

The background features several large, 3D-style geometric shapes. On the left, a large teal shape is partially visible. In the center, there's a purple shape and a lime green shape. On the right, another teal shape is visible. These shapes are layered and have soft shadows, giving them a three-dimensional appearance.

C I V I C

knows

***Linux Managed
Hosting
Definition***

Contents

- Service Overview.....3
- Virtual Machine Hosting.....4
- Hosting Environment.....4
 - Datacentre.....5
 - Networking Bandwidth and Connectivity.....5
 - Network Security.....6
 - Backup and Recovery.....6
 - Operating System Maintenance and Security.....7
 - Systems and Performance Monitoring & Diagnostics.....7
 - Availability.....7
- Accreditations.....7
 - ISO9001.....7
 - ISO27001.....7
 - DCI Cyber Essentials.....8
 - ISO20000.....8
- Helpdesk Support.....8
- Contact.....10



Service Overview

Virtual Machines (Infrastructure as a Service) deployed, hosted and optionally managed on highly secure, high-availability hardware suitable for private or public services implementing web applications or other networking technologies. All solutions are treated as bespoke solutions, with the service moulded around user requirements, not vice versa. CIVIC can advise clients on how to best meet their needs and can help with (or entirely take over) the day-to-day running of the machine and its services.

Hosting is in a UK datacentre run by UK companies. CIVIC is certified to ISO-9001, ISO-27001 and Cyber Essentials Security standards and have years of experience working with the Public Sector.

The main features of the service are:

- Offerings for single server VM solutions to dedicated, load balanced VM clusters.
- Performance and sizing options tailored to your requirements
- Fully Managed service with consultancy and support.
- Bespoke solutions to custom requirements.
- Uses KVM open source technology
- Thinner LAMP containers also deployed on demand. These can be fully managed by CIVIC.
- Full computer emulation available using QEmu for special requirements.
- Server resources are not over-committed, leading to low contention.
- UK-based company.
- Highly secure UK data centre.
- All physical systems are in the UK.
- ISO 27001, ISO 9001 and Cyber Essentials Security-certified processes.
- Separate, fully managed highly available email and DNS services are available.
- Consultancy and expert support available for all levels, from networking to software frameworks.
- Backups of data included, with up to 90 days of backup retention.
- All backups are encrypted.
- Doubly encrypted backups available on request.
- Off-site backup storage.
- Off-site Cloud backup archival available on request. (archival backups are also doubly-encrypted)
- Linux, Unix VMs.
- Multi-tier firewalling with VPNs.
- Access strictly via cryptographically enabled protocols.
- Resilient internet connections with high availability firewalls
- DDoS mitigation.
- All storage is redundant with high availability options.
- Typical availability exceeds 99.9%

- 24x7 systems diagnostics and monitoring.
- Experienced in working with the Public Sector.
- In-house experts with decades of experience in security, Linux, Unix, open source, networking, and web technologies.
-

Virtual Machine Hosting

CIVIC use industry-standard open source KVM hypervisor or VMWare software for virtualisation, with full system emulation available for special needs. We can install Linux, Unix and Windows Virtual Machines from scratch, or deploy a client's existing machines from disk images.

Virtual Machines may be client-managed, fully managed by CIVIC, or any suitable arrangement in between.

We can also offer additional services pertaining to the operation of virtual machines such as:

- Fully Managed DNS;
- Fully Managed Firewalling configuration;
- Fully Managed Mail Transport Agents (MTAs) for email handling;
- Provision and renewal of cryptographic certificates;
- Virtual Private Networks for remote access; etc.

Depending on client requirements, these additional services can significantly reduce the system requirements and thus the operating cost of a Virtual Machine. Many services, such as backups and network security are provided as standard.

Resources on the hypervisor are typically not over-committed, leading to higher performance.

For simpler requirements such as websites, it is also possible to deploy thinner virtual server containers running industry-standard Debian GNU/Linux. This is suitable for (among others) Linux, Apache, MySQL and PHP (LAMP) configurations. Such containers are bare-metal, providing very high performance.

Hosting is on a variety of industry-standard servers running Debian GNU/Linux, built for redundancy and high availability using redundant power supplies and redundant storage. High availability options for hypervisors and storage are available.

Hosting Environment

CIVIC's hosted solution runs on industry standard platforms with a strong preference for secure, open, peer-reviewed technologies. This provides a robust and reliable platform, which easily scales to support any increase in terms of users and data. This provides an industry standard solution without the 'big ticket' costs normally associated with such an infrastructure.

CIVIC hosts its service with a recognised hosting service company; Iomart at the Pulsant datacentre in Edinburgh. This enables CIVIC to offer a high level of service, which meets our customers for their business critical applications. Benefits of this service include:

- Operational management, monitoring and backup procedures.

- Physical security, resilience, availability and security of the network.
- High bandwidth.
- Service Level Agreement for network uptime, service response time, support and cover in and out office hours.

Datacentre

Pulsant provides over 44,000 square feet of high security collocation space, coupled with office accommodation and secure storage areas for documents, equipment and data. A purpose designed facility to cater for the hosting of complex technology environments; Pulsant's facility includes redundancy on all components from connections to the Internet, power supplies, to switching and routing equipment. There are no single points of failure within the facility. Fault tolerance, resilience and failover capabilities are key to Pulsant's facility, and the following section describes these.

Physical Security

Pulsant's entire site is monitored by a state-of-the-art CCTV system, both internally and externally, which consists of sixteen cameras with PIR motion detector units operating at 1Hz refresh rate on a unique network which is monitored 24x365. Programmed smartcard access strictly limits and monitors personnel movement within the building. Smartcards are tailored to the client's pre-existing integrated security policy; facility and customer rack keys are scrupulously managed by Pulsant Security, ensuring that they are not taken out with the facility; and during global security issues, a Prevailing Security Status procedure is put in place. Access to the facility may only be granted to authorised client personnel by prior arrangement only.

Environmental Control

Pulsant's fully quintuply-redundant (5x) air-handling units provide the data centre floors with a constant fresh airflow: 22.5°C (±2.5°C). The airflow is pushed into the under-floor void, drawn up through the racks, and returned to the system through the ceiling void. The AHUs automatically vary the air temperature in order to match power dissipation.

Facilities Management Systems

Pulsant's facility management systems ensure a robust data centre environment at all times, and include a Raychem Fluid Detection System, VESDA Smoke Detection Systems, and a Wormald Fine Mist Suppression System. CO2 and EB3 extinguishers are placed strategically throughout the building, and all office spaces are monitored by a domestic smoke detection system.

Power Supplies

Scottish Power supplies Pulsant's facility with power requirements. Pulsant's facility is power rich; dual independent 11kV feeds, backed up by dual battery string Chloride UPS systems and Cummins 1.4MW and 850kW diesel generator sets which are tested on a monthly basis. CIVIC are supplied with diverse 16A power strips in two power channels. Self-managed, doubly redundant (2x), remotely-accessible Power Distribution Units are connected to these channels, driving CIVIC's redundant server power supplies. Pulsant's fully redundant power system is capable of delivering the highest uptime, which is 100% to date.

Networking Bandwidth and Connectivity

CIVIC use quadruply redundant (4x), bandwidth suppliers for redundancy, allowing for a greater resilience. If any of these four suppliers fail, then the others continue to service client equipment and sites as normal without any disruption to the service. Civic impose no limit on the available bandwidth.

We operate on a self-managed industry-standard switching fabric designed for redundancy, includ-

ing warm-standby spares. The switches are purposefully under-committed to reduce strain on the switching backplanes and to allow leeway for various recovery scenarios.

A group of high-availability, redundant load balancers is available for clients operating multiple servers. The load balancers can direct website traffic to the least busy server and automatically remove from the roster unavailable servers. CIVIC work with clients to carefully configure and tune load balancing to client requirements.

Network Security

CIVIC utilise an upstream, high-bandwidth Distributed Denial of Service (DDoS) attack mitigation system that can recognise and block attacks at rates orders of magnitude higher than our normally available bandwidth. The mitigation system is able to distinguish between legitimate access and access matching the attack pattern and returns the system to normal service within seconds after an attack starts.

CIVIC employ redundant, high-availability perimeter firewalls supplemented by internal firewalls at key points, including on hardware and virtual servers. The perimeter firewalls can enforce geographic restrictions to sensitive connections, limiting what parts of the planet can attempt connections of certain types. This is habitually done for CIVIC staff access. The firewalls also employ automatic blocking of sources of repeated unauthorised access attempts. We work with our clients to fine-tune firewalling to find the optimum point on the security-usability curve.

CIVIC's security policy stipulates encryption on all communications from the Internet, unless impossible to do otherwise (e.g., HTTP, DNS and certain email exchanges). Staff access is strictly through duly authenticated, encrypted Virtual Private Networks (VPNs), with further encrypted communications routed over the VPN links for additional security. This applies to CIVIC offices as well.

A segregation policy is employed using the IEEE 802.1Q protocol at the switching level, such that sensitive equipment is inaccessible from other equipment. This is often extended to cover client requirements for additional security. Additionally, management ports for highly sensitive networking equipment such as switches, PDUs and server lights-out management is physically segregated from other networks using separate wiring and switches.

CIVIC employs strict ISO 27001 compliant security policies reviewed regularly.

Backup and Recovery

Complete system backups are taken on a daily basis and backup tapes are stored in a secure location. Backups run automatically. Backup processes are accompanied by appropriate Backup Logs to indicate the success or failure of each process within the backup, giving a meaningful description of the reason for any failure. Should a failure take place, steps are taken immediately to rectify the issue before then next backup.

Backup retention is up to 90 days (unless uploaded to Glacier, in which case retention is essentially permanent). All backup storage is encrypted using peer-reviewed, strong, open encryption algorithms. Sensitive client backups are further encrypted at the source and during transport, making backups doubly-encrypted.

We can also store backups on the Amazon Glacier archival platform, if this is compatible with the client's security policy. Backups are further encrypted before uploaded using local encryption opaque to Amazon.

In the event of a system failure the latest backup is used to recover the system. Every attempt will be made to restore the system within 24 hours unless it involves a hardware failure that cannot be re-

stored within that time frame.

Backups are regularly restored to spot-check media quality and processes, as per our ISO 27001 backup policies.

Operating System Maintenance and Security

Software and firmware on all network infrastructure equipment and servers is kept up-to-date via regular updates. Available online blacklist resources are also updated regularly to permanently block hijacked network blocks, malware and common sources of attacks. Additional security checks and penetration testing is performed regularly.

The operating system and database software on the main server are also kept up to date keeping up with the manufacturer's recommendations. Additional security checks and penetration testing are performed regularly. Intrusion detection systems are in operation.

Systems and Performance Monitoring & Diagnostics

All aspects of CIVIC's infrastructure are instrumented via SNMP, monitoring systems and software agents running on servers to monitor performance and to detect and respond to potential issues. Monitoring is 24x7. For websites, we also employ off-site monitoring services an additional level of redundancy and safety. Issues are communicated to CIVIC staff on call via:

- Mobile Phone text messages (SMS);
- Multiple Internet Messaging (IM) services;
- Twitter Direct Messages (DMs); and
- Email.

Clients' staff on call may also be plugged into the monitoring systems for additional peace of mind.

Availability

Notwithstanding unexpected hardware failure, CIVIC guarantee uptime of 99.9%.

Accreditations

ISO9001

CIVIC have been audited for ISO9001 for our project delivery processes, which support the Account Management, Monitoring and Reporting processes and have recently successfully passed an interim audit which qualifies CIVIC for the most up to date revision ISO9001:2008. Using our ISO9001 accredited Account Management methodology and support mechanism, we have a track record of continuous improvement and delivery.

Over the last fifteen years we have developed a number of systems ranging from simple online shops to full blown e-procurement systems for multinational companies. Our ability to understand the user requirements allows us to deliver a solution that is tailored to meet the needs of our customers, giving them a competitive business advantage.

ISO27001

Our ISO27001 accreditation comes an independent and internationally accepted quality assurance hallmark that acknowledges the significant importance we place on safeguarding all of our clients' assets. Our Information Security Policy applies to all business functions within the scope of the Information Security Management System (ISMS) which is controlled and audited through ISO27001 and covers the information, information systems, networks, physical environment and people supporting these business functions.

DCI Cyber Essentials

CIVIC has been awarded the Cyber Essentials Certification, which is backed by the Government and launched in close consultation with the industry, Cyber Essentials was developed as part of the UK's National Cyber Security Programme.

ISO20000

We are in the process of gaining this accreditation.

Helpdesk Support

The CIVIC Helpdesk is available from 09:00 to 17:00, Monday to Friday, excluding weekends and public holidays. Users can log issues with the helpdesk by phone, by email or using our issue tracking system (access available on request).

CIVIC employ experts in all aspects of running a networked service, from hardware to the day-to-day operation of Content Management Systems and our hands-on approach to solving issues often helps solve unusual problems and meet unique client requirements.

Response Times

Priority	Response Target	Resolution Target	Examples
1	0.5 working hour	1 working hours	Unavailability of the entire system
2	2 working hours	4 working hours	Unavailability of a key module or major function, causing significant business impact.
3	0.5 working day	5 working days	Problems causing inconvenience, minor disruption or restricting performance.
4	1 working day	As agreed	Non urgent problems causing slight irritation but where workarounds are available; cosmetic or general enquiries for information

Reporting

- **Trouble tickets:** Trouble tickets will be recorded in our issue tracker (<http://issues.civiccomputing.com>). Each ticket has a unique ID enabling you to find the ticket and review activity on the thread. Our system enables you to maintain a dashboard of your own tickets and filter them by component for a quick view on what's outstanding, resolved, awaiting QA or on hold. You'll also be CC'd by email on any ticket updates.
- **Server activity:** CIVIC's server monitoring software will create monthly reports on the availability and performance of applications and services. Exceptions and resolutions will be documented in our issue tracker.

Contact

CIVIC

12 South Charlotte Street
Edinburgh
EH2 4AX
T: 0131 624 9830
E: info@civicuk.com

www.civicuk.com
Registered in Scotland SC221925
VAT Registration No 774906100
CIVIC Computing Ltd

