/// VOLUME 1

CLASH OF CLOUDS

AWS V AZURE V GCP

LLOYD LOWSON

CLOUD & DEVOPS SPECIALIST
MAXWELL BOND

maxwellbond

TRUSTED TECH TALKS
WEBINARS · EVENTS · NETWORKING

WITH THANKS TO:

DAVE MASON
HEAD OF SOFTWARE ENGINEERING
GCP SPEAKER

ANDY NORTON
SOFTWARE DEVELOPMENT MANAGER
AZURE SPEAKER

PAUL MADDOCKS
LEAD SITE RELIABILITY ENGINEER
AWS SPEAKER

CLOUD SECURITY

LADBIBLE AND GCP

LADbible is the 14th busiest website, with over 100 million sessions per month. This means security is crucial. Within GCP you've got google cloud CDN (content delivery network) and Google Armour which works alongside it to provide predefined web application firewalls, as well as customised rule definition across layer 3 and layer 7.

Additionally, feeding the data into two places, the Security Demand Centre (where DevSecOps sits) and Cloud Logs, which can easily be expanded into Big Query (GCP's data lake product), has proven valuable. This comes with its own Sequel based analysis language which can query dozens of GB of log data, very quickly.

One problem that Dave has faced is content scraping. People were writing scraping scripts to steal content from LADbible pages, and reshare it on other websites. The problem here, in addition to the stolen content, related to the fact they where spamming their websites with tens of thousands of requests in seconds which reduced platform stability.

Big Query have come into use here, as they allow the breakdown of individual URL's based on IP addresses, and can then create custom firewall rules based on this collated, granular data. As Firewall changes are made, it is fundamental that they are tested against previous traffic in 'preview mode' to avoid potentially damaging mistakes.

Named IP lists can also white list traffic from certain IP addresses, and can automatically update rules when changes happen.

FOOTASYLUM AND AZURE

Andy at Footasylum operates a similar approach to security but also actively suggests using Azure Front Door (AFD) which sits at the front of the application. AFD offers a single secure global entry point for web applications, APIs, content and cloud services. Utilising a global infrastructure, Azure Front Door enables Azure customers to securely deliver and manage their global applications and content, migrate to cloud and modern microservice architectures and improve their users' experience.

Azure Front Door enables the building of secure, high performaning and highly available web applications through global load balancing with application acceleration and web application firewall.

In addition to this Azure offers the Azure Security Centre, which is a unified infrastructure security management system that strengthens the security posture of your data centres, and provides advanced threat protection across your hybrid workloads in the cloud and on premises. The Security Centre gives them full visibility across the whole platform and gives them full insight into traffic trends. It can identify strange activity and will suggest improvements and changes. Plus, if you're already with Microsoft the initial integration is easy.

SORTED GROUP AND AWS

Again, AWS offers security tools which are very similar. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. There is also the option to upgrade to include 24/7 access to a support team.

Additionally, Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. This is also easy to use and very easy to integrate.

Paul explains that the volume of logs for small teams can be overwhelming, but my automating large parts of this progress and the ability to rely on AWS to make suggestions, this relieves stress and pressure off development teams. An example of this is Amazon's Guard Duty, which identifies anomalous behaviour, flags it and then automatically blocks IP addresses.

BIGGEST COMMON CHALLENGES WITH CLOUD SECURITY

- Logging congestion and volume
- Amount of data can be hard to manage if you're not from a Security background
- It's often a steep learning curve in situations where you can't afford to get it wrong
- Can be easy to get blinded by the science
- Cloud can give a false sense of security

CONTAINERISATION AND KUBERNETES

LADBIBLE AND GCP

Dave is a strong believer in Kubernetes and believes GCP is the strongest cloud platform provider for Kubernetes. The biggest benefits and functionalities include:

1. They allow developers to run the same container on a laptop as on a much bigger scale which makes life much easier. The whole team doesn't have to have the same version of Node to make it work.

2. Using a Doc Composer tool, within 15 minutes developers can make a similar replication of production on their devices with hot code reloading, which means fast feedback and higher time efficiency.

3. Namespaces are used to create feature branch environments. When you have a feature on a branch, and push it up to Github, you get a web hook which kicks of something Cloud Run which creates a Kubernetes Namespace and then deploys the application into that Namespace with the code from your feature branch. It then also creates a DNS record. Within ten minutes you have a public URL which is great for showcasing.

4. The Blue Green Deployment Model helps get software from the final stage of testing to live production. You usually need to do this quickly in order to minimize downtime. The blue-green deployment approach does this by ensuring you have two production environments, as identical as possible. At any time one of them, let's say blue for the example, is live. As you prepare a new release of your software you do your final stage of testing in the green environment. Once the software is working in the green environment, you switch the router so that all incoming requests go to the green environment - the blue one is now idle.

5. Helm charts also make it easier to create deployments within Kubernetes that follow industry best practices.

6. Kubernetes scales really well.

FOOTASYLUM & AZURE (SERVERLESS)

Serverless has been around a lot longer than people realise and Andy suggests that this is where all services will eventually head towards, and Kubernetes is just a steppingstone along the way. He suggests that whilst Kubernetes can be a good tool, it is often just a knee jerk reaction by businesses who think they need it, when in some cases it actually adds no real value. It can also be a lot to learn.

Serverless, on the other hand, offers out of the box solutions including emulators and abstractions to test applications against the storage services locally without creating an Azure subscription or incurring any costs. By going serverless, it reduces the amount that developers have to manage so that they can refocus on more business-critical development tasks.

CONTAINERISATION AND KUBERNETES

SORTED GROUP & AWS

Paul cites the main benefit of Kubernetes as giving the developers the opportunity to pull containers together and do all the testing locally and pull forward into Kubernetes and touch the backend services. This means they can do full integration testing from their desktop without having to build a full testing environment locally. This is a huge time saver.

Also, because Kubernetes now spans across all cloud platforms, it eases the worry about vendor lock-in, as it enables businesses to effectively "lift and shift".

TOOLS

FOOTASYLUM & AZURE

Andy uses Azure DevOps, which provides version control, reporting, requirements management, project management, automated builds, testing and release management capabilities. It covers the entire application lifecycle and enables DevOps capabilities.

Azure DevOps enables CI/CD for any platform, and lets developers build, test, and deploy in any language, to any cloud—or on-premises. It can also run in parallel on Linux, macOS, and Windows, and deploy containers to individual hosts or Kubernetes.

Within 2 or 3 mouse clicks you can have a full build deployment for anything within Azure, which means they can move very quickly and efficiently. Plus if there is any problems, it's easy to identify and anybody can pick it up.

LADBIBLE & GCP

GCP offers the CI/CD tool Cloud Build. Cloud Build executes builds on Google Cloud Platform infrastructure and can import source code from Google Cloud Storage, Cloud Source Repositories, GitHub, or Bitbucket, execute a build to your specifications, and produce artifacts such as Docker containers or Java archives.

It has a great free tier, called Docker Compose, which makes it a great product for start up companies who are looking to cut excessive costs. However, it is not a mature product and still has some issues and significant limitations. For example, it has predefined build steps, so businesses find themselves building new custom build steps which eats into developer time. Additionally, there is no SSH debugging of the build agent or built in caching layer.

The main benefit of Kubernetes on GCP though, is automated, scheduled node upgrades. Neither Azure nor AWS offer this.

TOOLS

SORTED GROUP & AWS

AWS has many provisions in this area including CloudFormation, an easy way to model a collection of related AWS and third-party resources, provision them quickly and consistently, and manage them throughout their lifecycles, by treating infrastructure as code. A CloudFormation template describes your desired resources and their dependencies so you can launch and configure them together as a stack.

Whilst some users may be concerned around vendor lock-in when using native tools, Paul explains that there are a lot of benefits to using AWS native CI/CD tools such as:

1. No charge for CloudFormation utilisation

2. Access to Code Deploy, a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers, at no additional charge.

3. It's powerful from a Blue Green perspective as you can utilise and modify pre-made templates.

4. Security scanning of your container registries included.

AWS have done their best to create a user friendly and cost-effective product that will suit a wide variety of businesses.

KEY THINGS TO REMEMBER

ON COST

Serverless is not always the best option for all businesses. It always depends on specific user cases, requirements, and needs. Whilst serverless can be more cost effective on your cloud bill, but it can be timely and costly in terms of allocating employees to manage it for certain businesses. It's important to thing about cost holistically and look at the overall cost rather than just product cost.

ON MULTI-CLOUD STRATEGY

Some businesses utilise multiple cloud providers for different things. This has benefits including, avoiding vendor lock in, taking advantage of the strengths of each cloud provider, and maximises the opportunity to optimise cost and efficiency. However, it can pose security challenges, can affect your entitlement to certain customer perks, and can be very difficult to manage.

ON SECURITY MANAGEMENT & RESPONSIBILITY

It depends on the size and maturity of the business as to who is responsible for monitoring the security of a business's cloud platform. Ideally, a business would have a dedicated security team, or a dedicated DevSecOps team which would manage cloud security, however smaller businesses may not have the ability to do so. It's important that however a business is structured, the team knows whose responsibility it is to monitor security. Essentially though, everybody working on a product or software has responsibility to ensure it is secure. This includes vulnerability management, and an assessment of internal and external risks. Having robust policies is a must.

CONTACT US

BUILD HIGH PERFORMING DEVOPS, CLOUD & INFRASTRUCTURE TEAMS WITH MAXWELL BOND, THE RECRUITMENT PARTNER OF CHOICE ACROSS THE UK AND GERMANY.

LLOYD LOWSON

CLOUD & DEVOPS SPECIALIST
LLOYD. LOWSON@MAXWELLBOND.CO.UK

maxwellbond

TRUSTED TECH TALKS
WEBINARS · EVENTS · NETWORKING