standby facility for the customer’s infrastructure. The following Table provides the options available for Single site and Dual Site Infrastructure options and the corresponding Availability Service Level Agreement:

<table>
<thead>
<tr>
<th>Infrastructure Option</th>
<th>Availability SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Site</td>
<td>99.9%</td>
</tr>
<tr>
<td>Dual Site</td>
<td>99.95%</td>
</tr>
</tbody>
</table>

**2.3 Information Assurance**

The SMTC platform is accredited to hold and process information at Business Impact Level 0, 2 and 3 (IL0, IL2 and IL3)
IL0 IaaS Service
This service shall be delivered at Business Impact Level 0, IL0.
The IL0 IaaS platforms will not be connected to any of the Government Networks.
We shall have the right to disable or remove services that can be proven to cause a
security risk to the community as a whole.
This service is intended to provide a web tier capability with the option to connect to
the IL2 Business Impact Level via a pre-approved IL0 to IL2 Gateway Service.

IL2 IaaS Service
This service shall be delivered at Business Impact Level 2, IL2.
At IL2 the service shall be delivered from a pre-accredited infrastructure and shall be
connected to an appropriate Government network or the Internet via the IL0 Gateway Service.
It shall be the responsibility of the guest VM owner, IBM, SCC and the accreditor to
ensure that code of connection compliance is adhered to and that the service meets and
maintains the minimum requirements for an IL2 infrastructure service.
We shall have the right to disable or remove services that can be proven to cause a
security risk to the community as a whole.

IL3 IaaS Service
This service shall be delivered at Business Impact Level 3, IL3.
At IL3 the service shall be delivered from a pre-accredited infrastructure and shall be
connected to an appropriate Government network.
In order to maintain IL3 compliance for the Standard and Enhanced Virtual Machines,
We shall ensure hardening and patch compliance is maintained in line with the code of
connection and CESG Good Practice Guides.
It shall be the responsibility of the guest VM owner, IBM, SCC and the accreditor to
ensure that code of connection compliance is adhered to and that the service meets and
maintains the minimum requirements for an IL3 infrastructure service.
We shall have the right to disable or remove services that can be proven to cause a
security risk to the community as a whole.

SCC are able to provide a data transfer capability between the IL2 and IL3 impact levels
via the eSecure cloud based middleware (Integration Platform-as-a Service - iPaaS)
solution that delivers an industry leading solution for connecting highly-secured back
office systems to the Internet and cloud-based applications, enabling the secure transfer
of data between systems.
For further details on this service please see the SMTC Secure Managed Impact Level
Gateway Service Offering
2.4 Disaster Recovery
Where a customer has selected the 99.95%, higher availability service, the VM Image shall be replicated in real time to a secondary data centre. Compute resource shall also be allocated at the secondary site, providing a cold standby “Disaster Recovery” solution. In the eventuality that the primary site fails, and a Disaster is declared, the service shall be restored at the secondary datacenter.

2.5 Customer Responsibilities
The following are customer responsibilities:
• Sizing the server – the server will be provided to the specifications which the Customer specifies. We can work with you to help you to size the capability as part of the planning activities. Please note that the service may not be performant or function correctly without the allocation of sufficient resources.
• Integration of the server into a wider system or capability.
• Procurement, maintenance and management of any Customer data.
• Provision, maintenance and management as the case may be of any Customer content and configuration to be provisioned on the Server.
• Administration, management and control of Users access to the Customer’s applications and/or data stored on the Server.
• Should the Supplier determine that the Customer usage of the Infrastructure is not compliant with best practice guidelines then the Customer must comply with the Supplier’s reasonable requests for change.
• Procurement, maintenance and management of any Customer data communications lines not identified.
• Provision of ‘first response’ procedures
• Provision of contact list for ‘second response’
• The Server is provided on a pan-government accredited cloud. The Accreditation of the specific instance of the Server in the context of the Customers system will be done by the Customer.

In addition, to assist in the Incident and Problem Management process, the customer will be required to

1. report and provide the Service Desk with all information it may reasonably require in order to resolve the Incident
2. ensure an Incident Owner or a nominated deputy is available during Working Hours
3. provide the necessary resources to ensure that any changes to the Agreement are addressed and agreed with us via the Change Control Procedure in a timely manner
4. provide details of forthcoming change that may impact the SMTC service
5. liaise with our incident and problem management teams where required to aid incident and problem resolution activities

6. provide any required integration and communication functions between various 3rd parties eg application vendors, business users

7. ensure all users understand and comply with the various processes, policies and procedures of The Customer and as may be agreed between the parties from time to time

2.6 Service Changes
The primary mechanism for service management shall be through the Lifecycle Portal where Customers can request changes for the service. In addition, service status and billing reports can be made available in a pre-agreed format via a Customer Service Manager, should this be required.

2.7 Connections
All data centre operations conform to ISO2001/2, ITIL and the Code of Conduct for Data Centre Operations. Additionally SCC maintains Code of Connection agreements with Government network services providers such as GCF, PSN & IGSOC

2.8 Service Constraints
The service shall be allocated a maintenance window between the hours of 23:00 and 06:00 and the window shall be allocated during service initiation.

The service shall be Change Managed in accordance with SCC change schedules, change boards will sit weekly and changes shall be carried out during the subsequent change window.

Configuration changes that cause a reboot/downtime but are deemed urgent shall not impact Availability metrics and SLAs and the associated charging mechanism.

The ability to add move or change the number of VMs in the Customer solution shall be achieved via the Service Change request process and may be subject to appropriate financial approvals.

VMs shall be decommissioned via change control and images will be shut down. The images will be left in place for a further 24 hours after which point they will be deleted.

As part of any decommissioning process all virtual backups will be destroyed and any physical backups will be returned to the Customer or destroyed.

Decommissioned machines shall be quarantined and can be restored to full operational state within 24 hours of being decommissioned.

2.9 Exclusions
Services to manage your servers are limited to ‘first response’ with the ‘second
response’ being to contact an appropriate resolver. IBM can provide more extensive management if required, and this can be specified and provided at any stage during the provision of the service.

We will provide service and support for all aspects of the service as defined within scope of the service. The Service Levels Agreements (SLA’s) will measure our success in the delivery of those services.

Where external factors influence our ability to deliver against the contractual defined Service then we will not be liable for failure to meet the associated SLA’s. These include but are not limited to the following circumstances:

1. 3rd Parties, not engaged by IBM or SCC, fail to deliver services in accordance with their contractual commitments
2. 3rd Parties use the SMTC environment outside recommended best practice
3. Where the workload or the levels of utilisation of the Virtual Machines cause the system to become unresponsive or suffer from poor performance and where those levels of utilisation are deemed outside of the forecasted demand or sizing criteria of the service
4. Where customer requested configuration changes cause application downtime
5. Application Configuration causes Operating System instability
6. Application Level and End User Testing of all patches and security updates

2.10 Incident Management

We shall determine the severity of an Incident in accordance with the following severity criteria on underlying platform:

1 - (Critical)  The Service failure creates a serious business and financial exposure, causing a significant percentage of Users to be unable to work or perform an essential portion of their job, and there is no acceptable workaround to the problem.

2 - (High)    The Service failure creates a significant business and financial exposure, causing a high (fixed) number of Users to be unable to work or perform some significant portion of their job, but there is an acceptable workaround to the problem in the short term.

3 – (Medium) The Service failure creates a low business and financial exposure to an isolated number of Users causing them to be unable to perform a portion of their job, but they are still able to complete most other tasks, or; General Service related questions and requests for information.

4 - (Low)    The Service failure creates a minimal business and financial exposure causing one or two User to be unable to perform a minor portion of
their job, but they are still able to complete most other tasks.

The following table provides a maximum time before a response to an incident is provided by Incident management:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Response Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – (Critical)</td>
<td>30 Mins</td>
</tr>
<tr>
<td>2 – (High)</td>
<td>60 Mins</td>
</tr>
<tr>
<td>3 – (Medium)</td>
<td>4 Hours</td>
</tr>
<tr>
<td>2 – (Low)</td>
<td>73 Hours</td>
</tr>
</tbody>
</table>

### 2.11 Service Credits

1.1 Subject to Clause 1.3 below, in the event that we fails to meet the SLA Target for the applicable Service Level, then the Service Credit mechanism in Clause 1.2 shall apply;

1.2 We shall provide a rebate of 1% of the Monthly Charge for this Service, which is applicable over the Report Period for every 1% below the SLA Target to a maximum of 10% rebate. The applicable Service Credit shall be deducted off the next invoice due to The Customer.

1.3 Payment by us of Service Credits to The Customer shall be in full and final settlement of our liability to The Customer for failure to meet the Service Levels during the Report Period.

1.4 Service Levels will only be calculated against individual Virtual Machine instances and not against Application availability. Service penalties against the loss of a single virtual machine will not include other machines impacted by that loss.

1.5 Service Credits will not be applied where it is determined that we are not responsible for the cause of the breach in Availability performance.

### 2.12 Training

There is no training provided as part of the core SMTC IaaS service offering.

### 2.13 Trial Period

There is no option to consume this service for a trial period.

### 2.14 Off-boarding

The virtual machine shall be assessed to determine if there is any data encapsulated within the virtual machine file and, if so, determine the IL applicable to the data. This will ensure that appropriate measures (security, encryption etc.) are applied when transferring the virtual machine file back to the Customer.

The virtual machine file, together with the associated virtual machine configuration file shall be supplied to the Customer using either removable disk or optical media.
encrypted as appropriate and provided by the customer.

The Customer shall be responsible for validating the integrity of the returned virtual machine file – note that this step refers to the confirmation that a valid VM file has been supplied. We will not be responsible for ensuring that the virtual machine encapsulated within the file is correctly configured for any environment outside of our service provision.

Where a software license for the operating system or layered software within the VM file has been rented from us under a License Agreement the license key shall be removed prior to the return of the VM file.

We will then destroy all live and backup copies of the virtual machine file within our control in line with CESG guidelines and provide written confirmation to the Customer that this has been performed.

Any On Boarding or Off Boarding process is not part of the Monthly unit rate and will be undertaken as part of a project activity.

### 2.15 Data Extraction

<table>
<thead>
<tr>
<th>The data standards that will be in use (within the service).</th>
<th>This service shall deliver a single data standard and that is a VMDK Virtual Machine File.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A commitment to returning all consumer generated data (e.g. content, metadata, structure, configuration etc.) and a list of the data that will be available for extraction. Where there is a risk of confusion, data that will not be available for later extraction will also be published.</td>
<td>The return of customer VMDK files shall be performed with MD5 checksum in transit and shall rest on FIPS-140-2 compliant storage subsystem.</td>
</tr>
<tr>
<td>The formats/standards into which data will be able to be extracted and preferably a list other common services/technologies to which an export/import mechanism is available.</td>
<td>This service shall deliver a single data standard and that is a VMDK Virtual Machine File.</td>
</tr>
<tr>
<td></td>
<td>Import and Export of VMDK files shall be via an appropriate network to appropriate storage sub-system or via DVD media.</td>
</tr>
<tr>
<td>A price for the extraction of consumer generated data (or the migration to another service provider’s service).</td>
<td>Data Extraction shall be charged dependent upon the amount of data and media to be extracted to.</td>
</tr>
<tr>
<td>Confirmation that the Supplier will purge and destroy (as defined in security accreditation for different ILs) consumer data from any computers, storage devices and storage media that are to be retained by the Supplier after the end of the subscription period and the subsequent extraction of consumer data (if requested by the consumer).</td>
<td>All data at rest contained within the platform shall be purged or destroyed with standard service, volume, LUN deprecation procedures.</td>
</tr>
<tr>
<td></td>
<td>All data leaving the platform shall be purged or destroyed using CESG approved white spacing prior to shipping.</td>
</tr>
<tr>
<td></td>
<td>Where a physical drive from a drive set fails then that drive shall be destroyed in</td>
</tr>
</tbody>
</table>
2.16 Information Principles for UK Public Sector

Our services for the UK Public Sector support the defined Information Principles published where appropriate to the service being delivered. At the core of all of the services are principles 1 and 2 in that all data is valued and is managed in line with the appropriate UK Public Sector Information Assurance guidelines that define the security controls for holding the data.

Information Principles 3 through to 7 are considered and followed during the on boarding of systems in to the Cloud infrastructure. These principles will be considered and followed in line with the appropriate UK Public Sector Information Assurance guidelines.

2.17 Commercials

The price of the offering is made up of five components:

1. an initial fixed price setup fee;
2. an initial labour element, which will be based on the agreed statement of work and priced according to the IBM SFIA rate card;
3. a run fee which will be invoiced monthly;
4. optional increments to the run fee; and
5. optional incremental labour element, which will be based on the agreed statement of work and priced according to the IBM SFIA rate card.

The prices for (1), (3) and (4) are given in the offering pricing document.

The pricing for (2), (5) and any other work required will be agreed subject to the scope of work which will be set out in the Call Off Order Form and agreed by both parties.

- If assistance is required to plan and size the server(s) then this can be provided and will be priced using the IBM SFIA rate card.
- Follow on services to enable you to plan or complete implementation of cloud services can be provided by IBM. Details should be agreed via the Call-Off Order and priced using the IBM SFIA rate card.
- A level of support and systems management is included in the price of this offering, as described above, however this may be supplemented by the addition of further services to increase this level should this be a requirement. Details should be agreed via the Call-Off Order and priced using the IBM SFIA rate card.
2.18 Key Points

Other key points to note are as follows:

- This offering is subject to availability of IBM resources.

- The pricing and terms on individual call-off orders should be handled as commercially sensitive by the Customer.

- Where work is of a sensitive and secure nature, security standards will be agreed between IBM and the Customer, and if necessary IBM will ask the Customer to issue a Security Aspects letter.

- Whilst we do not propose to handle or have access to any personal data, we will suggest and agree alternative approaches such as the use of anonymised data for testing purposes.

- The work is subject to IBM’s Terms of Business, which are attached separately to this catalogue item.