QBurst | A High AI-Q™ Company



Scalable AWS Cloud Architecture & Disaster Recovery for Enterprise Web Systems

Delivering a highly available, scalable AWS infrastructure powering enterprise WordPress web platforms with Auto Scaling, shared storage, serverless database capabilities, and automated backup governance.

Overview

We implemented a highly resilient AWS web architecture for Brookfield, decoupling enterprise WordPress application layers using Auto Scaling EC2 compute nodes, Amazon EFS shared storage, and Amazon Aurora Serverless v2.

- **Decoupled Architecture & Auto Scaling Compute:** Deployed WordPress workloads on Amazon EC2 behind Application Load Balancers (ALB) with Auto Scaling, utilizing Amazon EFS for multi-instance persistent file synchronization.
- **Perimeter Defense & Accelerated Edge Delivery:** Configured Amazon CloudFront for global caching paired with AWS WAF to inspect incoming web traffic and mitigate malicious requests at the edge.
- **Automated Backup & Continuous Governance:** Integrated AWS Backup and dedicated Backup Vaults for automated EC2/EFS recovery, backed by UptimeRobot monitoring and CloudWatch alarms.



Client Profile

A leading global real estate owner, operator, and developer, Brookfield manages a diverse portfolio of office, multifamily, retail, logistics, hospitality, and mixed-use properties. Based in North America, the company delivers large-scale real estate solutions across major markets worldwide.

High Traffic Volatility and Multi-Node Synchronization

Delivering enterprise real estate digital experiences on WordPress presented significant infrastructure and operational challenges.

- **Variable Traffic Demand & Capacity Bottlenecks:** Required dynamically expanding and contracting compute capacity without single-server dependencies or downtime during peak visitor traffic.
- **Shared Storage Across Dynamic Instances:** Needed a centralized, highly performant shared file system for WordPress media uploads and core assets accessible across scaling EC2 nodes.
- **Public Edge Vulnerabilities:** Demanded robust perimeter security to inspect incoming web requests, block malicious bots, and prevent common web exploits before reaching origin servers.
- **Database & Recovery Overhead:** Required database scaling aligned with real-time application load alongside automated, policy-driven disaster recovery for application files and database states.

Scalable AWS Infrastructure & Edge Security

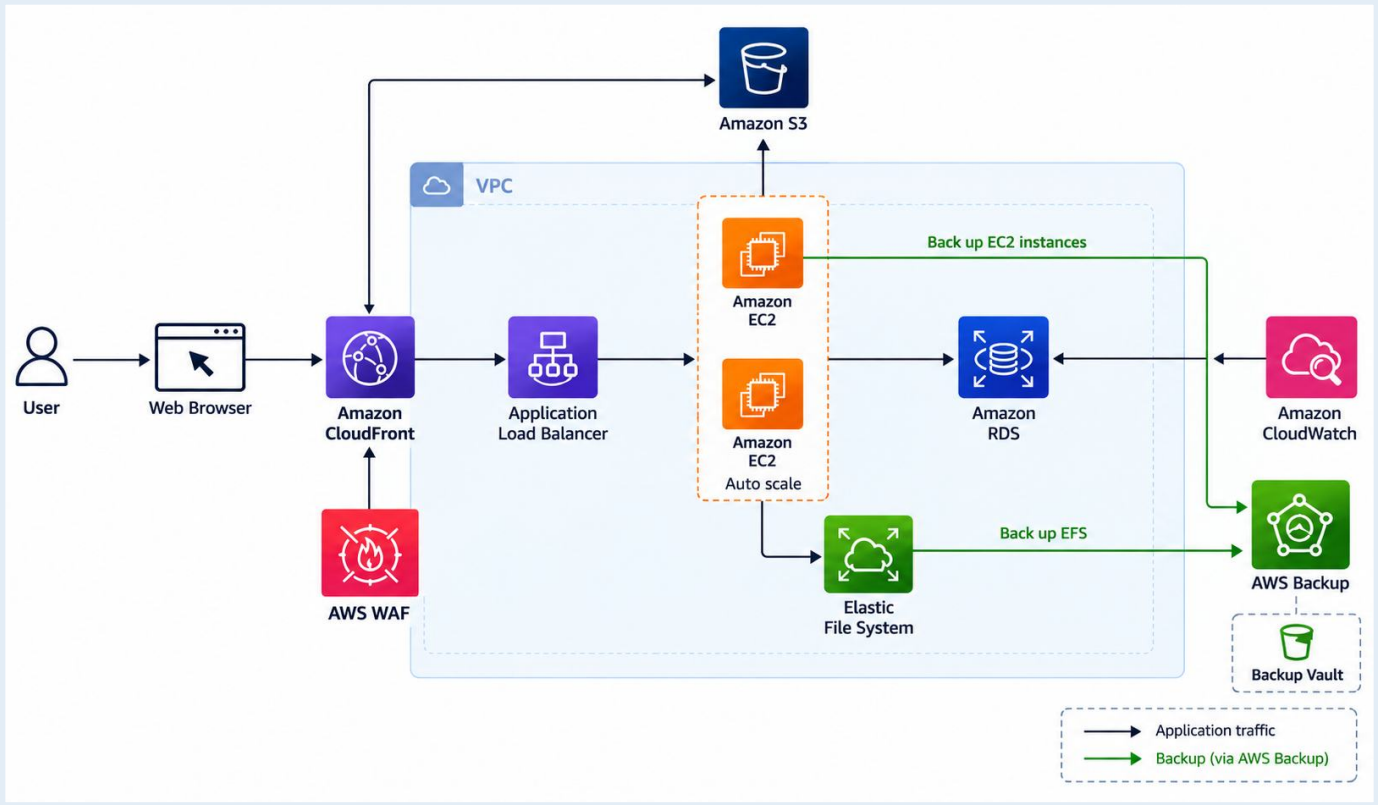
We built a secure, multi-tier AWS infrastructure within an Amazon VPC network foundation.

- **Load-Balanced Compute & Auto Scaling:** Hosted WordPress on Amazon EC2 instances behind an Application Load Balancer (ALB) that distributes traffic across healthy targets, backed by Auto Scaling policies.
- **Shared File Layer & Serverless Database:** Implemented Amazon EFS to provide a shared, persistent file layer across all EC2 nodes and deployed Amazon Aurora Serverless v2 (MySQL-compatible) for dynamic, auto-scaling database performance.
- **Edge Delivery & Threat Inspection:** Utilized Amazon CloudFront for global content delivery and caching, integrated with AWS WAF to filter malicious traffic and forward valid requests to origin ALBs.
- **Centralized Object Storage & Backup Vaults:** Managed operational assets, logs, and exports in Amazon S3, using AWS Backup and Backup Vaults to enforce automated recovery policies across EC2 and EFS resources.

- **Multi-Tier Operational Monitoring:** Configured Amazon CloudWatch for infrastructure metrics and log routing to QBurst DevOps, alongside 5-minute UptimeRobot availability checks alerting development, support, and client teams.

Technical Highlights

- **Compute & Load Balancing:** Amazon EC2, Application Load Balancers (ALB), Auto Scaling.
- **Edge & Security:** Amazon CloudFront, AWS WAF, Amazon Route 53, Amazon VPC.
- **Data & Storage:** Amazon Aurora Serverless v2, Amazon EFS, Amazon S3.
- **DevOps, Monitoring & Governance:** AWS Backup, Backup Vault, Amazon CloudWatch, UptimeRobot.



AWS Solution Architecture

Enhanced System Resilience and Proactive Recovery

- **Dynamic Traffic Handling:** Auto Scaling policies and ALB target balancing eliminated single points of failure and adjusted compute capacity seamlessly to match visitor spikes.
- **Shared File Consistency:** Amazon EFS ensured zero asset discrepancy or missing media files across dynamically launched or replaced EC2 instances.
- **Edge Threat Mitigation:** AWS WAF and CloudFront reduced origin server load, improving global cache hit ratios while blocking malicious requests before origin processing.
- **Automated Disaster Recovery Readiness:** AWS Backup Vault workflows ensured consistent backup success rates and rapid recovery point objectives (RPO) across EC2 and EFS storage.
- **24/7 Incident Escalation:** Integrated 5-minute external availability checks with CloudWatch alarms to provide real-time alerts to support and DevOps teams for immediate incident response.