Field View infrastructure and DR

Overview

The purpose of this document is to describe the infrastructure on which the Field View system is hosted, and also to describe the backup/disaster recovery (DR) strategy for Field View.

Infrastructure

Field View is hosted using a hybrid cloud facility within a UK data centre. Servers and storage are all dedicated to MCS, whereas switching, routing and firewall is shared with our provider's public cloud. This leverages the performance characteristics of the Cisco 10GB routing equipment.

Our provider is certified to the following business and IT security accreditations: PIC DSS, PAS 2060, ISO27001, ISO9001, ISO14001and is an NIC EIC Approved contractor.

The physical hardware Field View is hosted on is protected in the following ways. Access to data centres is by appointment only with photo ID; Staffed 24/7/365 (by SIA-accredited provider employed staff); CCTV - internal and external; 2.8m secure fencing and razor wire perimeter fence; Site-specific, dedicated firewall technology; 24hr NSOI-accredited security patrol. UPS systems are operational, standby diesel generators and high-density infrastructures in excess of 15kW per rack, power supply is resilient and uninterrupted. We have 24/7/365 access to the data centre.

With regard to availability, our provider has 4 fibre internet feeds into the data centre building from different physical directions from 4 disparate providers providing connection redundancy to our private cloud. Power supplies are redundant and resilient in an N+3 configuration across our blades with backup generators in an N+1 configuration which can run indefinitely. Server enclosures are protected against fire, lightning and water.

Field View is currently hosted on 2 Cisco UCS blades which provide the database, web, BI and synchronisation services. These servers are virtualised using industry standard VMWare ESXi virtualisation technology. In the case of node hardware failure, failover will occur within minutes. All hardware is buffered with on-site replacements for all parts. Connectivity between the blades and storage is via 8Gbps fibre channel. Servers are protected with redundant Cisco Firewalls and are routed via Cisco Nexus 10G switches. The data centre infrastructure also has measures in place to mitigate DDoS attacks.

Our virtualised infrastructure provides resilience, redundancy and failover capability to redundant nodes. Storage is provided using RAID10 disk arrays providing error correction, redundancy, 2 hot spare disks and hot-swap capability in case of hardware or node failure.

Backup and DR

Server images are backed up daily to the backup server backup server, maintained separately from the storage array, with 30 days retention. Database backups are taken daily with 30 day retention. Since data up to a day old would not be appropriate in a disaster situation, 15 minute log files are stored at the data centre and shipped to a physical different site where a warm backup is maintained and can be restored to within 15 minutes of the live database.