

MEDIAROOM

Products Hosting Infrastructure Documentation

Introduction

The purpose of this document is to provide an overview of the hosting infrastructure used for our line of hosted Web products and provide logistical information. The hosting facility is owned and operated by ViaWest, an experienced and trusted, super-regional provider of co-location, managed hosting and business continuity solutions.

Documentation covered in this disclosure includes the following:

- Hosting Structure (Redundancy & Load Balancing)
- Network and Hardware Redundancy
- Backup and Recovery
- UPS Systems
- Security Policy
- Monitoring (Alerts & Logs)
- Systems

Hosting Facility Overview

ViaWest designed data centers are built with multiple fiber and circuit entrances providing redundancy at the physical layer. These entrance facilities meet and/or exceed Bellcore standards for diverse entrances and physical separation.

Multiple Cores

- ViaWest data centers are designed with multiple core routers, allowing ViaWest to expand its network with little to no impact to customers

Multiple Switches

- Failure in the aggregation layer is minimized with redundant devices also directly interconnected and each having a connection to a core router. ViaWest also offers redundant connections through unique distribution switches.

Logical Redundancy

- ViaWest's backbone routers run an Open Shortest Path First (OSPF) protocol to determine the best path from one location to the other. If a circuit or device fails for any reason, each router automatically calculates the newest "best path" to forward traffic minimizing any impact a customer may experience.

Physical Diversity

- ViaWest has four data centers throughout the Rocky Mountain region, each containing a specified amount of redundancy and mirroring of operations across all data centers.

Network Redundancy

- ViaWest data centers are connected through a packet over sonnet fiber ring utilizing redundant circuits from various providers

Backup and Recovery

- The following disaster recovery services are provided:
 1. **Data Storage** – Data is regularly backed up and tapes are rotated to an offsite, fire-safe vault further ensuring if the main facility goes down, a back-up can be located off-site.
 2. **Load Balancing** – Web sites and data are run from two or more servers using a load balancer to route traffic between separate instances on different servers. In the event of a problem with a server, the load can be transferred to the remaining servers, with little or no disruption to service or loss of data.
 3. **Clustering** – Multiple servers are used as part of a single, clustered system. If one machine fails, the remaining servers will automatically redistribute the load, keeping services intact.

Maintaining/Restoring Business Operations

- Each of the ViaWest Network Operations Center's is independent of the other and is capable of monitoring and maintaining all of the ViaWest network and infrastructure independent of the other.
- If data recovery is required to resume normal business operations, remote copies of all critical data are stored off-site and can be used to restore operating systems, production data, databases, configurations and other records as needed.
- Critical data is maintained online at multiple locations and can be retrieved through the network to restore local copies.

UPS Systems

- In each location, multiple UPS systems are available to provide redundant power to the critical load. All locations have at least two UPS's deployed in an N+1 configuration that customers may take advantage of by having power from each UPS delivered to their equipment.
- In ViaWest facilities where power is run under the raised floor, all electrical cabling used is constructed of waterproof materials and is located off the floor so it will not be impacted by water or flooding. In addition, water sensors are located under the raised floors which will immediately notify local and remote personnel of the presence of liquid under the floor.

HVAC

- Each ViaWest Data Center is equipped with multiple independent condenser/air-cooled and dry cooler/glycol/water-cooled Heating, Ventilation, and Air Conditioning (HVAC) systems to minimize the single point of failure common in chiller-based systems.
- All ViaWest data centers are on raised floors and incorporate down flow air handlers for maximum cooling flexibility. Down flow systems feed cool air to the critical loads through perforated tiles in the raised floor and return warm air through filtration systems at the top of the air handler units.

Fire Detection and Suppression

- ViaWest incorporates dual-zone, two-stage fire detection systems in all of its facilities. A dual-zone system minimizes the possibility of a false alarm indication by having each detector installed in a different zone than its nearest neighbors.

Physical Security

- All persons who have authorized access to any ViaWest facility are issued photo ID/access cards. All access badges have different formats designating their security level. Each card is individually serialized and all entries to facilities are electronically logged.

Monitoring (Alerts & Logs)

- Each critical environmental system is individually monitored for correct operation. If any system fails its internal diagnostics, reports an error, or falls out of its nominal operating range, that symptom is immediately reported through an out-of-band connection to a remote monitoring station that will immediately dispatch the appropriate field service technician to the site where the potential problem is occurring.

1. **Monitoring Alerts** – An email notification is sent whenever the NOC detects a service interruption (HTTP, MySQL, SMTP, etc)
2. **Backup Alerts** – An automatic email is triggered whenever any errors are detected in nightly data backups
3. **Application Event Notifications** – Our applications rely on several timed processes, or "cron jobs", which send diagnostic information regularly about all of our web applications. For example, if a site template is pushed to production, or if there's an error subscribing someone to an email list.

Server Infrastructure and Architecture

Firewall Protection

- ViaWest uses industry leading firewall hardware to protect all applications and data. External and internal traffic is monitored continually by the company's system security administrators. All back-office systems are protected using standard SSL (Secure Socket Layer).

Firewall Configuration:

- NetScreen: managed by ViaWest security experts, our facility has two firewalls configured in High Availability mode. This allows the complete loss of one firewall and a seamless transition of traffic to the secondary firewall.

Network Routers, Switches and Servers

- All routers, switches and servers are kept in physically secure areas. Access to these secured areas is restricted to a select number of individuals. A current topology of the network is maintained and updated as new hardware and port assignments are made.

Network Intrusion Detection and Prevention

- ViaWest partners with the leading authority of Internet security in implementing security tool that allow us to secure our systems by monitoring the network and servers for signs indicating possible attacks. The ViaWest firewall and data network configurations are maintained at strict levels of security. Each external network port is configured according to internal guidelines and is monitored routinely.

Denial of Service (DoS) and Distributed Denial of Service Attacks (DDoS)

- ViaWest's strategy to combat DoS and DDoS attacks is a multi-faceted approach that includes detection, tracing and isolation of the network abuse events. The ViaWest policy is to act before other customers may be impacted. The NOC is equipped to monitor any alerts, allowing appropriate changes to be made, mitigating the affects of attack.
- ViaWest has working relationships and direct security contacts with all major network providers.
- ViaWest actively monitors and participates in security and Computer Emergency Response Teams (CERT) related communities and mailing lists.

Web Solution Infrastructure and Architecture

All Web solutions are built using our proprietary SPIN platform. Documentation covered in this disclosure includes the following:

- Database Requirements
- Software Specs (SPIN Configuration)
- Caching

Database Requirements

- A site/application built on the proprietary SPIN platform has very simple database requirements:
 - A single MySQL database
 - A single MySQL user with INSERT, UPDATE, SELECT, and DELETE privileges on that database
- SPIN has currently been tested on versions of MySQL up to MySQL 5. Current System Requirements are as follows:
 - RedHat Enterprise ES 3 (though any Linux should be fine)
 - Apache 2.0 (1.3 is fine)
 - MySQL 4.1.8 – standard

Configuration

- We utilize Web Servers behind a redundant load balancer.
- The Database Server's use MySQL 5 Cluster, a real-time transactional database designed for fast, always-on access to data under high throughput conditions. MySQL Cluster utilizes a “shared nothing” architecture which does not require any additional infrastructure.
- The servers are dedicated; eliminating constraints that shared services has with CPU/RAM hogging. Our current average utilization is 15% - 30% of this capacity.

Database Server

- DB-EdgeServer 200 Red Hat Linux ES Dedicated Server
- Intel Quad Core Xeon Processor
- Red Hat Linux ES OS Server license
- 24 x 7 on-site monitoring with event notification and ticket generation
- 24 x 7 on-site hardware management
- Local hardware sparing

Web Application Server

- Web AppServer 300 Red Hat Linux ES Dedicated Server
- Intel Dual Core Xeon Processor
- Red Hat Linux ES OS Server license
- 24 x 7 on-site monitoring with event notification and ticket generation
- 24 x 7 on-site hardware management
- Local hardware sparing

Caching

- Our Web products use server side caching of complete HTML pages. The benefit is to reduce repetitive queries to the database, which can dramatically increase the performance on a busy site. When a page is edited in Site Manager, the complete site cache is flushed. We are not aware of any limitations in our caching setup including memory or disk limitations.
- A site's cache directory has enough available disk space to support writing all pages of a site to this directory, but this should not be significant. A page is "published" (in real time) when editing the given page with the Site Manager and clicking 'Save'.
- A page is written to the Server Side cache directory when the first user accesses that page.