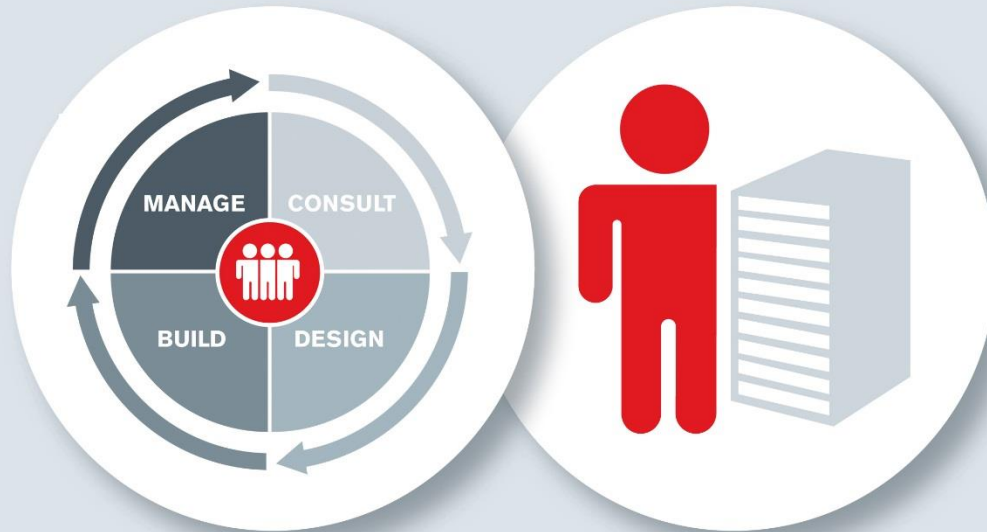


Claranet Service Description



Managed Hosting

Our proven service methodology starts with understanding your business needs, progresses through design and build of your solution, to the management and continual improvement of your in-life service.

Your tailored Managed Hosting solution combines multiple service elements specified in this Service Description. Each service element has a number of options to enable us and you to choose the right combination to suit your needs.

Version 11.1

Contents

Service overview	2
Compute services	4
Components	4
Storage options	6
Consult	7
High Level Options Analysis	7
Packaged Consulting	7
Consulting	8
Design	9
Managed Hosting sales specialist	9
Specialist solution design	9
Build	11
Specialist engineering	13
Project Management	13
Testing and acceptance	13
Manage	14
In-Life Management	14
Help and support	19
Service Levels	19
Managed Service Options	20
Appendices	21
Definitions	21
Claranet UK Data centres	22
Appendix: Compute services	23
Managed Server	23
Managed Self Service Hypervisor	25
Managed Hypervisor	28

Appendix: Components	28
Managed Load Balancer	28
Managed Backup	29
Managed SSL Certificates	31
Software Licences	31
Appendix: Roles	32
Managed Role Server	32
Managed Web Service	32
Managed URL Testing	35
Appendix: Storage	37
Managed Storage	37
Appendix: Support	38
Help and Support	38
Service Levels	40

The Service Description

This Service Description describes the service Claranet provides and details your responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties and all terms used within this document are in accordance with the terms to be found in the Master Services Agreement.

Service overview

Your tailored Managed Hosting solution can be designed from a combination of individual service elements. Each element has a number of options, to enable you to choose the right combination to suit your business and performance needs. The diagram below outlines the elements that are available.

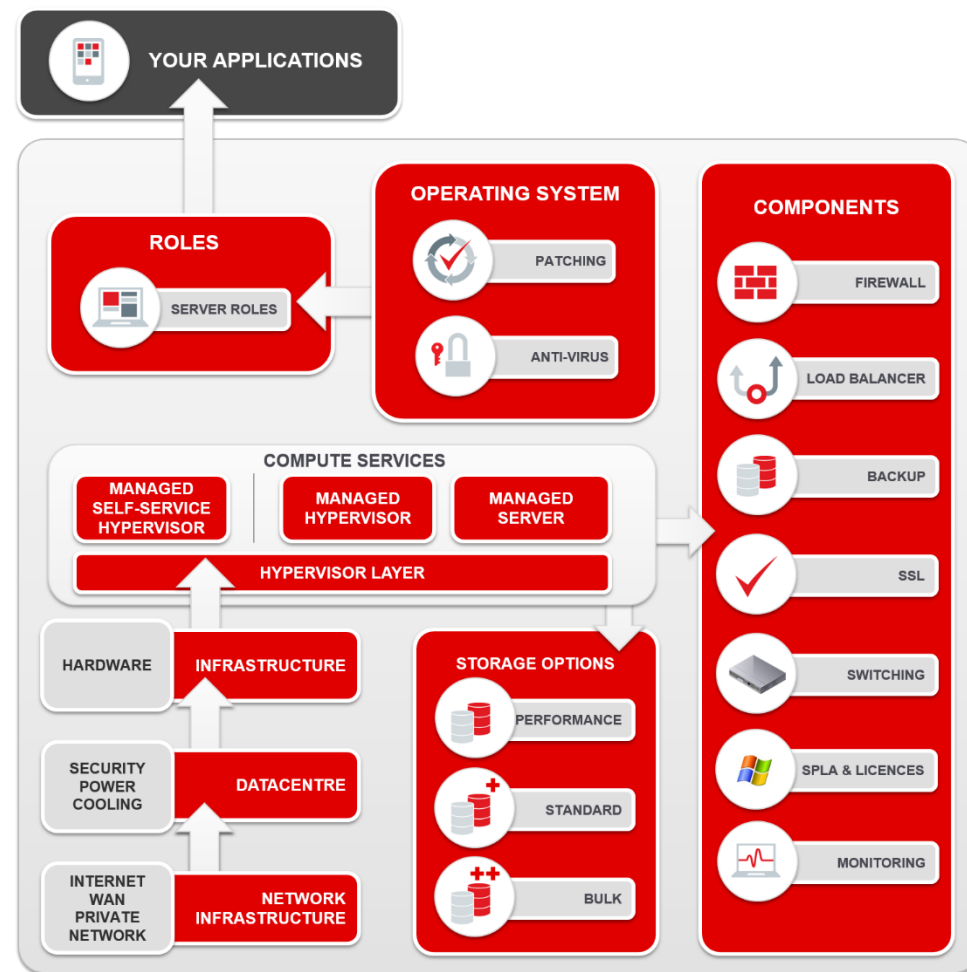
Data centres, Security and Network Infrastructure: Claranet provides you with a high level of security throughout our state of the art data centres. Specification details can be found in Appendix: Claranet UK Data centres. As network experts since 1996, we offer a comprehensive range of connectivity options to enable an end to end service. Please see the Claranet Connectivity Service Description for further details.

Compute Services: Claranet can provide a combination of a Managed Server, a Managed Hypervisor or a Self-Service Hypervisor. These three services all come with a number of Managed Components. The Hypervisor layer is VMware technology.

Components: Depending on which of the three Compute Services you select, these components are either mandatory (as in the case of the Managed Backup if you have selected the Managed Server option), or optional (e.g. if you select the Managed Self-Service Hypervisor, then you can choose to either select the Managed Load Balancer service or not).

Storage options: Simply choose from three options; Performance, Standard or Bulk

Diagram: Claranet’s Managed Hosting Service elements



Operating System: For the Managed Server or Managed Hypervisor, the OS remains under Claranet’s control and covers the patching and anti-virus capabilities.

Roles: Claranet can provide servers in a number of roles. e.g. as a Managed Database service, Dedicated Exchange or a Managed Web service. These options are not available with the Managed Self-Service Hypervisor. On this service you install your own virtual servers.

	Managed Server	Managed Hypervisor	Managed Self-Service Hypervisor
--	----------------	--------------------	---------------------------------

Server infrastructure

Dedicated hardware	Option	Yes	Yes
Virtual machines	Claranet	Claranet	You
vCenter access	No	No	Yes

Components

Managed Firewall	Yes	Yes	Yes
Load Balancer	Option	Option	Option
Managed Backup	Yes	Yes	Option
SSL certificates	Option	Option	Option
Switching	Yes	Yes	Yes
Hypervisor layer	VMware	VMware	VMware
Hypervisor management	Claranet	Claranet	Claranet
SPLA & Licencing	Yes	Option	Option

Storage

Performance	Available	Available	Available
Standard	Available	Available	Available
Bulk	Available	Available	Available

	Managed Server	Managed Hypervisor	Managed Self-Service Hypervisor
--	----------------	--------------------	---------------------------------

Operating System

Management	Claranet	Claranet	n/a
Patching	Claranet	Claranet	n/a
Anti-Virus	Claranet	Claranet	n/a

Server Roles

Managed Database	Available	Available	
Dedicated Exchange	Available	Available	
Managed Web	Available	Available	

Consult

HLOA	Yes	Yes	Yes
Packaged Consulting	Option	Option	Option
Consulting	Option	Option	Option

Design

Statement of Works	If required	If required	If required
Sales Specialist	Yes	Yes	Yes
Specialist Solution Design	Option	Option	Option

Build

Standard Engineer	Yes	Yes	Yes
Project Co-ordinator	Yes	Yes	Yes
Runbook	If required	If required	If required

	Managed Server	Managed Hypervisor	Managed Self-Service Hypervisor
Build (contd)			
Specialist Engineering	Option	Option	Option
Project Management	Option	Option	Option
Manage			
Platform maintenance	Claranet	Claranet	Claranet
Patches to hypervisor	Claranet	Claranet	Claranet
Change requests	Claranet	Claranet	You
Availability monitoring	Claranet	Claranet	Infrastructure only
Installation of application	You	You	You
Support			
24 x 7 support	Yes	Yes	Yes
Escalation option	Yes	Yes	Yes

To help your decision making you are supported by a team of highly experienced technical professionals, who use their considerable expertise and experience to design your hosted solution based on enterprise-grade technology. You also benefit by being able to consume and pay for the capacity you need as required on an OpEx basis, rather than having to make large upfront capital investments in hardware. In addition, Claranet's managed approach means you select a required "service level" rather than select your own vendor and infrastructure.

Compute services

Managed Server:

An instance of an Operating System running on either a hypervisor or directly on physical hardware. Claranet manage the infrastructure up to and including the Operating System configuration. You have full administration privileges and can connect to the Operating System to install software. Further details on the Managed Server service can be found in the **Appendix: Managed Server**.

Managed Self-Service Hypervisor:

Claranet will provide a virtualisation hypervisor on hardware dedicated to you. The vCenter instance allows you to provision and change virtual machines, and manage all Operating Systems, applications and databases. Further details on the Managed Self-Service Hypervisor service can be found in the **Appendix: Managed Self-Service Hypervisor**.

Managed Hypervisor:

The Managed Hypervisor component is similar to the 'Managed Self-Service Hypervisor' except that the vCenter instance is not provided and all provisioning is performed by Claranet. We then manage up to the Operating System. Further details on the Managed Hypervisor service can be found in the **Appendix: Managed Hypervisor**.

Components

Claranet provide the following components as part of the Managed Hosting service, either mandatory or as an option as specified.

Managed Firewall

Claranet provides a Managed Firewall service for both physical and virtual environments. We will provide you with a firewall and configure it to your specifications. Your service is monitored, measured on availability and supported 24x7.

Full details of the Managed Firewall service options for hosting, delivery timescales and monitoring can be found in the Managed Firewalls Service Description and Service Summary.

Managed Backup

Managed Backup provides a means to recover your data in the event of disk failure, accidental deletion of files or other loss of data. All data is backed up to a separate backup infrastructure in the same data centre as the server and replicated to a secondary UK based data centre for off-site protection. Where your solution includes a 'Managed Server' and 'Managed Hypervisor', it is mandatory to take the 'Managed Backup' service to enable Claranet to restore the server in the event of data corruption.

Claranet performs an initial full backup and then an incremental backup every night. In the event that a recovery is requested, data will be restored to the original environment in the original data centre. Claranet will not proactively restore your data from backups as part of this service, because typically you will first need to re-install and configure your applications. A restore will be limited to the restore of files and database and does not include any configuration of applications.

Claranet can offer Disaster Recovery services to match the plan for business continuity within your organisation. However, this service is not a disaster recovery solution, and does not include recovery of data and/or Service at the "off-site" data centre if the primary data centre is lost. These backups should not be used to provide 'rollback' snapshots or disaster recovery. The backup platform is not designed to address any specific legal or compliance regulations, for which you are solely responsible. It is not for backing up individual appliances e.g. PCs etc. which can be backed up using an alternative service, Claranet's Business Cloud Backup. Full details of the Managed Backup service including retention rules, backup windows etc. can be found in the **Appendix: Managed Backup**.

Managed Load Balancer

The Managed Load Balancer distributes inbound network traffic to two or more active servers that perform the same function, such as web servers. The load balancer cannot be exposed directly to the Internet, and must always sit behind a firewall supplied by Claranet.

One or more Virtual IPs (VIPs) are created for you, with each VIP representing a combination of an IP address and a port number. Traffic sent to a VIP is routed through Claranet's resilient shared load balancer platform, which contains physical load balancers located in the Claranet data centre. The appliances then distribute packets between two or more Customer servers. Your traffic is securely isolated from other Customers. Further details can be found in the **Appendix: Managed Load Balancer**.

Managed Switching

Physical hardware deployed for you, including some firewall configurations, may require additional physical network ports. These ports connect into switches at the top of a hosting data centre rack, or directly into core network switches. One or more managed network switches within a single rack may then be used to extend this into more ports for equipment. All of these variants can only be selected by a Claranet Solution Architect as part of a solution design.

Managed SSL Certificates

Claranet can procure SSL certificates on your behalf. These can be used both for public-facing web servers and to secure Operating Systems and applications.



What Claranet will do

Installation of SSL Certificates: Install the SSL certificates onto those servers within the Managed Server; Managed Role Server, Managed Database Service, Managed Web Service options and Load Balancers where applicable.

Renewal of SSL Certificates: Renew the SSL certificates for the duration of your contract unless you instruct otherwise in writing through the Claranet Change Control process.

What you will do

Requested information: Provide any requested information or Proof of Identity that is required.

Further details of the options available can be found in **Appendix: Managed SSL Certificates**.

Storage options

Managed Storage provides disk storage space on multi-tenanted, enterprise grade storage equipment, using a mix of Near Line SAS and SSD drives. You can select from different storage performance options which will allow you to tailor storage performance levels to meet the requirements of your applications.

There are three tiers of storage: Performance, Standard and Bulk.

Performance

Performance storage is an all-flash, high performance tier utilising solid state flash memory to provide a block-based storage environment option in lieu of traditional spindle-based storage.

Flash-based Performance storage provides a greater number of IOPS per GB of allocated storage, and supports optimally configured workloads in a manner that provides for significant performance, mitigating the performance bottlenecks associated with legacy storage.

Standard

This is the most common storage level employed for mission critical or production workloads. This storage utilises solid state drives and this block-based storage infrastructure works well for most applications and databases but lacks the performance

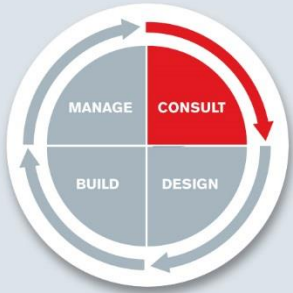
which is sometimes necessary for those databases and applications requiring a higher performance level. Mission critical data is that data which is required for the core day-to-day operation of the business, e.g. ecommerce and an internal line of business applications.

Bulk

Storage at this tier is compatible with best-effort, block-based data storage. This data is commonly used for record-keeping or compliance reporting requirements. Data at this tier is seldom accessed and is considered historic (or archival) in nature. Users and application workloads accessing data in this tier do not require significant performance, or require low response / data access times. It is not high performing storage and so applies only to those data files which can be accessed without concern for latency or IOPS requirements.

Bulk storage most commonly supports Windows/Linux file systems. As files are served from a multi-tenanted storage infrastructure without I/O performance requirements, the hardware element is comprised of lower performing SATA NL (Near Line) drives.

For full details relating to the specification of the three storage tiers, please refer to the **Appendix: Managed Storage**.



Consult

Claranet's consulting process ensures that you have the right information, the right recommendations, and the right service options available to you to achieve your business outcomes.

Understanding your business is paramount to ensuring that you have the right solution for your business outcomes. In the Consult stage, Claranet will discuss your business requirements with you prior to recommending a solution.

Depending on the complexity of requirements, one or more workshops between you and Claranet may be arranged in order to outline your requirements. These may be conducted by Solutions Consultants, Strategy Consultants, Solutions Architects and Enterprise Architects who will be applied at our discretion. It is in everyone's interests to ensure that the proposed solution will meet your requirements and one of our first roles is to focus on your business, your IT requirements and to produce a high level scoping report, the High Level Options Analysis. This will allow you to make an informed choice as to the recommended path.

High Level Options Analysis

What Claranet will do

Deliverable: The High Level Options Analysis report. A short, high-level scoping document.

Time to complete: The High Level Options Analysis is a consulting based service and is included up to a maximum of 2 days work at Claranet's discretion. In some instances, the work required to produce a High Level Options Analysis could extend beyond this e.g. where the requirements need extensive discussion or the options are particularly complex. If this is the case, Claranet will agree with you a charge for the additional work required to produce a High Level Options Analysis to establish the requirement.

What Claranet will do

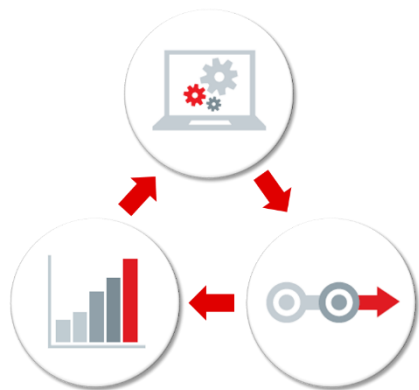
Technical Design: Technical work beyond this falls outside of the scope of the High Level Options Analysis and is carried out in the Design phase.

What you will do

Information sharing: Provide any requested information to allow Claranet to deliver a High Level Options Analysis. This will include full details of on-going technical contacts within your organisation. This information will form the basis of the Initial Configuration, so it is your responsibility to ensure the information provided is correct.

Packaged Consulting

Claranet has a number of pre-packaged assessments and audits that help to outline your readiness in respect of particular IT options. It may be that the completion of one or more of these packaged consultancy engagements is made as a result of the recommendations made in the High Level Options Analysis report. The completion of these assessments follow a general pattern:



Current State

Performing a real life assessment of your current environment and understanding where your business needs, and your current technical setup, may diverge.

Future State

A vision of the future for your company, taking into account strengths, weaknesses, opportunities and threats.

Transformation

The enablement program to be undertaken as a priority to advance your organisation to the desired level of maturity.

What Claranet will do

Assessment options:

- Linux Infrastructure Maturity Assessment (LIMA)
- Infrastructure Maturity Assessment (IMA)
- Cloud Readiness Assessment
- Open Source Assessment

Pricing: This additional packaged consulting service is optional and is a chargeable event. Claranet provides three prices for each assessment depending on the size of your company and the complexity of your requirements: Small / Medium / Large.

Consulting

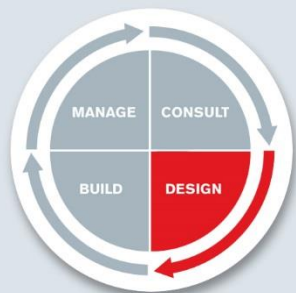
A packaged consulting approach can be of significant help to many organisations. However, Claranet also provide a specialist consulting service that can be used at any time (including pre-contract) to help you in areas outside of the packaged offering. This engagement is specific to you and can cover any area that is needed with regard to your business and technology.

What Claranet will do

Specialist consulting: Provide a range of specialist expertise in a variety of areas. This includes a detailed focus on your business in order to ascertain the scoping requirement or where you are unsure as to the direction your business should take in the ever-changing IT environment.

Outcomes: Provide a full and detailed report on your available options along with recommendations of the next steps to take.

Pricing: This additional consulting service is optional and is a chargeable event and is based on a consultancy day rate.



Design

Your Claranet Managed Hosting Solution is a combination of many service elements and options. The choice as to which elements and options will be used to meet your requirements is made in the Design stage.

Claranet will undertake to identify which elements and options are required and how they should be configured to meet your requirements. Your solution will normally require the utilisation of a Solution Architect and the output of this process is a proposal document and a Statement of Works (SoW). This forms part of your agreement and will provide the technical specifications for your solution.

Typically the technical design will be completed prior to order, but further detail can be refined once the order has been placed. Any technical design work is conducted on a 'reasonable commercial endeavours' basis and will be based on assumptions made by you and Claranet.

What Claranet will do

Deliverable: A proposal document and a Statement of Works which forms part of your agreement which is detailed enough to allow a full quotation.

Standard level of design work: Produce design work on your proposed solution at a level commensurate with that of the market. It will be sufficient to allow further decisions to be made and may include input from a Claranet Sales Specialist. However, fully specifying a complex complete new hosting infrastructure is not part of the standard design work. If this is required at this stage, it can be completed using Claranet's Specialist Solution Design service.

Additional components: In the event that additional components are required outside of the SoW, Claranet will levy additional charges for the implementation and management of the modified solution. If this is the case, a new proposal and SoW document is produced. This must then be signed by you to acknowledge and accept the changes before any work is performed.

What Claranet will do

Additional load: Identify any substantial increment in either traffic or load on your solution. Claranet may also recommend that additional components are purchased to support the changes. If these recommendations are not taken this may affect your SLA and Service Credits.

What you will do

Systems outline: Outline the purpose of any system to Claranet, in order to ensure that Claranet may assess whether the solution is suitable for the requirement.

Managed Hosting sales specialist

As part of your standard Managed Hosting Service, Claranet provides a Managed Hosting sales specialists who has detailed knowledge within this particular field, or within your own specialist vertical industry, and will support your Account Manager and Solutions Architect with your proposal. Part of their role is also to help ensure that the proposed technical solution will fit your business and achieve the outcomes you are looking for.

Specialist solution design

At times, the complexity of your solution design will require additional or specialist design work in order to detail your requirements.



What Claranet will do

Specialist level of design work: Produce technical design work on your proposed solution in order to specify your requirements fully. This may be completed by a Solutions Architect or a Claranet Technical Specialist in that particular field.

Pricing: This additional specialist solution design service is optional and is a chargeable event and is based on a day rate for the service.

Extreme scenarios

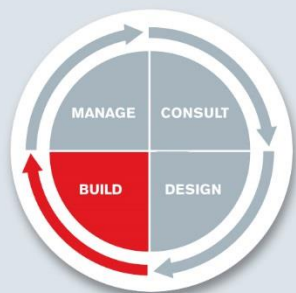
Whilst the Managed Hosting Service portfolio is designed to cater for the most typical requirements, there are some scenarios where these services may not fulfil your specific requirements. Some examples may include:

- Where high level security and compliance accreditation is required. As an example, where UK Government Business Impact accreditations are required at secure confidential (IL2/3) or higher. These may include government, military and health systems.
- Where extremely low latency is required, such as financial trading platforms.
- Where the software used will generate abnormally high I/O workloads, such as a cloud-based anti-virus scanning platform.
- Where the software used will generate abnormally high graphics I/O, such as virtual desktop infrastructure or computer aided design (CAD).
- Where the software used will generate abnormally high levels of network traffic, such as providing an online backup service, where multiple Customers may restore or perform seed backups at any one time; or any other file sharing services.



What Claranet will do

Extreme scenarios: Advise that the services are not fit for purpose and propose alternatives within the Claranet portfolio or provide alternative suppliers where this is applicable.



Build

Once your order has been placed, Claranet will perform installation and configuration activities to build your solution in the Claranet datacentre.

The **Build** section covers the steps involving the configuration and installation of the Managed Hosting Service according to the agreed specifications. At the completion of this phase, the service is fully tested and handed over to you with a Handover Document. Once accepted, any future changes will be managed as part of In-Life Management, details of which can be found in the **Manage** section.

The implementation of your solution follows the process defined in the document “Welcome to Service Delivery”.

Building your solution

Claranet provide the necessary engineering and project co-ordination in order to deliver your solution to you. This will involve engineering support from within the Hosting Implementation team to build your solution as well as a Project Co-Ordinator who will guide your project from implementation through to handover. There are a number of steps that need to be followed and our support teams are there to ensure it goes smoothly.

The table below shows a listing of the activities performed as part of a managed build for the general platform, not all of which may be applicable. The list of tasks does not imply an exact order in which tasks are performed and is to be used as an example. Details of the build requirements for a Managed Server, a Managed Self-Service Hypervisor and a Managed Hypervisor can be found in their respective sections in the **Appendix**.

Table: Build task list for a general platform

Tasks
Procure (if required) and configure your compute layer
Procure (if required) and configure your storage
Allocate a block of public and a block of private IP addresses
Register all public IP address allocations with RIPE
Purchase SSL certificates
Configure firewall to default configuration and customise firewall policies based on your request
Setup Internet or network bandwidth and routing to firewall
Allocate virtual IP(s) for load balancing if required
Install and configure hypervisor where required
Create new account on vCentre (Managed Self-Service Hypervisor only)
Create pools of vCPU, vRAM and storage resource
Prepare monitoring system to monitor new services

What Claranet will do

Additional tasks: Perform additional tasks outside those described below and as part of the service elsewhere in the document. There is an additional charge for the engineering time incurred to perform these tasks. Any requirements in

addition to those agreed in the order may be able to be fulfilled; however, this will also have an impact on the implementation time frame. Claranet reserves the right to charge on a time and materials basis for any additional work.

Managed Server and Managed Hypervisor

As part of the build process, the default configurations used are as follows:

Table: Configuration parameters for the Managed Server and Managed Hypervisor

Operating System	Configuration parameters
Windows Server	<p>System, security and application logs will be overwritten when <16MB in size</p> <p>Web application DLLs can be installed at provisioning time if commercially available and supported by a software vendor</p>
Linux	<p>System and security logs are rotated every week maintaining 4 weeks' worth of log information</p> <p>All services other than SSH will be set to not start on system boot</p> <p>Claranet will utilise only packages supplied by the Linux distribution vendor only. Non-vendor packages are not supported</p> <p>No compilers (C, C++, etc.) are installed or supported</p>

What you will do

NOT Install: Unless an exception is formally approved, you are **not permitted** to install or use the following.

- Hypervisor software such as Hyper-V, VMware Workstation or KVM, whether standalone or integrated into the Operating System
- The Storage Spaces feature of Windows Server 2012 onwards, or any storage de-duplication software or feature
- Windows Deployment Services (WDS)
- Application virtualisation or streaming technology such as Microsoft App-V
- Active Directory Rights Management Services (RMS)
- Any backup or replication software, including those that perform a backup to a remote server (sometimes called 'online backup')
- The terminal services/remote desktop services role of Windows Server (any version) except for system administration and limited to 2 users

- Software applications that synchronise data from a server to a server in a service provider's data centre, such as Drop Box. This is prohibited in order to prevent data being transferred outside the security boundary of the Claranet network
- Software that performs monitoring of servers or traffic sniffing
- A bare-metal hypervisor (such as VMware) or a hypervisor within an Operating System (including software such as Parallels or VMware Workstation)
- Software that performs provisioning of virtual machines or other resources that are within the Claranet data centre
- Software that performs a large or high intensity transfer of data away from, or into, the server such as a batch import process or upload of a virtual machine contents to a public cloud
- Any application or feature that consumes or creates abnormally high I/O throughput
- Any illegal software that could be used to probe/interrogate/hack along with any software that could be used to cause copyright infringement or circumvent any licensing on servers
- Any software that allows remote access publicly to the server that hasn't been security vetted by Claranet
- Booting a physical server from an Operating System image (PXE boot) on shared storage is not permitted. Use of CD or DVD media is not permitted and you should upload any media as an ISO images

Runbook

For complex platforms or applications e.g. those that involve the 'Managed Web Service' or 'Managed Database Service' components, Claranet may, during the **Build** phase, create a **customer runbook**. A runbook is a support document that is maintained by Claranet and yourself for the duration of the contract, and acts as an authoritative source for technical information about your applications used in the solution. The runbook is useful in helping Claranet and yourself resolve any application issues which may arise.

What you will do

Runbook: Contribute to the content and maintenance of the runbook documentation where applicable.

Specialist engineering

It may be that your particular setup requires additional specialist engineering work. This will be quoted individually and could include specialist change requests, work on piloting projects or prototyping.



What Claranet will do

Specialist engineering: Provide a quotation for specialist engineering work based on a day rate.

Project Management

Some Claranet projects are small, simple and very straightforward and the management of these is part of the normal operation carried out by your Account Manager, the Solution Architect and Project Co-ordinator who are already built into the cost of delivering your standard service. Other Claranet projects are much more complex and require more comprehensive project management to bring together the many elements that are needed. Claranet is conscious of the fact that the introduction of a Claranet Project Manager is a chargeable event but will suggest this when we believe it is justifiable and necessary. In addition, it may be that only a short time needs to be spent by a Claranet Project Manager in overseeing and authorising the Claranet project e.g. at the start of the project, where the project is then managed by a Project Co-ordinator, helping to keep your costs to a minimum.



What Claranet will do

Project Management: Allocate a Claranet Project Manager who is PRINCE2 qualified who will ensure that the project is initiated, implemented, carried out and closed according to PRINCE2 methodology and will be responsible for the overall control and management of the Claranet project. Full details of this can be found in the Project Management Service Description and from your Account Manager.

Testing and acceptance

Testing

The engineer configuring your service will ensure that any testing process is as transparent as possible. If actions are identified as part of this process they will be included in your delivery plan and managed to closure by your Project Owner.



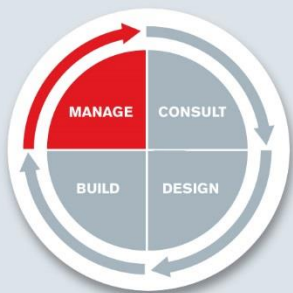
What Claranet will do

Testing: Test the hosting environment to ensure that it performs in terms of connectivity in accordance with the Service Levels.

Backing up the login details: Take a backup of any configuration (e.g. firewall) and retain this along with details of the administration logins and password prior to acceptance.

Acceptance procedure and Handover Document

Once the hosting service is setup and connected, the ongoing management is under the process of the In-Life Management process managed by our Service Operations Team. As part of the acceptance procedure, you will be provided with a Handover Document. This contains details of how to make the most of the support facilities and who to contact in case of a query or fault.



Manage

Your solution is managed In-Life by our Service Operations team who provide a pro-active, ITIL aligned service. You also have access to your customer portal, Claranet Online.

In-Life Management

Once your service is up and running, and the Handover Document is completed, Claranet will monitor your storage platform against a number of performance and availability metrics and where applicable, manage your service 24x7x365 in order to maintain its operation. The parameters of the ongoing management of the service and the appropriate roles and responsibilities are outlined in the areas below.

Planned changes, emergency maintenance

What Claranet will do

Notice: Provide at least seven working days' notice of any planned maintenance work where an outage is expected or a reduction in the resiliency of infrastructure, wherever possible.

Supplier planned Engineering: Notify you of any supplier planned engineering works where it is likely that you will experience an outage within one day of receipt of the notification from our supplier wherever possible.

Notification: Notify your nominated contacts through two primary channels, Claranet Online and by email notification. An email is sent to the nominated contact and details are announced through the notifications in Claranet Online. The notification will contain the date and time of the maintenance, the reason, the service affected and the likely impact to you.

Problems occurring during planned maintenance: The Major Incident process will be invoked during the maintenance window where a rollback or issue mitigation process does not exist, or should the planned work extend beyond the planned maintenance window.

What Claranet will do

Emergency maintenance: Provide as much notice as possible and we will seek to ensure minimal disruption. Wherever possible, changes will be made at periods of low service utilization. It may be necessary to make changes **without** prior notification to ensure the continued operation of the managed service.

Patching: Apply all critical patch updates on an as required basis. Where non-critical patches are released, Claranet can apply these at your request.

Emergency outages: In some extreme cases, Claranet may require an emergency outage to rectify a problem. In such cases, Claranet will work with you to agree a mutually convenient time, but you agree that in such cases the problem cannot be rectified until the outage has taken place.

What you will do

Contact list: You will be responsible for providing and maintaining the contact details including the levels of authorisation that any individuals may have. Claranet will only provide any reporting information and change requests, to those personnel in accordance with this information. These details can be maintained within Claranet Online.

Patching

What Claranet will do

Patches to the hardware and hypervisor: Apply patches to the hardware and hypervisor as deemed appropriate and at Claranet's discretion.

Patches to Operating System: Apply patches as deemed to be critical or security related and at Claranet's discretion and based on classification by the respective vendor. Patching of the Operating System requires agent software to be installed in the Operating System.

Maintenance window: Apply the patches during the maintenance window except in the case of emergencies.

Automated software patches: The patches distributed by the automated software are tested and deployed as required. This means that some servers will have certain patches and some will not and there is not a blanket push of all patches to all servers. On occasion this means that some patches deemed necessary may be missed. These can be manually installed at another time or on request.

Workload transfer during patching: Engineers typically place one of two nodes into maintenance mode and transfer the workload onto the other. The first node will then be patched and tested. The same procedure will be repeated on the second node. This is generally appropriate to hypervisor or hardware related patches.

Patching the Managed Self-Service Hypervisor tooling: Patch the self-service tool used for the 'Managed Self-Service Hypervisor' component where necessary and this should not interrupt functioning of the hypervisor nodes, but access to the tooling will be disrupted.

Testing of patches: Test patches on a Claranet shared test server before rollout. The patches are not tested on your individual server. Patches will be rolled back if it appears to cause a serious degree of system instability.

What you will do

Opting out of patching: You can manually request to opt out of patching, by specifically requesting this during the pre-sales process. Where this has been requested, it will be recorded in the Handover Documents. You then accept any responsibility for any issues caused by Operating System patches not being applied, and Claranet may at its discretion decline to provide support for issues where a patch should, in Claranet's opinion, have been deployed.

Prohibiting patching: You are responsible for ensuring that your personnel do not in any way delay or prohibit the application of mandatory patches to servers, applications and databases.

Maintenance windows

Claranet operate a number of maintenance windows. The selection of a maintenance window for each option minimises disruption because, for example, two Managed Servers which are performing the same role can be taken offline for patching on different dates. The maintenance period during these windows will often be brief or not used at all, and your service is typically uninterrupted during scheduled maintenance windows.

Table: A schedule of the maintenance windows

Day	Window start time	Window end time
First Tuesday of each month	Tuesday, 23:50 GMT	Wednesday, 03:00 GMT
First Wednesday of each month	Wednesday, 23:50 GMT	Thursday, 03:00 GMT
First Thursday of each month	Thursday, 23:50 GMT	Friday, 03:00 GMT
Third Tuesday of each month	Tuesday, 23:50 GMT	Wednesday, 03:00 GMT
Third Thursday of each month	Thursday, 23:50 GMT	Friday, 03:00 GMT

What you will do

Select a maintenance window: You will select a maintenance window to help minimise disruption.

Changes requested by you

Where you require specific changes to be made to the configuration of your Managed Server or Managed Hypervisor, Claranet will be responsible for making the change as you are not permitted to access the Operating System, hypervisor (where applicable) and compute hardware in order to change the configuration yourself. Change requests are made by raising a ticket through Claranet Online and details of how to do this can be found in the **Appendix: Help and Support**.

What you will do

Access to change the configuration: You will have no access to change the configuration of the Operating System, hypervisor (where applicable) and compute layer.

Change control process: It is your responsibility to familiarise yourself with the official Claranet change control process and to follow this process every time a change to the Service is required. Details of this process can be found in **Appendix: Help and Support**.

Change request impact: It is your responsibility to ensure that any changes will not directly cause a service outage or other disruption of the service.

Change of services: If you request a new service, a change of service type, additional users or a change in service features they must be requested via your Account Manager and may be subject to prevailing fees.

Monitoring of the platform

Claranet will monitor key technical performance thresholds relating to your Managed Hosting Service 24x7x365. A list of the metrics that are monitored and the frequency of the monitoring can be found below.

What Claranet will do

Platform monitoring: Monitor for signs that indicate that the Managed Server or the Managed Hypervisor may have malfunctioned or is likely to do so. Claranet will then undertake technical engineering tasks either to resume the Service or prevent interruption to Service. Such tasks include:

Resolve identified issues:

Monitor the platform and take appropriate action to resolve identified issues.

Faulty hardware:

Replacement of faulty hardware components.

Rebuild:

Re-build of the Operating System disk in the event of corruption.

Monitoring of storage metrics

Table: Technical Metrics – Storage performance and availability

Monitored item	Threshold	Severity
Capacity management Free space left within Datastore - for dedicated or SSH	<=12% and/or <=200GB remaining	Warning
Capacity management Free space left within Datastore - for Managed Server	<= 100GB remaining	Minor
Capacity management Free space left within Datastore	<= 60GB remaining	Major
Performance Rejected I/O's	I/O's are rejected	Major
Performance Delayed I/O's	I/O's below latency threshold	Warning
Performance I/O thresholds are breached within a VVSET	>100% (I/O's are dropped)	Minor
Bandwidth Bandwidth utilisation too high (for dedicated or SSH)	>85% of bandwidth available	Minor

Monitoring a Managed Server or a Managed Hypervisor

What Claranet will do

Installation of a monitoring agent: Install a monitoring agent on to each Managed Server. These agents continually send data to the Claranet monitoring system about the monitored items shown in the following table which shows the default values. These values may be adjusted during the life of the contract subject to the mutual agreement of you and Claranet.

What you will do

Installation of 3rd party software: Check and verify with Claranet that any agents you wish to install will not adversely affect the operation of any other agent.

Responsibility for issues arising: You are responsible at all times for issues arising where the suspected cause is your software or your code running on the server. For the avoidance of doubt, any support to resolve these issues is provided by Claranet on a reasonable commercial endeavors basis only.

Notification: You are responsible for notifying Claranet of any changes that may affect platform stability or security.

3rd party hardware: Should a server or other hardware which is not housed in a Claranet data centre be included in any configuration (including as part of a SQL replication topology), you accept responsibility for the configuration, management and maintenance of those servers or hardware

Default values for monitoring of servers running Microsoft Windows

Monitored item	Threshold	Frequency	Persistence	Severity
Availability General connectivity (ping)	Ping failure	300s	1	Major
Performance High Physical Memory utilisation	>=90%; and Pages/sec >= 200	300s	3	Minor
Performance High Virtual Memory utilisation	>=85%	300s	3	Minor
Performance High CPU Utilisation	>95%	300s	3	Warning
Capacity management Available Logical Disk Space (per disk volume)	<=5% and MB Free < 5120 MB	300s	3	Minor
Capacity management Available Logical Disk Space (per disk volume)	<=5% and MB Free <=2048 MB	120s	5	Minor
Performance Paging file utilisation	>=85%	300s	3	Minor

Performance High Network Errors 4	>5%	300s	3	Warning
Availability Service Not Running 5	n/a	60s	5	Minor
Availability Unexpected Shutdown (Error ID 6008)	n/a	n/a	1	Minor

Default values for monitoring for servers running Linux

Monitored item	Threshold	Frequency	Persistence	Severity
Availability General connectivity (ping)	Ping failure	300s	1	Major
Performance High Virtual Memory utilisation	>=90%	300s	3	Minor
Performance High CPU Utilisation	>95%	300s	3	Warning
Performance High System Load ¹	>=(CPU count*4)	300s	3	Warning
Performance High CPU I/O Wait State ²	>80%	300s	5	Warning
Capacity management Available Logical Disk Space (per disk volume)	<=5% and MB Free < 5120 MB	300s	3	Minor
Capacity management Available Logical Disk Space (per disk volume)	<=5% and MB Free <=2048 MB	120s	5	Minor

Availability Available Logical Disk I nodes	< 5%	120s	5	Minor
Performance High Network Collisions ³	>=5%	300s	1	Warning
Performance High Network Errors ⁴	>=5%	300s	1	Warning
Availability Any of the following processes are Not Running: crond, ntpd, sendmail, sshd, syslogd ⁵	n/a	120s	3	Minor

For Physical Servers ⁶

Monitored item	Severity
Any of these events have occurred: Availability Hard disk failure, Power Supply Unit Failure, RAID controller failure (if applicable), Logical drive failure, System temperature anomalies, Network interface card failure, System Fan(s) Failure.	Major

For Hypervisors

Monitored item	Severity
Availability ESX host failure occurs	Major

Notes:

¹ High system load over the previous 60s has been greater than 4

² Aggregate for all processors installed in the system

⁴ As a percentage of all network packets in a 300s allotment of time

³ Network collisions within a 300s allotment of time

⁵ The following system services: dnscache, eventlog, lanmanServer, LanmanWorkstation, PlugPlay, RpcSs, lanmanserver, lanmanworkstation

⁶ Supported models only

Technical engineering

With a Managed Server or a Managed Hypervisor, Claranet assume responsibility for the hardware, the compute layer and up to and including the Operating System.

What Claranet will do

Technical engineering during business hours: Perform technical engineering tasks to manage physical hardware, the VMware hypervisor and the OS configuration on behalf of the Customer. Claranet will perform the following tasks:

Anti-Virus:

Management of Operating System anti-virus protection.

Changes:

Make the changes in accordance with the change request procedure for any server configuration. This includes any changes requested to allocated CPU and memory to your individual virtual servers. These changes may require a reboot.

Capacity increases:

Add additional capacity to shared infrastructure where required.

Technical engineering outside business hours: Perform technical engineering tasks to manage physical hardware, the VMware hypervisor and the OS configuration on behalf of the Customer. Claranet will perform the following tasks:

Patching:

Please see the section on patching; Upgrades to a new version of an Operating System, e.g. Windows Server 2008 to Windows Server 2012, are not included.

This component does not include the setup or configuration of Microsoft Active Directory Services (AD DS). A separate Service is available which provides these services.

When a threshold is breached

Where the monitoring system identifies that a threshold is breached, alarms are triggered to alert Claranet support staff to investigate the cause and resolve the issue. For example, storage threshold alerts can be seen below.

What Claranet will do

Monitor storage averages: Monitor based on 5 minute averages due to the nature of storage traffic to ensure the highest performance and stability of the array and all customers' volumes. Very short peaks in latency or performance may average out across this time. Claranet has designed the monitoring agents in this way in order to avoid flooding the arrays with monitoring data.

Pro-active alerts: Monitor pro-active alerts that are in place on the platform and datastores to ensure there are no bottlenecks.

Individual storage VMDKs: Peaks in I/O may be down to a specific application's requirement at a specific time. Claranet do **not** alert on the individual VMDK's. The priority is to ensure that each drive has availability to the performance relating to the tier. We will not receive a proactive alert if those limits are being reached.

What you will do

Contact support: If you do experience continued loss of performance, please contact the Claranet support desk and raise a support ticket so that it can be investigated.

If a threshold is breached or a service affecting event occurs, the Claranet Operations team are notified to raise a ticket and take appropriate action to resolve the issue. This could include troubleshooting and resolving the problem, or notifying you that your application may be pushing a large amount of data. There are predefined response times to event notifications based on the severity of the issue. These are outlined below.

What Claranet will do

Severity response times: Respond to a threshold breach depending on the severity of the breach:

Major:
Claranet will acknowledge any alarms on the system within 30 minutes

Minor:
Claranet will acknowledge any alarms on the system within 60 minutes

Warning:
Claranet will acknowledge any alarms on the system within 1 day

Change to monitoring tools: Reserve the right to change its monitoring tools, methods, parameters and polling intervals over time

Where these storage thresholds have been breached for three consecutive calendar days, any downtime resulting directly or indirectly from insufficient storage will not be counted in the calculation of availability Service Levels.

Help and support

Service Desk support

What Claranet will do

Support times and Service Desk: Provide support 24x7x365 once the Managed Service has been handed over to you. Full details of how you can make the most of this service will be provided in your Handover Document.

Raising tickets: Changes to your service configuration can be made through the Claranet Online ticket request and details of this can be found in the **Appendix: Help and Support**.

Escalation: In the event that an escalation is required, Claranet provides a clear escalation process to allow you to contact the appropriate person within the company. Details of this can be found in the **Appendix: Help and Support**.

Service Levels

The Service Level determines the parameters by which the service is accountable. Many of the components of your service are designed to operate in a high availability configuration, with which there is an implied acceptance that from time to time an element of infrastructure may fail. Therefore for high availability options of components, unscheduled downtime is not considered to have occurred if one element fails and another element takes over the workload. For example, in a server environment consisting of four nodes

designed to suffer the loss of a single node, loss of a single node would not be considered downtime if workloads are restarted on other nodes, but loss of two nodes would be considered downtime or if the workload fails to restart. Details of the metrics showing the expected service levels can be found in the **Appendix: Service Levels**.

What Claranet will do

Information delivery: Obtain the results for each of the metrics above and contact you according to your list of authorised contacts in the event that any results fall outside of the acceptable parameters.

Archiving results: Retain an archive version of the monitoring results for up to 90 days which can be available to you on request through the Claranet Online portal.

Metrics exceeding the thresholds: In the event that a monitored metric exceeds the acceptable thresholds, Claranet will raise a support call to investigate the incident and contact you in accordance with the escalation details held.

Managed Service Options

As competition in your industry increases and product lifecycles become shorter, IT departments face constant pressure to respond efficiently. The ability to do this is often limited by workloads, IT expertise and budget restrictions causing delays and shortfalls. Claranet provide a flexible range of Managed Services levels around the Managed Hosting Service to allow you to select precisely the level suited to you and the level of your business expertise.

Standard Managed Service

With this level, Claranet will measure and monitor specific technical and service metrics associated with the Managed Hosting service you have purchased. Typically these metrics are based around availability and performance and are used to ensure that the service is available. Claranet will test the service around given thresholds and the results are communicated to you through Claranet Online and/or by email notification. It may be that Claranet acts automatically on this information to ensure the smooth running of your Service. Details of the specific metrics for the Managed Hosting Service that are covered

as Standard are detailed in this document within this section as well as in individual sections in the Appendix.

Additional Managed Service Levels

Claranet appreciate that some customers require a more detailed and pro-active Managed Service and offer 3 levels of service. These levels are chargeable and details of the respective levels can be obtained from your Account Manager.

- Service Managed
- Service Managed Premium
- Service Managed Premium Plus



Appendices

Here you will find further information regarding the technical specifications of the service as well as standard procedures and agreements.

Definitions

The following terms refer to Claranet deliverables, departments and technology:

Term	Definition
Handover Documents	Set of documents produced by Claranet for you. These detail the technical configuration, usernames, passwords, contact details, information and processes relevant to the support of your solution.
Solution Support	Facility that Claranet provides for you to raise issues, faults and questions related to the Services purchased via telephone, email or some other communication medium. Calls to Solution Support will be answered in English.
SoW	Statement of Work. A Claranet document used to capture your specific requirements for the implementation of your Service. The SoW forms part of the Order.
Open Files	Data files on a server that are actively being accessed by a user or a software program and may be in the state of being updated. In some circumstances, a backup of these files cannot be taken.
Operating System (OS)	Basic software installed on a server which provides an interface between the server hardware and the various applications running on it. Examples of an Operating System are Microsoft Windows Server and Linux.

Term	Definition
VLAN	Virtual Local Area Network. The term VLAN was specified by IEEE 802.1Q; it defines a method of differentiating traffic on a LAN by tagging the Ethernet frames. By extension, VLAN is used to mean the traffic separated by Ethernet frame tagging or similar mechanisms.
Virtual Volume Set (VVSET)	A logical container holding one or more volumes.
Volume	An amount of storage attached to an individual Drive in a server.

The elements of this service are:

Term	Definition
Compute services	
Managed Server	To provide an instance of an Operating System that is running on either a hypervisor or directly on physical hardware. Claranet manage the infrastructure up to and including the Operating System configuration. You have full administration privileges and can connect to the Operating System to install software.
Managed Hypervisor	Similar to 'Managed Self-Service Hypervisor' except that a self-service portal is not provided and all provisioning is performed by Claranet.

Term	Definition
Managed Self-Service Hypervisor	To provide a virtualisation hypervisor on compute hardware dedicated to you. You can use a self-service portal to provision and change virtual machines, and you are responsible for managing all Operating Systems, applications and databases.
Components	
Managed Firewall with Internet Breakout	To secure incoming and outgoing traffic, secure traffic between servers, and breakout to the Internet from hosting servers or a Claranet MPLS network.
Managed Load Balancer	To distribute incoming network traffic evenly between multiple servers performing the same role.
Managed Backup	To allow data to be recovered if accidentally deleted and within a certain time window.
Managed SSL Certificates	To facilitate encrypted communications with a website and to confirm to a user that a server is not impersonating another.
Managed Switching	To connect physical hardware such as servers and SANs to the physical network.
Roles	
Managed Role Server	Similar to Managed Server, except that one or more server roles are also managed by Claranet.
Managed Database Service	Similar to Managed Server, but is used to provide an instance of an Operating System that is running database server software such as Microsoft SQL Server. Claranet manage the infrastructure up to the database server configuration level. You can access the database instance using database tools to perform queries but cannot access the Operating System or database server configuration to make changes.
Managed Additional Database Instance	Used to split a Managed Database Server into multiple, segregated database environments.

Term	Definition
Managed Web Service	Similar to Managed Server, but is used to provide an instance of an Operating System that is running just web server software such as Microsoft IIS or Apache. Claranet manage the infrastructure up to the web server configuration level. You upload new code to a holding area, and then raise a change request for Claranet to make the code 'live'. You cannot access the Operating System or web server configuration to make changes.
Managed URL Test	To perform a regular automated test that verifies if a web site is functioning as expected, triggering alerts if a test fails.
Design phase	
Managed Technical Design	To translate your requirements into a technology solution.
Build phase	
Managed Build	To install and configure the solution. For more complex solutions, Claranet will also produce Customer specific documentation called a 'runbook' that contains relevant detail about the Customer applications.

Claranet UK Data centres

The services are provided from two of Claranet's UK data centres – London Hoddlesdon and London Sovereign House. Both of these data centres meet the following specifications:

- Redundant power supplies are implemented. Hardware is connected to two separate Power Distribution Units (PDUs)
- Very Early Smoke Detection Apparatus (VESDA) is used
- A fire suppression system is installed - at London Sovereign House, a water-based system called micro-mist is used and at Hoddlesdon a gas based system is used
- All components are fire-retardant including racks, cables and cable management
- The environment is maintained by close-control down-flow air conditioning units that offer stable temperatures and humidity

- The data centre is manned and monitored by on-site security personnel with CCTV motion-sensitive and time-lapsed perimeter and interior monitoring
- Dual-authentication access is in place for Claranet technical staff, using Proximity Access Control (PAC) keys and biometric scanning

These services can also be provided in the Claranet Bristol Abbeywood datacentre, but only for Customers who already have a significant number of services located in that data centre. The services are not currently available in any other Claranet data centres.



What Claranet will do

Data centre audit requests: Provide the facility for organised data centre visits. Claranet retain the right to charge for any expenses incurred during an audit visit. An audit will be defined as allowing a review and examination of systems, data security and physical security of the Data Centre. Any questions and names of individuals must be forwarded prior to the audit to the Account Manager assigned to you within Claranet. Claranet will specify a date and time when it is suitable for an audit to occur. This can be arranged by contacting the Account Manager.

Location within the data centre: Where your solution includes hardware dedicated to you, and unless specifically stated otherwise, Claranet will allocate data centre space at its discretion. Claranet cannot therefore make any guarantees or commitments with regards to the physical proximity between pieces of hardware allocated to you.

Relocation of equipment: Be entitled, upon giving no less than three months written notice to you, to move equipment used in connection with the provision of the Services between Claranet data centres within the UK. You agree to co-operate in good faith to facilitate any such relocation. Claranet shall be responsible for any costs and expenses incurred as a result of any such relocation and will use reasonable efforts to minimise and avoid any interruption to the Service.

Appendix: Compute services

Managed Server

General scope

Claranet will provide an instance of an Operating System that is running on either a hypervisor or directly on physical hardware. Claranet manage the infrastructure up to and including the Operating System configuration. You have full administration privileges and can connect to the Operating System to install software.




What Claranet will do

Operating system: Provide an instance of an Operating System that is running on either a hypervisor or directly on physical hardware.

Management scope: Manage the infrastructure up to and including the Operating System configuration. Claranet manages the configuration of the Operating System, hypervisor (where applicable) and compute hardware. You have full administration privileges and can connect to the Operating System to install software.

Rebuilding of the Operating System: Re-build the Operating System back to the initial state at which it was handed to you if you damage it. Claranet will not attempt repairs to the Operating System.

Changes to platforms: Reserve the right to change its tooling, methods, monitored parameters and polling intervals on an as needed basis.

 **What you will do**

Installation of software: Install and manage your own software onto the Operating System using a remote connection. Claranet do not support any customer applications.

Building your Managed Server

Table: Build task list for each Managed Server

Task

- Create virtual machines
- Install Operating System
- Install anti-virus agent and apply latest updates (if applicable)
- Patch Operating System to all current updates
- Configure Operating System
- Configure Windows clustering (where required)
- Install loopback interface for virtual machines using load balancer if required
- Configure virtual machine backup snapshot schedule
- Install backup agent software onto server (where required)
- Take a full backup of each server
- Install Operating System monitoring agent
- Add each virtual server to monitoring
- Configure server to use SMTP relay (where required)

Each server can be delivered in one of three ways:

1. Shared Virtualised Host:

The server is setup as a virtual machine on the secure, enterprise grade Claranet Hosting platform;

2. Dedicated Virtualised Host:

As above, except that the virtual machine is running on the Managed Hypervisor service, or where two or more physical servers are dedicated to the Customer and are running a hypervisor;

3. Dedicated Physical Host:

As above, except that a hypervisor is not used and the Operating System is installed directly ('natively') onto physical hardware.

Operating Systems

Each server runs either a Microsoft Windows Server or Linux Operating System. This component provides support for the versions of Operating System shown in the table below. Any other software or versions must be agreed as a bespoke service. Claranet will only be able to support Operating Systems that are maintained at a level supported by the Operating System vendor and this level of support cannot be extraordinary support. Once an Operating System is no longer supported by the software vendor, Claranet may continue to provide reasonable support, however this level of support invalidates the Service Level Agreement.

Table: Supported Operating System versions

Family	Version
Microsoft Windows Server	Microsoft Windows Server 2012 R2
	Microsoft Windows Server 2012
	Microsoft Windows Server 2008 R2 Enterprise Edition 64-bit (default)
	Microsoft Windows Server 2008 – Enterprise Edition
	Microsoft Windows Server 2008 – Web Edition

Family	Version
Linux	Centos 6 (default)
	Centos 7
	Ubuntu 14.04

Repositories

What Claranet will do

RHEL based repositories: By default use RHEL based repositories and are therefore supported by RedHat.

SCL repositories: On occasion and by request, Claranet can also use SCL. Please be aware that this repository is CentOS based, open-source and therefore not supported by a vendor. Whilst SCL is generally considered a reliable source, Claranet will take no responsibility if requested to use this repository and there is a failure in the Operating System. In this instance Claranet will rebuild the Operating System back to the original state as outlined, but will not attempt repairs. The Service Level Agreement will not apply.

Anti-Virus

What Claranet will do

Installation: Install a software anti-virus agent onto each Windows Managed Server and is configured for best performance. Claranet can install a software anti-virus agent onto Linux on request, but this is not standard. Claranet reserves the right to change the deployed anti-virus technology from time to time.

Updates: The Claranet agent will check in on a regular basis with the shared Claranet anti-virus server and then deploy the latest anti-virus updates onto the server.

Scanning: Operate real-time scanning and a full scan outside of the core business week (any time other than 08:00 to 20:00 on each week day).

What you will do

Before uploading files: You are responsible for scanning any data (such as executable files) before uploading it to a Managed Server, and for taking appropriate precautions to prevent the transmission of viruses onto and away from the servers.

The hosting platform

All hardware is owned by Claranet and located in a Claranet data centre. All servers will have resilient connections to the power system via Redundant Power Supply (RPS) to separate Power Distribution Units (PDU). You may not physically access the server under any circumstances.

The Claranet Hosting platform is built using industry standard blade servers which are securely segregated using a hypervisor for consumption by multiple Customers. Memory in the servers is not contended (shared across multiple virtual machines). Virtual processors (vCPUs) are contended because on average CPUs are not fully utilised. Claranet monitor the platform on an on-going basis and apply a contention ratio that ensures maximum cost effectiveness for Customers without causing detrimental performance.

The available options of this component are shown below. You can purchase one or more of each of the Managed Server options, each representing a single virtual server.

Dedicated hardware is not included as part of this component.

Description

Managed Server (Shared Virtualised Host) – Windows

Managed Server (Shared Virtualised Host) – Linux

Managed Server (Dedicated Virtualised Host) – Windows

Managed Server (Dedicated Virtualised Host) – Linux

Managed Server (Dedicated Physical Host) – Windows

Managed Server (Dedicated Physical Host) – Linux

Managed Self Service Hypervisor

Managed Self-Service Hypervisor delivers an enterprise class, scalable IT infrastructure in a secure hosted environment that allows you to self-provision virtual machines on hardware

which is dedicated to you. Managed Self-Service Hypervisor provides a platform for you to deliver your applications back to the business without the need to purchase or manage the underlying infrastructure.



What Claranet will do

Management scope: Manage the platform up to the hypervisor level.

Installation of the hypervisor: A number of physical server blades (called 'nodes') are dedicated to you, onto which Claranet installs the VMware vSphere hypervisor. Each node will be the same specification.

Customer segregation: Provide access to an instance of management software for you to build and manage your virtual machines. Each Customer is securely segregated using the vCenter software.

Orchestration software: Modify or replace the orchestration software from time to time if necessary and any alternative will provide similar or enhanced functionality.

Nodes

Each node has two CPU sockets. Each processor socket uses a hex-core (6 core) processor. Each physical core is divided into four virtual CPUs (vCPUs). Each vCPU can only be assigned to one virtual machine, and least 30% of the total available vCPUs must be reserved for high-availability failover.

The available nodes are:

- 96GB RAM with 12 CPU cores (which provides 48 virtual CPUs)
- 192GB RAM with 12 CPU cores (which provides 48 virtual CPUs)
- 256GB RAM with 12 CPU cores (which provides 48 virtual CPUs)

It is not possible to buy a node with a different specification to those above. Each node is added to VMware vCenter as a host, and VMware High Availability is configured so that in the event that an individual node fails, virtual machines on that node will be automatically restarted on the another node. Nodes are split between two blade enclosures within the same data centre to provide increased resilience.

The available variants of this component are shown below.

Description

Managed Self-Service Hypervisor – Node with Windows (48 vCPUs, 96GB RAM)

Managed Self-Service Hypervisor – Node without Windows (48 vCPUs, 96GB RAM)

Managed Self-Service Hypervisor – Node with Windows (48 vCPUs, 192GB RAM)

Managed Self-Service Hypervisor – Node without Windows (48 vCPUs, 192GB RAM)

Managed Self-Service Hypervisor – Node with Windows (48 vCPUs, 256GB RAM)

Managed Self-Service Hypervisor – Node without Windows (48 vCPUs, 256GB RAM)



What Claranet will do

Node monitoring: Monitor the server hardware and the vSphere hypervisor software running on each node for errors but does not monitor the availability of your individual virtual machines.

Node availability guarantee: Guarantee the availability of the nodes under the Service Levels but, as the virtual machines are under your control, the availability of a specific virtual machine cannot be guaranteed.

High Availability: High Availability (HA) is configured by default and cannot be turned off.

Licensing: Provide licensing of VMware vSphere. Claranet license VMware, based on the quantity of RAM installed across the nodes, and cannot provide licensing based on the amount of RAM actively being used by virtual machines.

High Availability headroom: The licensing assumes that 30% of RAM installed across the nodes is reserved as "headroom" for High Availability. If at any point, you are using more than 70% of the installed RAM, additional licensing charges will apply and the Service Levels will not apply.



What you will do

Purchase of nodes: Purchase between 2 and 8 nodes, but all nodes must use the same variant (server model).

Access to the dedicated hardware: Ownership of hardware remains with Claranet at all times and you do not have physical access to the dedicated hardware.

Management scope: Manage the provisioning and configuration of the virtual machines, operating system, applications and databases.

vCenter account: Login to your account on vCenter. You will only see and be able to operate the virtual machines on your nodes. If you leave the service, you will not be entitled to use the VMware orchestration layer.

VM configuration: Agree to comply with any Claranet or vendor recommendations for virtual machine configuration, which may change from time to time.

VMware Tools: Agree to ensure that each virtual machine is always running the current version of VMware Tools.

VMware features: Some features of VMware may not be available to you in the VMware management software. You are able to perform live migrations of powered-on virtual machines (using the vMotion technology) but may not use the Distributed Resource Scheduling (DRS) feature of VMware.

Migration of powered off VMs: You are able to migrate powered-off virtual machines.

Snapshots: You are able to create multiple snapshots using vCentre. These should not be kept for longer than 48 hours. You acknowledge that the use of snapshots can degrade virtual machine performance and that any performance issues experienced whilst snapshots are in use will not be investigated. You also acknowledge that where snapshots are present, backup using the 'Managed Backup' component will fail for that virtual machine.

High Availability headroom: When provisioning and changing virtual machines, it is your responsibility to ensure that at least 30% of memory (vRAM), vCPU and storage are kept free at all times for vSphere High Availability (HA). The Service Levels will not apply for any period during which the nodes are in breach of this rule.

Breach: Alert restriction: If the 30% threshold is breached, alerts will not be triggered until there is 12% or less of resource available.

Breach: Licensing charges: Agree to inform Claranet via the Change Control process if at any time this is breached, as this will affect VMware licensing charges. In such circumstances, you agree to pay any additional licensing charges

Templates: Create your own templates using VMware vCenter as Claranet do not provide virtual machine templates or Operating System ISO images as part of the Service.

Software licensing



What Claranet will do

Windows Server Licensing: Provide two variants of the Self-Service Hypervisor, one with Microsoft Windows Server licensing, and one without. If any virtual machine will run Windows Server, then Windows licensing must be purchased from Claranet for all nodes. Claranet will then provide licensing for unlimited virtual machines running across the

nodes. You are not able to license Windows Server using your own License Mobility agreement and licenses provided by Claranet cannot be used outside of the nodes.

SQL SPLA licensing: Microsoft SQL Server is licensed based on the total number of virtual CPUs available to all virtual machines running SQL Server. The sum of the number of vCPUs for each applicable virtual machine must be provided to Claranet. Claranet will then license these under the Microsoft Service Provider Licensing Agreement (SPLA).

Licence ownership: Retain ownership of any licenses provided by Claranet that are provided for your use as part of the Managed Self-Service Hypervisor option. Claranet will ensure that the licenses remain in good standing with the respective vendor for the duration of your order.



What you will do

Microsoft Licence Mobility: You may choose to license other Microsoft software such as SQL Server using Microsoft License Mobility, where applicable. These licences must be maintained by you.

Microsoft Licence responsibility: Prove to Claranet that you have valid Microsoft licences for any other Microsoft software and keep these in good standing with Microsoft. You are responsible for paying any backdated charges and fines from Microsoft if you have:

- Told Claranet that you will supply licenses and have not done so; and/or
- Have not selected the options that include Windows licensing, but have been using Windows Server; and/or
- Any Microsoft licenses that are not valid for any reason.

If you have a Microsoft Select or Enterprise Agreement then you may provide your own Microsoft licenses, provided that you sign a hosting verification form. By signing the hosting verification form, you accept all responsibility for the software licenses and shall indemnify and hold Claranet harmless against any violation of the Microsoft licensing agreements

Licence responsibility: Ensure you have sufficient and appropriate software licences for the number of virtual machines and applications deployed. You are solely responsible for licensing of any software other than the Operating System, hypervisor and database clearly identified as being provided as part of the Service in this document. You must ensure that any other software supplied by you is licensed in accordance with the vendors licensing agreements. Whilst Claranet may assist in identifying the number of licenses required, it is ultimately your responsibility to ensure that you have sufficient and appropriate software licences for the number of virtual machines and applications deployed.

File transfer



What Claranet will do

FTP Server: Provide a File Transfer Protocol (FTP) server onto which virtual machine images or ISO files of up to 10GB in size can be uploaded. This is solely for the temporary storage of ISO and VMDK files before they are imported into a datastore.

FTP Server storage allocation: Provide storage allocation of 10GB per customer. Images should be kept on the FTP server for no longer than 3 working days. Any files above the 10GB size will be reviewed on a case by case basis, and Claranet may require you to purchase a dedicated FTP solution, which is outside the scope of this Service.

Transfers - Sovereign House: Transfer files where the nodes are located in Sovereign House at your request.

What you will do

Transfer media: Transfer files using FTP as files cannot be supplied on USB or other physical media.

Large file transfers: Make bespoke arrangements for images that are larger than 10GB in size. Such arrangements are outside the scope of this Service, and may incur additional charges.

Transfers – Hoddesdon and Sovereign House: Transfer files from the FTP server to your storage datastores where the nodes are located in Hoddesdon datacentre. Where the nodes are located in Sovereign House, this must be performed by Claranet and is requested via a Service Request. You remain responsible for the allocation of resources to your virtual machine.

Managed Hypervisor

The Managed Hypervisor component is similar to the ‘Managed Self-Service Hypervisor’ component, with a few differences:

What Claranet will do

Hardware reservation: Reserve the hardware exclusively to be used for hosting the ‘Managed Server’, ‘Managed Role Server’, ‘Managed Web Service’ and ‘Managed Database Service’ components.

RAM licensing: RAM is license based on RAM allocated to virtual machines, rather than the amount in the physical hardware.

Access and features: Use certain VMware features that are not available in Managed Self-Service Hypervisor, e.g. vMotion, as you have no access to the VMware management tools and you are not able to provision or change the virtual machines.

High availability headroom: Ensure that at least 30% of capacity is reserved for high availability.

What you will do

Templates and FTP server: You are not permitted to upload your own templates or use the FTP server.

Purchase of nodes: Purchase between 2 and 8 nodes, but all nodes must use the same variant (server model).

The available options of this component are shown below.

Description

Managed Hypervisor – Node with Windows (48 vCPUs, 96GB RAM)

Managed Hypervisor – Node without Windows (48 vCPUs, 96GB RAM)

Appendix: Components

Managed Load Balancer

What Claranet will do

Access to the Load Balancer: Access the Load Balancer to make any changes, as you do not have access to perform this task.

Number of changes: Make up to 5 changes to the Load Balancer configuration in a calendar month in accordance with your requirements. There will be a charge if the number of requested changes exceeds this number.

Load Balancer Algorithms: Implement one or more of the following Load Balancer algorithms, depending on your requirement:

Round Robin: new inbound traffic is routed to one of a list of servers on a rotating basis

Least Connections: number of active connections to the server is tracked and new inbound traffic is directed to the server with the least number of active connections

Hash: the source IP of a user is stored in an index table so that when an end-user returns at a later time, they are sent to the same sever each time. If a server becomes unavailable, the table is updated. 'Source IP' is the only supported hashing mechanism.

By default, Round Robin will always be used unless an alternative algorithm has been selected by the Solution Architect.

Failover: Configure failover, which removes a server node from the group automatically if the Load Balancer detects that the node is not reachable.



What you will do

Request for change: Make change requests through the change control process within Claranet Online and details of this can be found in the **Appendix: Help and Support**.

Adding a Load Balancer: If a Load Balancer is being added to an existing solution, you may be required to renumber your IP address ranges.

The shared load balancing cluster is 'local', meaning that traffic into a specific data centre can only be sent on to virtual servers in the same data centre. The load balancer can be used to balance any TCP or UDP port and is typically used for HTTP, HTTPS, FTP, SMTP and POP3 traffic. The originating IP is retained in all traffic, which means that web server logs will show the correct client source IP address, rather than causing all traffic to appear to originate from the load balancer.

Limitations

The following limitations apply to each virtual IP (VIP):

- 10-30 mbps throughput per virtual IP
- 400 new connections per second per virtual IP
- 800 concurrent connections per second per virtual IP

Whilst these limitations are not precise, in the event that they are exceeded, Claranet reserves the right to throttle throughput. If you regularly exceed these limitations, you should consider a dedicated load balancer. Use of a dedicated load balancer can be arranged as a bespoke solution upon request to your Account Manager, but is outside the scope of this Service, and is not described in this document.

Managed Backup

Where your solution includes a 'Managed Server' or 'Managed Hypervisor' it is mandatory to take the 'Managed Backup' service to enable Claranet to restore the server in the event of data corruption. The Managed Backup service can be taken with the Managed Self-Service Hypervisor as an option.

Managed Backup with Managed Server or Managed Hypervisor



What Claranet will do

Applicable to: Managed Server, Managed Hypervisor, Managed Web Service, Managed Role Server, Managed Database Server (please see separate Service Description).

Agent based: Install an agent into the Operating System to accommodate the backup process.

Initial backup: Take an initial backup in full and store a copy of all files that are held inside the Operating System.

Incremental backup: Once the initial backup is taken, further incremental backups take place within a fixed backup window, which runs from 9.00pm to 8.00am each night. The timing of this is random and determined by the backup server. Claranet does not offer fixed start or end times. The data stored are of files that have been added, changed or deleted.

Open files: Make four attempts to backup files that are 'open'. If the file remains open after four attempts, it will be skipped and will not be backed up. The platform should be considered that it **cannot** backup 'open' files.

Volume of backed up data: Only data is backed up and free space does not need to be included in the backup. Claranet assumes that there is an average of 50% across all of your volumes. If Claranet or you has reason to believe that the disk utilisation is too low (i.e. there is less free space available) then a manual quotation for backup must be produced. Claranet reserves the right to request that you purchase additional backup space to accommodate this.

Estimated data change: Estimates that the rate of change per day (data created, changed or deleted) is 5%. If Claranet or you has reason to believe that your data may change more, then a manual quotation for backup must be produced. Claranet reserves the right to request that you purchase additional backup space to accommodate this.

Setup and file selection: Perform all backups. Claranet will amend the backups accordingly if any changes are made to the servers.

Virtual machine snapshots: Take up to 12 snapshots of your virtual machine per annum.

Data retention: Retain data for 14 calendar days known as ‘the retention period’. If a file is present on Day 1 and is deleted on day 2, it will be permanently deleted on the backup on day 15 and cannot be restored after that time. The retention period cannot be changed.

Failed backup: Fully monitor the backup process. After every backup cycle, Claranet Service Desk are notified of any backup failures. If a backup failure is detected, Claranet will attempt to troubleshoot and fix the problem. If the problem persists, Claranet will contact you and will work with you to resolve the problem and resume normal backups. Backups may fail for a number of reasons:

- All virtual disks must be initialized
 - All VMs that require a backup must have a virtual SCSI controller present
 - Disks must not be using Independent Mode
 - Any mounted media was not dismounted before a backup is taken
 - Snapshots exist for a virtual machine
 - IP addresses on cloned servers have not been changed or removed (this is essential to make sure the live server is backed up and not the clone)
-

Server check before restores: Ensure that the server onto which data is to be restored to, is in an operational state so that files can be recovered onto it. Where this is not the case, the server will be re-built or re-configured to a point that is sufficient for the restore to be started.

File restores: Restore individual files or folders to a destination other than the original location.

Restoring data: Will perform restores on an “as needed” basis when a request has been received after you have raised a ticket through Claranet Online.

Limitations to restores: Restoring data files directly into an application e.g. Microsoft SQL will not be done. Instead, files will be restored on to the server and, in the case of Managed Database Service, Claranet would import data from the database. Claranet will not restore whole images of a server.

Number of restores: Perform two restores per server per month. Additional restores can be performed and Claranet reserve the right to charge for these.

Restore times: Have a target to initiate a restore within four working hours from the time that you initially request the recovery. The request can be made either inside or outside of working hours. The time taken to recover increases as the volume of data backed up increases. Other factors affecting the time to recover data include, but are not limited to, the type of data and the number of individual files to be restored. Claranet therefore cannot provide a guaranteed time to complete a recovery.



What you will do

Backup applications: You will not install any backup software or replication software onto the server because of the network traffic generated by performing a backup or transfer of the data.

Data encryption: You will obtain pre-approval for any requests to encrypt data. Additional charges may apply as encrypted data cannot be de-duplicated thereby increasing the backed up storage volume.

Contact details: You must ensure that Claranet has the correct contact details of the nominated person within your organisation to contact in the result of a backup failure.

Requesting restores: You can request a restore by raising a ticket through Claranet Online. You can request the restore of any daily backup taken during the retention period. Any data older than the retention period cannot be recovered. When requesting a restore, you will need to confirm the following information:

- The name and IP address of the server to recover from;
 - The data to be recovered (exact folder structure);
 - The desired date and time to recover back to (Claranet will select the nearest backup).
-

Restoring files: You are not permitted to invoke backups or file restores and the recovery of files can only be done by Claranet.

Failed backups: You will be required to take action when backups fail due to your applications or your managed third-party applications that are not supported by Claranet. If you are either unwilling or unable to take such action, then Claranet may be unable to resume backups. Additionally, Claranet cannot be held responsible for backups that fail if Claranet is denied electronic access to your servers by you which includes any modification or deletion of the backup agent and/or associated files. You will still be liable to pay the service fees whether backups are continuing to run successfully or not.

Managed Backup with Managed Self-Service Hypervisor

The Managed Backup service when used in conjunction with the Managed Self-Service Hypervisor is similar to when used with the Managed Server, but with the following differences:



What Claranet will do

Applicable to: All virtual machines on the Managed Self-Service Hypervisor service.

Agent based: No agent is installed and a snapshot of the virtual machine is taken once every 24 hours.

Initial backup: Take an initial backup in full and store a copy of the full VMware disk image. This taken using a VMware snapshot.

Incremental backup: Once the initial backup is taken, further incremental backups store just the data blocks in the virtual machine disk file that have changed since the last backup. The backup is not aware of individual files within the Operating System.

Limitations to the backups: The backup platform cannot be used to backup Microsoft SQL server, Microsoft Exchange or any other applications with “uncommitted” data. Data must be available in a format that can be backed up, e.g. exported by you from Microsoft SQL to a flat file.

Volume of backed up data: Back up 100% of the disk volume size, regardless of whether there is free space or not.

Estimated data change: Estimates that the rate of change per day (data created, changed or deleted) is 2%. If Claranet or you has reason to believe that your data may change more, then a manual quotation for backup must be produced. Claranet reserves the right to request that you purchase additional backup space to accommodate this.

Setup and file selection: Will wait until a request to back up a specific virtual machine has been received from you, before starting a backup. Virtual machines are not backed up by default. The backup platform does not detect the creation, change to or deletion of virtual machines. Backup changes will only be initiated upon receipt of a request from you and until the time that the backup platform is re-configured, no backups will be taken.

Virtual machine snapshots: Take up to 12 snapshots of your virtual machine per annum.

Data retention: retain data for 14 calendar days known as ‘the retention period’. If a file is present on Day 1 and is deleted on day 2, it will be permanently deleted on the backup on day 15 and cannot be restored after that time. The retention period cannot be changed.

Restoring data: Will restore a copy of the virtual machine disk image onto your datastore to restore the entire virtual machine. There must therefore be sufficient space available in that datastore to restore the entire virtual machine. Claranet will therefore not restore individual files or folders or re-configure the virtual machine.

What you will do

Contact details: You must ensure that Claranet has the correct contact details of the nominated person within your organisation to contact in the result of a backup failure.

Limitations to the backups: You are responsible for making any arrangements to ensure a copy of the data is available in a format that can be backed up e.g. exporting SQL server data to a flat file.

Configuring the backups: You are responsible for ensuring that a virtual machine is scheduled to be backed up. You must provide the Claranet Service desk with a list containing the display name and IP address of each virtual machine you wish to back up. Virtual machines are not, by default backed up. The backup platform does not detect the creation, change to, or deletion of virtual machines so you must make a request to change the backup. Until the backup platform has been re-configured, no backups will be taken. It may take several days from receipt of the list before the first full backup has been successfully taken. Claranet do not take any responsibility for not backing up virtual machines where the details submitted have been incorrect.

Managed SSL Certificates

The options for this service are shown in the table below. You may purchase any combination of these options and you are able to buy more than one of each of these. For example ‘Managed SSL Certificate - Basic’ could be purchased twice or more.

Description	Recommended Usage
Managed SSL Certificate - Basic	Any Web site, intranet, or extranet conducting low volume, or low money value secure online transactions. Includes £50,000 guarantee from certificate provider.
Managed SSL Certificate - Pro	Any Web site, intranet, or extranet conducting medium to high-volume or medium to high-money value online transactions. Includes £1 million guarantee from certificate provider.
Managed SSL Certificate - Wildcard	Any organisation that needs multiple SSL certificates from a single domain name. Includes £1 million guarantee from certificate provider. (Used to secure server1.ab.com, server2.ab.com, etc.)

Software Licences

What Claranet will do

Appropriate licences: Provide appropriate software licences for Operating Systems, databases and/or hypervisors wherever required. These licenses are the property of Claranet and provided to you as a part of the solution only. They are not to be replicated elsewhere.

What you will do

Independent Software Licences: You will provide licences for any software not provided by Claranet, and are solely responsible for the compliance of those software agreements.

The scope of this Service Description does not include the provision of licenses such as Microsoft Exchange or Microsoft Remote Desktop Services. These licenses may be

available as part of separate service offerings from Claranet and are detailed in their respective Service Descriptions.

Appendix: Roles

Managed Role Server

The Managed Role Server component is similar to the 'Managed Server', with a few differences:

What Claranet will do

Configuration management: Perform additional management activities to manage the configuration and uptime of the bespoke applications or server roles such as the Varnish Web Caching software.

Limitations to roles: Provide **alternative** services for the provision of certain roles. The following roles **cannot** be provided with the Managed Role Server:

- Microsoft Active Directory Domain Services (AD DS) role;
- Microsoft File and Storage Services role;
- Microsoft Print and Document Services role;
- Microsoft Remote Desktop Services (RDS) role

What you will do

Bespoke applications: You will agree with Claranet the bespoke applications and server roles with Claranet and these will be documented in the Statement of Works (SoW) and agreed in writing.

Access to the server: You do not have access to connect to the server, either to install software or to complete other tasks.

The available options of this component are shown below. You purchase one or more of the Managed Role Server options, each representing a single virtual server. Dedicated hardware is not included as part of this component.

Description

Managed Role Server (Shared Virtualised Host)

Managed Role Server (Dedicated Virtualised Host)

Managed Role Server (Dedicated Physical Host)

Managed Web Service

The Managed Web Service component is similar to the 'Managed Server', with a few differences:

What Claranet will do

Configuration management: Perform additional deployment and management activities to manage the configuration and uptime of the web engine and application framework software running on the server.

Web Server software support: Provide support for the following versions of web server software:

- Internet Information Server 7.5 running on Windows Server 2008 R2
- Internet Information Server 8.0 running on Windows Server 2012
- Internet Information Server 8.5 running on Windows Server 2012 R2
- Apache Web Server version 2.2.3 running on Red Hat Enterprise 5
- Apache Web Server version 2.2.15 running on Red Hat Enterprise 6
- Apache Web Server version 2.4.6 running on Red Hat Enterprise 7
- Apache Web Server version 2.4.x running on Ubuntu 14.04 LTS
- Nginx version 1.4.6 running on Ubuntu 14.04 LTS
- Nginx version 1.4.6 running on Red Hat Enterprise 7 (via SCL repositories)

Software and application framework support: This component also includes support only for the following software and application frameworks. As a general rule, Claranet will only support the two most recent stable versions of each of these features and where you do not wish for these to be updated, they will no longer be supported.

- ASP Classic
- ASP.NET / .NET
- Java
- PHP / Zend

- Ruby
- Perl
- Python
- Node.js

What you will do

Access to the server: You do not have admin access to the server, either to install software or to complete other tasks.

Testing of code: As you cannot publish code, directly to the web server, you must test code in a pre-production environment, package the code in an agreed format and then raise a ticket through the Change Control Process for Claranet to grant you access to publish the code. Testing should include testing of vendor supplied patches against production code prior to publishing the new content on the server. Service levels are suspended if untested code is released.

With regard to the In-life management activities of the Managed Web Service:

What Claranet will do

Activities undertaken under IIS admin:

- Create and delete web site objects in IIS
- Configure, enable, and disable logging
- Create additional user and/or FTP accounts
- Configure authentication
- Add, configure and remove supported Internet server API (ISAPI) filters
- Add, configure and remove supported Apache RPM modules
- Add and remove application mappings
- Add and remove application pools
- Set up redirection to another URL
- Change the default document
- Set content expiration
- Enable content ratings
- Change website identification (e.g. IP, port number, host header)
- Enable process throttling
- Create or change the location of virtual directories
- Change application-protection modes (i.e. in process, pooled, out of process)

- Redirect to a Universal Naming Convention (UNC) pathname)
- Application and application server restarts
- Security configuration changes

Should you require Claranet to deploy code on your behalf, this is a bespoke requirement and you should outline this requirement during the design. All code deployments will be performed by our Change team and processed on your behalf. To facilitate this there will be a requirement for pre-deployment testing of code on a staging or test server to ensure that any potential risks are evaluated and mitigated. All code deployments will either be performed by deployment tools or by a fully documented deployment process supplied by the your developers

The following are specific items that are not provided as part of the service and are therefore performed by you.

What you will do

Activities undertaken:

- Create and amend application code (HTML etc.)
- Test and perform quality assurance tasks on application code
- Resolution of issues related to the application code, where the Operating System, database and infrastructure are operating within normal parameters;
- Resolution of issues caused by errors in application code
- Speed or performance tuning

Configuration parameters

The following configuration parameters are applied.

Technology	Configuration parameters
Apache	<ul style="list-style-type: none"> Log files created by the web server will be rotated every 4 weeks. After 4 weeks log files will be purged from the system and will no longer be available to the Customer. Document root: /u01/www/<websitename>/htdocs Private web root: /u01/www/<websitename>/private Web logs: /u01/www/<websitename>/logs
IIS	Claranet will back up a copy of the IIS metabase with the nightly backup job. In the event of an issue, Claranet will restore the last good copy of the metabase.

The following items are monitored in addition to those defined in the 'Managed Server' component:

Microsoft Internet Information Services (IIS) Web Servers

Monitor name	Threshold	Frequency	Persistence	Severity
Availability IIS Service (Failed Service)	n/a	60s	5	Minor
Availability IIS Web site status (running)	!= 'Running'	60s	5	Minor
Performance IIS ASP Error Rate	Error Rate >= 1	60s	5	Warning
Performance IIS ASP Queue Length	Requests queued delta > 0	60s	5	Warning
Performance IIS Application Pool Status	!= 'Started'	60s	5	Warning

Apache web server (running on Linux server)

Monitor name	Threshold	Frequency	Persistence	Severity
Availability HTTP/HTTPS port listening	n/a	60s	5	Minor
Availability Apache Service Down	n/a	60s	5	Minor

The available options of this component are shown below. As with the 'Managed Server' component, there are three types: Shared Virtualised Host, Dedicated Virtualised Host and Dedicated Physical Host. You purchase one or more of each of the Managed Web Service options, each representing a single virtual server. Dedicated hardware is not included as part of this component.

For each 'Managed Web Service' option, quantities of both of the RAM and CPU core variants are added. The quantity of these options can be any number, with a minimum quantity of one for both.

Description
Managed Web Service (Shared Virtualised Host) – Windows
Managed Web Service (Shared Virtualised Host) – Linux
Managed Web Service (Dedicated Virtualised Host) – Windows
Managed Web Service (Dedicated Virtualised Host) – Linux
Managed Web Service (Dedicated Physical Host) – Windows
Managed Web Service (Dedicated Physical Host) – Linux

Building your Managed Web Service

Table: Build task list for each Managed Web Service – *In addition to the Managed Server*

Tasks

For Internet Information Services (IIS)

- Create virtual directories
- Create default web site with the provided domain name
- Create relevant directories/containers for Customer code
- Setup SSL certificates where required
- Create one FTP account for use for IIS servers
- Create application pools
- Create virtual hosts
- Remove any sample code
- Install application frameworks
- Installation and configuration of supported ISAPI Extensions for IIS
- Creation and configuration of any required database connectors
- Creation and configuration of session replication
- Copy Customer web code onto web server
- Enable FTP to allow Customer to upload data
- Setup bespoke URL and/or transaction monitoring

For Apache Web Server

- Installation of Apache and appropriate modules
- Creation of one SSH account to SCP (Secure Copy) content to web servers

Tasks

- Add and remove supported Apache modules
- Creation of security permissions
- Configure SSL certificates
- Copy Customer web code onto web server
- Enable FTP to allow Customer to upload data
- Setup bespoke URL and/or transaction monitoring

Managed URL Testing

What Claranet will do

Monitor Individual URLs: Monitor individual URLs to ensure that a website is available for servers that are hosted in Claranet datacentres.

Generation of an alert: Check that the correct HTTP response code (200) is received from the web server. If any other code is received, Claranet will generate a critical alert and an event is generated.

Content level inspection: Provide content-level inspection for web-sites. The URL testing platform effectively performs synthetic (fake) transactions that simulate a real user performing a task such as doing a search for a specific product on a retail website. This is available only for sites that are available on the Internet. This cannot be used to monitor sites located on private networks. These synthetic transactions are always performed using Internet connectivity not provided by Claranet to provide the most realistic simulation of end-user experience. You engineer web code that returns a single string that indicates the success of a transaction. The system will look for this string on the web page being monitored. If this string is not present, or an error is generated, a critical alert will be generated.

Issues detected: Perform monitoring to detect any of the following issues for one or more jobs, each with up to three URLs for sub-transactions such as transitions between pages.

- All sub transaction within a job must reference the same single web site. Combining two or more jobs to obtain more than 3 transactions is not a supported configuration.
- Missing content on the site (string is not returned as expected)
- Slow response times (as defined by you and Solution Architect, and must be the same for all sub-transactions)

Completing the job: Each job will run every five minutes to complete all defined transactions. If there is an issue in completing a job, the job will re-run in its next scheduled slot. If a sub-transaction fails, it will be retried two times before generating an alert. The retries will be three seconds apart.

Pop Up Windows: URL testing cannot be used with web sites that use pop-up windows as part of the functionality being monitored or that use Macromedia Flash.

Home page redirection: As the Service will not support HTTP redirection from the home page (which returns an error code of 302), Claranet will configure the URL monitor with the URL of the page that redirection would send the browser to.

Enabling web server error handling: Enable the web server error handling on the web server. All web servers configured by Claranet will have this turned on by default.



What you will do

Web code: You will engineer web code that returns a single string that indicates the success of a transaction. The system will look for this string on the web page being monitored. If this string is not present, or an error is generated, a critical alert will be generated.

URL provision: You will provide the URL at which each string will be generated, as Claranet are not involved in the management of the web code or functionality. You must also provide any test information required for form submission (i.e. information that will be appended to the requested URL) including any credit card numbers required for e-commerce functionality.

Pop Up Windows: You accept that, as web technology evolves, new technologies may emerge that you wish to use which cannot be monitored using this component.

Automated redirection: Where your code uses automated redirection for HTTP error codes or non-standard HTTP error codes, you must notify Claranet so the monitoring can be adjusted accordingly.

Material changes to the web code: You must notify Claranet of any material changes to the web code in advance as Claranet will need to manually change the platform.

Web analytics configuration: You are advised to configure any web analytics solution to exclude IP ranges used by Claranet for transaction monitoring, as all URL monitoring will originate from this range of addresses and this could create misleading analytics data.

HTTP Error Codes

400Bad Request	408Request Timeout	416Requested Range
----------------	--------------------	--------------------

HTTP Error Codes

401Unauthorized	409Conflict	417Expectation Failed Not Satisfiable
402Payment Required	410Gone	500Internal Server Error
403Forbidden	411Length Required	501Not Supported
404Not Found	412Precondition Failed	502Bad Gateway
405Bad Method	413Request Entity Too Large	503Service Unavailable
406None Acceptable	414Request-URI Too Long	504Gateway Timeout
407Proxy Authentication Required	415Unsupported Media Type	505HTTP Version Not Supported

The available options of this component are shown below, with each variant representing one transaction. You are able to buy more than one.

Description

Monitored Synthetic Transaction Test

Appendix: Storage

Managed Storage

Differences between the three storage tiers, Performance, Standard and Bulk, can be seen in the table below.

Tier Classification	Available IOPS Per GB*	Expected Latency (m/s)**
Performance	4	< 2
Standard	1	10 - 15
Bulk	0.06	30

*Indicative IOPS based on a 16KB block size with 50/50 read/write profile. Please note this is a random workload

**Expected latency is an indicative figure only

Managed Storage volumes are measured in useable GB (i.e. the amount of data available after any disk resilience has been applied but before the storage has been formatted by one or more Operating Systems). For example, if you purchase a total of 100GB 'Standard' tier storage and you have two virtual machines with 50GB each, the free space on each virtual machine will be smaller than 50GB because of space lost to the overhead of the Operating System file system.



What Claranet will do

Control of the functionality: Functionality of the storage device, such as replication or snapshotting, is not accessible to the Customer.

Thin provisioning: Use thin-provisioning (a storage technology where space is only allocated as it is required). This is transparent to any server / virtual machine operating system.

Fair usage: Operate a fair use policy, which is used to prevent performance being degraded by prolonged, sustained high demand caused by an individual host or server.

Limiting of the storage I/O: Reserves the right to limit the storage I/O throughput for any individual host or server which is adversely affecting the performance of a Virtual Volume Set (VVSet).

Performance expectations: Provide advice where you are expected to require performance that is significantly different to the guidelines listed in the tier classification table. The advice could be to consider dedicated infrastructure.

OS De-duplication: Claranet does not allow OS de-duplication to be run.

Compression and Encryption: The service does not support mass compression or encryption.

The Managed Hosting service contains two storage variants: **Managed IaaS storage** which is designed for Self-Service Hypervisor or any dedicated compute offerings; and **Managed Server Storage** which provides storage for all types of managed servers.

Managed IaaS storage

Managed IaaS Storage is implemented using a Virtual Volume Set (VVSET) bound to a single hypervisor cluster, or in some cases a single host.

Only volumes of the same tier can reside in a VVSET. This means a single customer may have one or more VVSET for Bulk, Standard and Performance.

The IO size has an impact on the overall performance of the array (the smaller the block size, the better the performance). We therefore recommend that all platforms be configured so that anything above a 128KB IO Size be split into multiple 128KB transactions. This can easily be enforced using VM IO Limits on the ESX hosts. This is to limit the performance impact of a single VM on a cluster.

There is a size limit of 2TiB per volume. Additionally, in order to protect the performance of the storage volumes on the array, and to ensure all customers receive the requisite performance tier; Claranet have limited the contention on the network. For this reason, each host is limited to a maximum of 2x1GB fibre channel connections

Managed Server Storage

Managed Server Storage also utilises Virtual Volume Sets (VVSets) for the requested tier(s) of storage.

Performance thresholds will be set by drive within the managed server. This will allow a mix of storage performance on the same managed server. These thresholds will be managed by the IO limits within the datastore. Claranet will carve out containers of storage at different tiers and the appropriate drive will be associated with the required tier of performance. Within the VVSet there will be one or more LUNs, or datastores. Each datastore will hold one or more VMDK files (virtual disks).

The size of an IO transaction as well as the amount of IO generated can have a significant impact on performance for the customer and the overall storage solution. For this reason Claranet has implemented three additional measures within the managed virtual server environment to help protect customer experience.



What Claranet will do

Limit to the base amount of IO: Limit the base amount of IO that a single managed server can generate to 3500 IO. This is to limit the potential damage that a single managed virtual server can do to the available hosts bandwidth.

Splitting large transactions into multiple transactions: Set the virtualization host (i.e. VMware ESX) to split any transactions with a larger IO size than 128KB into multiple 128KB transactions. Claranet feels this this size provides the best combination of storage array performance and network utilisation for traffic requiring higher bandwidth rather than allowing much larger IO sizes which the array is not optimised to handle. The 3PAR arrays work best with a <16K IO size.

VM IO limits are specified against each VMDK disk: This stops any given VMDK from consuming all the IO resource available to the VMFS datastore hosting it. However, it also adds an IO cost to larger IO sizes generated within the virtual machines Operating System as per the following chart.

IO Size (K)	IO Cost
0 - 31	1
32 – 63	2
64 – 95	3

IO Size (K)	IO Cost
96 – 127	4
128 – 159	5
160 – 191	6
192 – 223	7
224 – 255	8
256 – 287	9

Appendix: Support

Help and Support

Change Control Process

Claranet’s Change Management team are responsible for requests relating to any product and service configuration changes you wish to make. The team specialise in configuration and follow strict processes and ensuring that the changes are authorised. The Change Management team are also responsible for Claranet’s Change Advisory Board (CAB), which discusses and approves changes raised internally. To make a change request, see the section below on “Raising a support ticket”.

Raising a support ticket and a Request For Change (RFC)

Claranet provides two ways for your approved contacts to raise, track and update standard support tickets; through Claranet Online and by telephone. For security and audit reasons, you are required to make all requests for change through the customer portal and only

portal users with the correct privileges can request a change. You will only see your services listed so please select the service relating to the request for change. In the event that the customer portal is unavailable, please contact Claranet by telephone, where an emergency procedure will be in place to log change requests on your behalf. Request for changes will not be accepted through this number at any other time.

What Claranet will do

Through Claranet Online: Support tickets raised through Claranet Online are assigned to the appropriate support team based on the service you need the support for. You will only see your services listed so please select the service relating to the incident or to the service request. The response time will start from as soon as your ticket has been submitted.

By telephone: It is not always convenient to raise support tickets through the portal and therefore you may choose to use the telephone instead. When choosing to raise a support ticket using the telephone you must provide proof of identity following Claranet's standard security procedure. The response time will start from as soon as your telephone call has ended.

Escalating a ticket

In the event that you need to escalate a ticket, Claranet is ready and available to help you quickly bring your issue to closure. Within each level of the escalation path the person you speak with is responsible for evaluating your situation, facilitating the resolution plan and acting as your sponsor. The benefits of the escalation procedure are:

- ITIL accredited staff owning your escalation
- A focus on service recovery
- Improved communication
- Consistent process

An escalation may be initiated when, after working through our standard support processes and with our teams, you are not satisfied with the level or timeliness of the service you have received. Additionally, an escalation should be initiated when there is tangible impact to your production environment, or there is high risk to your business operations.

What Claranet will do

Escalation Manager: Assign an Escalation Manager who will deal with your escalation and collaborate with you to develop a communication plan. A technical plan of action may be needed to ensure resolution of a technical issue. Your Escalation Manager works as your advocate internally and will become a virtual member of your own problem resolution team. Should you feel dissatisfied with the escalation process, please contact your Account Manager directly.

Service Delivery – Fix levels and response times

The circumstances where a fix service level is deemed to be met are:

- When the service has been fixed within the standard and expected response time
- Where you receive a telephone call (within the service level response time) resulting in a fix over the telephone
- Where you receive a telephone call and you defer the visit of an engineer to a specific time, the fix time is measured from the specific time you specify
- When a part which can be fitted by you arrives on site
- Where it is subsequently discovered that the issue giving rise to the telephone call falls outside the Services agreed to be provided by Claranet
- When the equipment has been returned to an acceptable operational status or an item of loan equipment has been supplied
- Where the fault relates to an excepted Service

What you will do

Efforts to resolve an issue: You are responsible for providing reasonable efforts support and information to Claranet to help in the resolution of any technical issues.

Service outage: In the event of a Service outage, you are responsible for complying as quickly as possible with any requests from Claranet for help with diagnostics. Any delay in resolving the fault due to you not being available or not complying with Claranet's requests may impact the validity of any Service Levels.

Table: Service Level Response Times

Priority	Service Level Response	Description
1 – Critical	Within 1 hour	Total service is unavailable
2 – Major	Within 2 hours	Partial service, an element of the total service has failed
3 – Minor	Within 4 hours	Impaired service, no element has totally failed but there is a quality issue
4 – Request	Within 1 Business Day	The service is unaffected. Request for product related technical advice or configuration change
5 – Question	Within 1 Business Day	General information and feature questions related to the Service

Service Levels

If Claranet fails to deliver the stated service level, Claranet agrees that you shall be entitled to receive, in lieu of all other remedies available to you, Service Credits as set forth in this section against the fees owing to Claranet under the Agreement.

Measure of availability

Any time in which the Claranet monitoring system is unable to receive or process monitoring data shall not be assumed to be unscheduled downtime. If you initiate a Service Credit request, this will put into a process where Claranet coalesce the systems monitoring data and logs with your own record of when and where an outage occurred. The Service Credits will be available for that agreed window. You have the option to dispute records with Claranet, where upon systems monitoring data can be provided to you.

Table: Technical Metrics –Availability showing expected service level availability

Component	Source of availability data	Unscheduled downtime identified by	Exceptions	Service level
Managed Technical Design				No service level offered
Managed Build				No service level offered
Managed Load Balancer	Connectivity Ping test from Claranet monitoring platform sent every two minutes	Every ping test that does not receive a response = 2 minutes of downtime Alert is triggered after 3 consecutive, unsuccessful tests	Monitoring is disabled during maintenance window	99.9% availability = Downtime < 43 minutes per month
Managed Switching				No service level offered
Managed SSL Certificates				No service level offered
	Availability Alert raised by VMware monitoring that datastore has become unavailable to a host			
	OR			
Managed Storage and Backup	Alert raised by storage device that one or more volumes has gone 'offline'	Time between alert opened and alert closed = downtime	Alert is disabled during maintenance window	99.9% availability = Downtime < 43 minutes per month
	OR			
	Alert raised by backup platform, during backup window, that storage used to store backup data is 'offline'			

Managed Self-Service Hypervisor	Availability Alert raised by VMware vCenter showing two or more nodes are unavailable	Time between alert opened and alert closed = downtime	Alert is disabled during maintenance window	99.9% availability = Downtime < 43 minutes per month
Managed Hypervisor	Availability Alert raised by VMware vCenter showing two or more nodes are unavailable	Time between alert opened and alert closed = downtime	Alert is disabled during maintenance window	99.9% availability = Downtime < 43 minutes per month
Managed Server All variants	Connectivity Connectivity test from Claranet monitoring platform sent to agent on server every two minutes	Every test that does not receive a response = 2 minute of downtime	Tests are disabled during maintenance window	99.5% availability = Downtime < 216 minutes per month
Managed Role Server All variants		Alert is triggered after 3 consecutive, unsuccessful tests		
Managed Web Service All variants				
Managed URL Test	Connectivity Transaction test, performed every five minutes, generates an error	Each failed test = 5 minutes of downtime	Tests are disabled during maintenance window	99.5% availability = Downtime < 216 minutes per month

In the event that you and Claranet agree that Claranet has failed to meet any service level guarantee during any given calendar month, Claranet will credit your account with a Service Credit. Service Credits shall apply only to the fee(s) for the affected service(s). Service Credits shall be deducted from the relevant monthly fee due in respect of the second month following the month in which an agreed Service Credit is claimed. The maximum amount of Service Credit a Customer can receive in each calendar month relating to this agreement is fixed to 50% of the fee for the affected Service. The Service Credits issued are liquidated damages and, unless otherwise provided in this agreement, such Service Credits will constitute your sole and exclusive remedy with respect to the failure for which they are payable.

Service availability guarantee

If Claranet fails to meet the availability guarantee, Service Credits will be paid according to Table 2 below. Only one credit may be selected and the credits are not cumulative. For example:

- If a component has an availability SLA of 99.5%; and
- percentage Service availability in the calendar month was 96.0%; then
- the percentage credit for “Less than 97.0%” is selected (15%).

Table: Service availability commitments

For components where the service level is 99.5%

Percentage service availability per calendar month	Percentage credit of monthly charge for the variant, for the calendar month in which non-availability occurs
Equal to or greater than 99.5%	No credit
Less than 99.5%	5%
Less than 97.0%	15%
Less than 95.0%	40%

For components where the service level is 99.9%

Percentage service availability per calendar month	Percentage credit of monthly charge for the variant, for the calendar month in which non-availability occurs
Equal to or greater than 99.9%	No credit
Less than 99.9%	10%
Less than 97.0%	30%
Less than 95.0%	60%

Compensation claims

Compensation claims must be submitted, in writing (email or letter), within 30 days from the service level guarantee breach to which they refer. All claims must be submitted to the appointed Account Manager and/or Service Manager. You agree to correct problems and to attempt to minimise the recurrence of problems for which you are responsible that may prevent Claranet from meeting the service level guarantees. Requests for support received by the Service Desk by means other than telephone or request ticket (for example, by fax) will be excluded when calculating service levels.

Exceptions

Claranet excludes responsibility for meeting any service levels to the extent that meeting the service levels is affected by the following items:

- if you are in default under the Agreement;
- in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
- in the event that the Service is disrupted due to unauthorised users or hackers;
- in the event that the Service is unavailable due to changes initiated by you whether implemented by you or Claranet on behalf of a customer;
- in the event that the Service is unavailable as a result of you exceeding system capacity;
- in the event that the Service is unavailable due to viruses;
- in the event that the Service is unavailable due to the your failure to adhere to Claranet's implementation, support processes and procedures;
- in the event that the Service is unavailable due to the acts or omissions of you, your employees, agents, third party contractors or vendors or anyone gaining access to Claranet's network, control panel; or to your website at the request of a customer;
- in the event that the Service is unavailable due a Force Majeure Event;

- in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
- in the event that the Service is unavailable due to any event or situation not wholly within the control of Claranet;
- in the event that the service is unavailable due to your negligence or wilful misconduct of you or others authorised by you to use the Services provided by Claranet;
- in the event that the service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by you;
- in the event that the service is unavailable due to any failure local access facilities provided by you; and
- in the event that the service is unavailable due to any failures that cannot be corrected because the you are inaccessible or because Claranet personnel are unable to access your relevant sites. It is your responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing the technical contact details.

Exceptions specific to Managed Hosting

Claranet service levels will not apply during any period in which access to the services is prevented due to the failure or incorrect operation of telecommunications services connecting the edge device(s) of your information technology network (whether comprising your equipment or otherwise) to the edge device(s) of the information technology network from which we provide services.

Claranet cannot control the flow of data to or from our network and other portions of the Internet. Accordingly Claranet disclaim any and all liability resulting from or related to such event including but not limited to delayed delivery, non-delivery or misrouting of e-mail.

Cancellation of service



What Claranet will do

Equipment storage costs: You must remove equipment on or before the cancellation date. If your equipment remains within the facility after the cancellation date, then Claranet will turn off the equipment and charge for the storage of the equipment at the applicable daily rate and pro-rata. If your equipment is not collected by yourself within 3 months, Claranet will assume ownership over your equipment. Any costs associated with the disposal of such equipment will be re-charged to you.

Decommissioning the service: Uses management software to perform deletion of data on disk. As physical disks used in shared storage devices are securely shared between Customers, they are not physically destroyed but rather the relevant data is deleted. Claranet do not overwrite each individual bit of data on the disk (which is known as 'zeroing' the data). Instead, each individual bit on the physical disk will be overwritten randomly over time by new data