Autimo and Concert Properties collaborate on a robust and innovative web hosting platform in AWS

aws partner network

CONCERT® PROPERTIES

Overview

Autimo worked to migrate current web applications to a secure, highly available, containerized solution in AWS. A key requirement was well documented backup and disaster recovery capabilities, and integration of identity and access management into Azure identity providers for authentication. The new autoscaling, highly available containerized solution allows Concert Properties to grow and manage their business in a secure and stable way.

The Challenge

Concert Properties has a diversified portfolio, requiring the development and deployment of new websites and domains as projects come to market. Concert Properties has made the strategic decision to host and manage these sites in-house to ensure stability, agility and security. At the time they reached out to us, Concert Properties was managing 30 live sites and 120 domains, deployed to a variety of hosting and service providers, including managed services and co-located servers.

- Maintenance was an issue with some environments running legacy versions of supporting libraries.
- Monitoring was limited or non-existent, with members of the business providing the first indication a site had errors.
- Creating new sites was a laborious and error prone manual process.
- Reliability and security of environments was being impacted.
- The team didn't have a centralized capability for managing updates

Concert Properties partners with a number of development agencies to develop and maintain websites, allowing for the highest standards of creative control within the business, but creating challenges with ensuring standards are consistent and appropriate access is provisioned. This led to inconsistencies, and varying levels of documentation, which impeded attempts to deploy a consolidated web strategy.

"Autimo's ability to rapidly respond to emergent requirements and deliver stable, dependable support and services has given us the confidence to rely on them for all of our AWS infrastructure support and service needs" ***- Adam Fletcher, Director Tech Infrastructure and Operations at Concert Properties***

AUTIMO

Company: Concert Properties
Industry: Real Estate Development
Country: Canada (HQ)
Employees: ~500
Website: concertproperties.com

Since 1989, Concert Properties has proudly developed, acquired and managed Canadian real estate in pursuit of building a people-first future. With over $8 billion in assets, they are backed and owned by over 200,000 Canadians, represented by union and management pension plans. Concert Properties comprises three corporate entities, Concert Real Estate Corporation, Concert Infrastructure and Concert Income Properties. Within these entities, they develop and manage rental apartments and seniors' active aging communities; develop condominium homes; develop, acquire and manage commercial and multi-unit residential properties; and invest in, develop and manage public infrastructure projects across Canada. In each area of their business their vision remains the same: build resilient, inclusive and sustainable communities.

The Solution

An initial audit determined that there were around 120 hosted sites, although only 30 were active and in use. The rest were legacy, development or cloned environments used for testing.

Working with members of the Technology Infrastructure and Operations team, we categorized these sites as:

- Active - Live production environments, with a need for dev and staging environments.
- Legacy - Legacy production site. Testing, & development environments no longer in use.
- Developmental - Currently used as development and testing environments

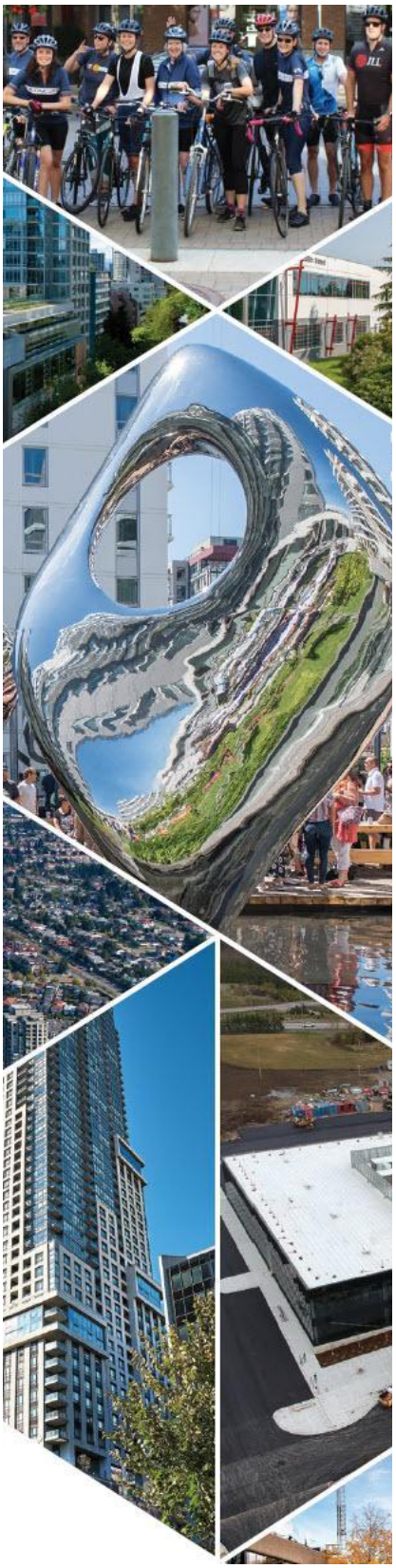
In the interests of controlling cost and eliminating needless work, Concert Properties opted to configure a full set of environments (dev, stage and production) for the Active sites, and additional environments for Legacy sites would be provisioned when requested by development teams. The time taken to configure new environments enabled by the use of terraform and Infrastructure as Code is now counted in minutes instead of days.

The overarching containerized design selected by Autimo utilizes ECS in Fargate with RDS and EFS for persistent data storage, cached by Cloudfront as required. This allows us to offer an arbitrary set of libraries to each site (i.e. support for legacy sites 'as-is') and offers a "batteries included" horizontally-scaling solution that can within seconds gracefully and automatically meet fluctuating traffic loads experienced.

Templated deployment solution via Terraform Infrastructure as Code. The infrastructure implemented as part of this deployment was codified with Terraform and stored in an AWS CodeCommit git repository. Using an IaC approach reduces the likelihood of misconfiguration due to human error, allows for rapid redeployment in the event of disaster and allows for rapid operational support deploying new sites and environments. It also offers a "live view" of the current environment state which can be used alongside documentation, forming part of a standards compliant environment.

For the live sites we defined a **development platform with continuous integration (CI)**. Starting with the customers and working backwards, developers interact with an Azure DevOps git repository, (selected in order to **take advantage of the existing corporate IAM and user accounts in Azure Active Directory**). Utilizing a branch-based deployment strategy, a commit in Azure DevOps is mirrored to an equivalent repository in AWS CodeCommit. An Azure DevOps pipeline performs this action.

As a result, we can still build in the event of an Azure outage. When a commit is pushed to the appropriate CodeCommit repository, it triggers a pipeline run in AWS CodePipeline that then builds out a new container. Containers are pushed to an ECS Container Repository and then the pipeline updates services to run the latest containers. This is implemented for dev, stage and production branches as standard, but could be extended should the need arise.



Logging and reporting, application and operating system logs are all shipped to CloudWatch, joining the logs from other AWS services. A custom dashboard showing overall site health as well as utilization of shared resources allows the Concert Properties operations team to inspect load and performance in real time. **Alerts are configured to raise tickets** in the appropriate ticketing system for respective services and a monthly report of ALB activity is emailed to selected contacts via an email distribution list.

Security. Utilizing a containerized approach reduces the 'blast radius' of any possible compromise to just the single site in question, a considerable improvement to the shared hosting used previously. The use of IaC reduces the chance of misconfiguration and facilitates easier inspection and audit by InfoSec teams. To provide an additional layer of protection a WAF attached to the platform's ALB is used. These rules, available by subscription from an AWS partner, **guarantee (with SLA) mitigation from CVE's related to the specific workloads (Drupal, Wordpress, ASP.net and Java)** within hours of CVE publication.

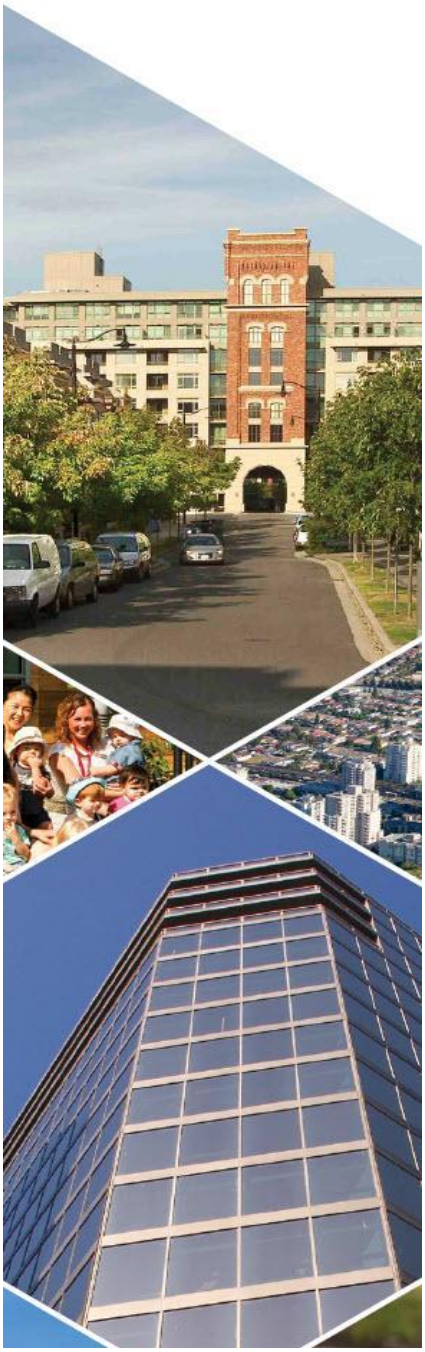
Multi-tenant access to files. A secure solution using an SFTP jumphost on the public internet was designed to provide secure public internet access to files in EFS. This enables multiple staff members from agencies to gain access to the document root of just the site(s) they are working on in a secure way, with full logging of access and activity transferred to cloudwatch.

HA & DR. RDS and EFS are configured for multi AZ replication, ensuring all non-ephemeral data is highly available. Containers are also retained in a multi-region library. Currently in the event of an AZ outage, manual intervention would be required to **spin up the infrastructure in a new AZ within minutes** using the existing terraform Infrastructure as Code.

Self healing. The containers themselves are configured with health checks running from the ALB, and efforts have been made to ensure that the test represents end-to-end health (i.e. ensures the entire stack is operational, not just the HTTP server). In the event of a failed test, the container is automatically replaced, a process that takes around 15-30 seconds. For high priority sites, multiple instances are operational at once, ensuring that the site will remain available even if a container fails. This ensures the entire stack is highly available and self-healing.

In the event of a site being compromised and/or defaced, a plan was put in place and playbooks produced to ensure business continuity utilizing a variety of measures designed to be compatible with Concert Properties' 24/7 support desk capabilities.

Backup. Non-ephemeral site assets are all stored in EFS and RDS. RDS is configured with point in time recovery, and EFS has regular incremental backups enabled, with periodic full backups and a suitable retention period. Code is stored in git and retained reliably by CodeCommit. Containers, which could be rebuilt from source if needed, and are also stored in a redundant fashion.



Consolidate and migrate DNS. Concert Properties' domains were registered in multiple locations with various levels of security and privacy enabled. We worked to move all the domains to a single registrar protected by two-factor authentication and out of band human approval for domain migrations. Route53 was then used for hosting DNS zones.

Training and ongoing support. Concert Properties continues to work with Autimo on an ongoing basis as we cross-train and educate the Concert Properties team, with the long term plan of enabling self sufficiency. As one of our core values at Autimo is education, we feel it's hugely important to ensure continuity of operation through on-the-job knowledge transfer and training.

The Result

The containerized solution designed and implemented by Autimo has allowed Concert Properties to gain full control and insight into their web estate. **Reliability has improved, and security risks have been mitigated**. Sites are now hosted in a highly available state and a disaster recovery plan has been implemented. Concert Properties is now able to move faster and more efficiently with a customized process for rapidly deploying new sites.

This dynamically scalable solution now means that all sites can **scale to handle an arbitrary amount of traffic and scale down when traffic is low**, ensuring cloud infrastructure operational costs are reduced without impacting performance.

In terms of numbers, the Concert Properties team has been able to **reduce operational cost by 70% compared to spending on previous hosting solutions**. Migrating all sites to a single solution has also reduced maintenance overhead and, although unquantified and anecdotal, the number of issues and time spent managing change has seen significant improvement.

Security posture has improved, with developers no longer having direct access to production environments, and process and approvals have been implemented for production releases.

As a result of this successful project, Concert Properties and Autimo continue to collaborate and iteratively improve the infrastructure via an operational support contract.

Autimo, a cloud engineering and DevOps services provider headquartered in Vancouver, Canada, works with customers across North America and Europe.

Going beyond pure services, we believe relationships and education are as important as technology and are committed to growing and learning alongside our customers, partners, the community and each other.

We specialize in long term, integrated partnerships with customers to develop their cloud practices interfacing at the strategic, consultative, implementation, and ongoing support levels.

As an AWS Advanced Tier Partner, we ensure that we carefully understand the challenges that our customers are facing and work closely to form a cloud strategy that will allow them to leverage the best AWS services for their business.

Autimo specializes in:

- Cloud Strategy
- Platform Engineering
- Infrastructure as Code (Terraform, CloudFormation, etc.)
- Containerization (k8s, Helm, etc.)
- Well Architected Framework Review. & Remediation
- Landing Zones & Multi Account
- Pipelines, CI/CD & infrastructure integrations
- Software Development Lifecycle & Process Design
- DevOps on Demand

For more information visit us at https://autimo.com

AUTIMO