Access UK Ltd

Data centre Security

Date:	12th January 2017
Version:	1.1
Authors:	Tracy Wiseman/ Rob Parkinson / Daniel Gould

consulting | software | solutions
www.theaccessgroup.com

Table of Contents

Introduction

Access provides management of the hosting environment up to and including the application infrastructure layer. This includes all hardware, VMWare hypervisor software, storage, operating systems, SQL Database Servers, IIS Web Servers and RDS Servers.

Two datacentres run in an Active-Active mode, all services run within the primary active datacentre and can be failed over to the active secondary datacentre automatically. This gives an enterprise level of resiliency which is far in excess of the traditional cold standby disaster recovery datacentre.

Access are registered with the Information Commissioners Office; Z5042164

We are UKAS certified ISO27001:2013, the scope of which encompasses every office and the certificate Scope of Registration is "The Information Security Management system in relation to hosting, payroll services, software development, client data and infrastructure related to the organisation's software products in accordance with the statement of applicability (Appendix A)

Our Certifications

- ISO 27001:2013 (UKAS)
- ISO9001
- Government G-Cloud

Our Infrastructure

The Access Hosting solution has been designed to enterprise level with the highest possible specification for resilience and replication- split across 2 premium data centres

The solutions operate in a near continuous state across both datacentres minimising data loss in the event of a total data centre blackout. This is achieved using Zerto Virtual Replication and VMWare vSphere being delivered as a service to the Access user.

The Primary active datacentre is Telehouse West in the Docklands with the secondary datacentre being Equinix LD3 in Park Royal. The Solution allows for services to be migrated from one datacentre to another in real time as and when required.

The connections between the two datacentres are based upon Dark Fibre DWDM (Dense wavelength division multiplexing), this provides an exceptionally fast connection with a low latency of less than 10ms.

The Hosted Environment

Firewalls

Perimeter Firewalls **-** Cisco ASA v9.8 with IDS (Fire-Power) modules connecting to a switching fabric provided by Cisco Nexus and Catalyst switches.

Server Firewalls **-** Windows Firewall and Sophos AV is deployed to all servers, desktops and laptops**.**

PCs & Laptops – Windows Firewall and MS Endpoint Protection**, a**ll Access laptops are encrypted with Bitlocker and staff using workstations are issued with encrypted drives or have secure network areas for data storage.

AV Updates **-** Signatures are updated hourly. / Rules are reviewed at minimum every 3 months. Logs are reviewed at minimum every 3 months. Any security issues are notified to the NOC for immediate investigation too

Availability and fault monitoring

Cacti and Nagios are used for and we offer a chargeable option to have IDS for isolated clients

Data Encryption

Data is encrypted in transit, with SSL offloaded on Brocade Traffic Managers, supporting TLS 1.2.
SSL certificates are signed by a commercial root CA with 2048-kit keys and AES256 encryption.

SQL data can be encrypted at rest if required by the client.

Security Incident and Event Management

We use AlienVault SIEM

Patching / Maintenance

The Hosting environment is patched and audited by our patch management system. This allows us to track and apply patches in a controlled fashion (pre-prod, UAT, Prod) All non-critical OS patches are applied within one calendar month of release, first into pre-production and then into production, as part of the scheduled maintenance window.

Security Logs

Monitored by 3rd party MSSP on request

Operational Logs

Are stored centrally and included in the daily backups with 1 year retention

Penetration Testing

Access carry out penetration (Pen) tests in addition to the standard quality assurance processes that form part of our agile software development. The penetration tests are undertaken by an external Crest Registered 3rd party company who are specialists in the field of Internet security. The Pen tests are segregated between infrastructure (networks, firewalls, ports etc.) and individual application tests (cross site scripting, SQL injection etc.). Penetration tests are scheduled to occur regularly and dovetailed with major software version releases.

In addition to human pen testing Access also carry out weekly automated vulnerability scans. This is an additional level of defence to automatically check if changes to the environment have exposed new vulnerabilities.

The Datacentres

UK - Telehouse West

Website

Certification

- ICO registration Z8030846
- ISO/IEC 27001:2013 (Information Security Management)
- ISO 22301:2012 (Business Continuity Management)
- PCI-DSS v3 (Payment Card Industry Data Security Standard)
- ISO 9001:2008 (Quality Management system)
- ISO 14001:2004 (Environmental Management)
- ISO 50001:2011 (Energy Management)
- BS OHSAS 18001:2007 (Occupational Health and Safety Management)
- RMADS (Public Sector Compliance)

Physical Security

- Independent client card identification access system.
- The data centre is constructed of Block & Metal cladding
- Secure & monitored single person point of entry, physically guarded 24/7
- Integrated digital video camera surveillance.
- Proximity card access from the main Data Centre building to specific facilities management suites.
- Strict security processes in place to ensure delivery and loading of goods are secure.
- CCTV coverage for the perimeter, common areas and facilities management suites.
- Protected perimeter fence fitted with intruder sensing.
- Secure access procedures to ensure you and your nominated staff gain authorised access to the facility whenever you require, day or night.
- Windows are fitted with bomb film protection.
- Mantrap access to Data centre
- 2.3 metres min perimeter fencing with motion detection in place
-

Power

- Four redundant HV power systems, from separate grids to each building on the Docklands site.
- N+1 redundant standby generators.
- Standby generators with a minimum of 24 hours autonomy at full capacity.
- 8 x 2.5MVA 11kV Generators.
- 2(N +1) redundant UPS floor by floor
- Redundant A & B power feeds to customer equipment

Cooling

- 6 x 2.7MW chillers N+2 configuration.
- Room Air Conditioning Units (RACUs) to provide down flow chilled water system at N+25%.
- RACU with bundled floor area and water leakage detection and monitoring.
- Hot aisle/cold aisle zone design.
- 800mm raised floor design with airflow space to provide the most efficient cooling.
- Free cooling operation in winter.
- Maximum external ambient temperature of 35 degrees Celsius dry bulb.
- The in-room units provide full function, closed control air conditioning, with cooling, humidity and de-humidification control.

Fire Suppression

- Data Centre areas are fitted with a fully addressable two stage fire detection system that monitors the under floor and the room.
- Detectors with 50% mix of optical and ionisation are installed split across 2 separate zonal-loops, to meet BS 5839, 6266, 5445 and 5588.
- Very early smoke detection alarms (VESDA) are installed throughout the facility.
- Dry sprinkler fire detection system to meet BS 5306, 3115 and with LFEPA approval.
- Gas suppression areas available for dedicated tenancy areas.
- Systems are designed to minimise any possible customer disruption and to ensure that any minor problems remain localised.

Connectivity

The facility has availability of wide connectivity to major telecoms and network service providers, and is connected to all Access data centres via the Access Alto network. In addition, LINX, the London Internet Exchange, has a live presence on the site, offering global peering and connectivity options for customers.

Access Alto uses multiple Tier 1 transit providers to ensure high speed uncontended connectivity.

Connectivity can be provisioned through 2 redundant meet me rooms offering true diverse network locations.

UK - Equinix LD3: Secondary

Website

Certification

- ISO 9001: 2008 – Quality Management
- ISO14001:2004 – Environmental Management System
- OHSAS 18001:2007 – Health & Safety Management
- ISO/IEC 27001:2013 – Information Security Management
- ISO50001:2011 – Energy Management System
- PCI-DSS v2.0

Security

The physical security of each IBX datacentre is one of our highest priorities. Each datacentre utilises an array of security equipment, techniques and procedures to control, monitor and record access to the facility. Some key features include:

- IBX datacentres are manned by onsite security on a 24x365 basis
- All doors, including cages, are secured with biometric hand geometry readers or access cards
- A silent alarm and automatic notification of appropriate law enforcement officials protect all exterior entrances
- CCTV digital camera coverage of the entire site, including cages, with archival system, integrated with access control and alarm systems
- Motion-detection for lighting and CCTV coverage
- All equipment checked upon arrival
- Visitors are screened upon entry to verify their identity, and in shared situations, are escorted to their appropriate locations
- Shipping and receiving area walled off from colocation areas

Power

Equinix IBX datacentres are designed with power systems that have built-in redundancy, full Uninterruptible Power Supply (UPS) systems with up to N+1 levels or greater, and backup generator systems in the event of a local utility failure.

Air Conditioning & Cooling

Precision HVAC systems cool the most demanding high-power deployments. The HVAC system provides appropriate airflow, temperature, and humidity to provide optimum conditions for equipment operation and to minimise downtime due to equipment failure.

Connectivity

The following Interconnection options and services are available:

- System – Overhead proprietary cable tray system with multi-tier ladder rack or underfloor tray work
- Cross Connects – Enables customers to connect to other parties within an IBX data centre or IBX datacentres on a campus location using copper or fibre services
- Metro Connect – Extends choice and reach for carrier and network availability across metro areas
- Equinix Carrier Ethernet Exchange – Enables Ethernet Service Providers to interconnect to CENs and expand the reach of Ethernet services
- Equinix Connect – provides a bundled IP transit solution for Equinix customers who require a single source solution.

Access Alto uses multiple Tier 1 transit providers to ensure high speed uncontended connectivity.

.