CloudFormation Based Automated HA Deployment

Assumptions

* This automation template deploys a n-tier Architecture on a single AWS region; this template uses amazon linux ami's. in case you want to change the Operating System please change AMI ids in template File.
* This template assumes you have created an EC2 Keypair for SSH Access

Steps to run the Script

* Login to Console using below credentials
* Create an Ec2-Keypair for SSH access to instances
* launch a Stack from the automation template
* Once Automation Template is ended launch the MyBB appliation using load balancer name mention in the output variable
* you can evaluate the work by below credentials
* URL :- **https://moingodil.signin.aws.amazon.com/console**

username :- Viewer

Password :- p0\*Dj\*OgRFK\*

* the above account has read only access till 15 th feb 3 PM IST
* MyBB application Administrator Account:

Username: admin

Password: Admin@123

What will happen post execution of Template

Cloud Architecture

VPC

AmazonELB

Internet Gateway

Multiple Availability Zones

Web Server (EC2)

Web Server (EC2)

Web Server (EC2)

Multiple Availability Zones

MySQL Slave (Read Replica)

Mysql Master RDS Instance

AutoScaling Group

DB s

## Security considerations

- The entire infrastructure is encapsulated into a VPC; all Internet traffic goes through:

- \*\*VPCInternetGateway\*\*: gateway to Internet for VPC components (PublicSubnet\*).

- There are two main Security Groups which separate the internet-facing parts of the architecture,

meaning the web-servers (and associated components), from the private parts, meaning the database

cluster mainly.

- \*\*WebServerSecurityGroup\*\*: HTTP/HTTPS/SSH access permitted from outside.

- \*\*DBSecurityGroup\*\*: Database, access permitted only from Web Server to DB Server.

- There are two Subnets associated with each group (in distinct availability zones):

- \*\*WebServerSubnetA/B\*\*: web servers stack, the subnets are publicly accessible.

- \*\* RDSSubnetA/B\*\*: database stack, the subnets are not publicly accessible.

The routing for these subnets is as follows:

- \*\*RouteTable\*\*: opens traffic from the public subnets to the Internet.

- \*\*PrivateRouteTable\*\*: ensures privacy for the hidden subnets.

Currently the private subnets have no access to the outside world.

## Scalability considerations

- \*\*Web Cluster\*\*: the web servers are governed by an AutoScalingGroup and sit under an ElasicLoadBalancer instance for load-balancing and fault-tolerance.

- \*Vertical scaling\*: web servers can be upgraded to larger memory/compute/storage capacities without downtime.

- \*Horizontal scaling\*: The AutoScalingGroup implements policies for scaling up or down based on CPU usage metrics of the nodes (implemented via CloudWatch Alarms).

- \*\*Database Read Replicas\*\*: The Mysql cluster has a master (writer) DB and also a read replica at this time.

- \*Vertical scaling\*: instances can be upgraded to larger memory/compute/storage capacities without downtime.

- \*Horizontal scaling\*: up to 15 read replicas can be added without downtime; to scale write operations partitioning would be an option.

- \*\*Networking infrastructure\*\*:

All networking (glue) components such as ELBs, ASGs,InternetGateway, VPC Router (and probably many more) are scaled-out by the AWS ecosystem.

## Availability considerations

- \*\*Web Cluster\*\*: Both the ASG and ELB instances which govern the web servers currently span over two Availability Zones\*\* (although probably all should be used).

- \*\*Database Cluster\*\*: AWS You also benefit from enhanced database availability when running Multi-AZ deployments. If an Availability Zone failure or DB Instance failure occurs, your availability impact is limited to the time automatic failover takes to complete: typically under one minute for Amazon Aurora and one to two minutes for other database engines (see the [RDS FAQ](http://aws.amazon.com/rds/faqs/#45) for details).

- \*\*DDoS by attack or failure\*\*: I tried as much as possible to avoid any SPoFs (single-point-of-failure) to keep this infrastructure robust and my intent was that DDoS attacks would either:

- be avoided; mostly by encapsulation (VPC, subnets, traffic rules etc.) or...

- translate to high loads which AWS can take without experiencing service outage; obviously this is still bad, but manageable.

## Monitoring and alerts

- The ELB for the web servers commits logs into an S3 Bucket (every 5 minutes).

- Following CloudWatch alarms are defined:

- \*\*Scaling up alarm\*\*: send email on ASG events (when CPU usage is over 70%).

- \*\*Scaling down alarm\*\*: send email on ASG events (when CPU usage is under 40%).

- \*\*Billing alarm\*\*: send email when costs exceed a threshold USD amount (1000).

- Alarms will notify the "OperationalEMail" address when triggered.

## Further improvements

The current state of the automation template reflects what I managed to build in the time I had available, and so there are a few aspects which could (and probably should) be improved before going live with it (note that some are more important than others):

- \*\*Add S3/CloudFront support for uploaded files\*\*: I intentionally did not use S3FS for storage and retrieval of uploaded files. I would definitely avoid this option if possible and use the AWS PHP SDK to write the files straight to S3. Here's why:

- Using a FS abstraction is more difficult to control and debug, errors are less likely to be visible and we can't enforce retries or other type of error handling.

- Reading those files would take them from S3, through the EC2 machines to the user; this complicates the architecture badly, will perform badly and denies use of CloudFront.

I've taken a look over the MyBB codebase and it should not be difficult to add support for S3 file uploads, which easily extends to support \*\*downloading files via CloudFront CDN\*\*. This would perform and scale better.

- Add \*\*CLoudWatch Alarms\*\* for:

- \*\*Abnormal Bandwidth usage\*\* (signs of attack);

- \*\*ELB latency\*\*;

- \*\*Database instance failures\*\*.

- Add \*\*CNAME parameter\*\* to the template so that the MyBB code will use the custom domain name instead of the public endpoint generated for the AWS balancer. The template outputs the "WWWBalancerDNSName" variable which is the public DNS-resolvable name to the main ELB instance;

this should be CNAME'd to a custom domain name or handled via Route53.

- Define \*\*Network ACLs\*\* for controlling traffic at subnet level; currently rules are enforced only by security groups.

- \*\*Remove Public IPs in PublicSubnets\*\*: Currently I set "MapPublicIpOnLaunch" to true on public subnets for a quick way to debug the launch configuration; a \*\*bastion\*\* server should be used.

- Define clear \*\*Stack update and delete policies\*\* to avoid downtimes during updates and to retain data (logs, databases etc.) after stack operations.

- \*\*Track CloudFormation calls via CloudTrail\*\*: For additional security and as a measure of historical reference, CloudTrail should be used to log all CloudFormation API calls into a selected S3 bucket. The benefit is good and the costs should be negligible.

- \*\*Restrict SSH access\*\*: By default the "SSHAllowedSources" parameter is set to "0.0.0.0/0" to allow any SSH connections to the nodes from any public IP address; this setting should be considerably more restrictive.

- Add \*\*parameter for MyBB Admin credentials\*\*; currently they are hardcoded (see "Evaluation access" section).

- \*\*Split template\*\* into separate stacks: (A) vpc, (B) web servers and (C) database; this would allow each stack to suffer updates and maintenance with less consequences to the other stacks; it would also make things more complex, of course.

- \*\*Tag everything\*\*.

- \*\*Custom AMI\*\* or \*\*make cloud-init scripts more private\*\* (S3 or CodeCommit): The automation template (along with the documentation) are revision-controlled on a public \*\*GitHub repository\*\*; this repository is also used (for simplicity) to host the \*cloud-init\* installation script for MyBB 1.8.6 (including MyBB sources). It would be preferable that this whole thing would be turned into a new AMI instance or at least the codes would be placed in a more controlled environment (S3 or CodeCommit).

- Use \*\*all Availability-Zones\*\* in the region; currently only two AZs are used.

- \*\*Outbound access for DB servers via NAT\*\*: It could be useful to allow outbound access to the Internet for the machines residing in the private subnet of the VPC (for updates and such) by using a \*\*NAT Gateway\*\*.

- Add an \*\*ElasticCache/Memcache\*\* deployment to improve performance.

- \*\*Time-based scaling\*\*: Currently, the Auto-Scaling Groups resize solely based on CloudWatch

performance metrics; rules for timed scaling could be defined to optimize costs.

- \*\*HTTPS support\*\*: For a production environment I would enable HTTPS support and even try to

force traffic through it (redirect "http://" traffic by HTTP 301 to "https://").

## That's it.

#### Thank you!