Contents

[1. Purpose 2](#_Toc512892200)

[2. Objective 2](#_Toc512892201)

[3. Recommendation 2](#_Toc512892202)

[4. Assumptions 2](#_Toc512892203)

[5. Logical Architecture Diagrams – Option 1 2](#_Toc512892204)

[6. Network Diagram – Option 1 3](#_Toc512892205)

[7. Architecture Description 3](#_Toc512892206)

[8. Alternative Architecture Diagram – Option 2 4](#_Toc512892207)

[9. Alternative Network Diagram – Option 2 4](#_Toc512892208)

[10. Alternative Architecture Description 5](#_Toc512892209)

[11. Security Considerations 5](#_Toc512892210)

[12. Other Architectures 5](#_Toc512892211)

[13. Cloudformation & Automation 6](#_Toc512892212)

[13.1. Logical Architecture Diagrams 6](#_Toc512892213)

[13.2. Architecture Description 6](#_Toc512892214)

[13.3. Automation 6](#_Toc512892215)

# Purpose

To document architecture and recommendations for wordpress site.

# Objective

To provide infrastructure architect to host a wordpress site with MySql database to support the site.

# Recommendation

Alternative architecture (Option 2) is better approach to implement the architecture to reduce security risk from the two options

# Assumptions

# Logical Architecture Diagrams – Option 1



# Network Diagram – Option 1



# Architecture Description

In the above architecture, webserver is place in public subnet while the DB server is placed in private subnet within the same VPC. A security group for webserver allows only SSH, HTTP and HTTPS traffic, while db server security only allows mysql/aurora and SSH traffic from the webserver only.

DB server has the ability to access outside VPC thru NAT gateway while the traffic from outside cannot reach db server. This will provide ability to maintain the server or download patches/software from outside the VPC.

Network ACLs for the webserver is restricted to only the three protocols that need to move in or out. For traffic into DB server is restricted to only webserver security group so no traffic will flow from elsewhere.

# Alternative Architecture Diagram – Option 2



# Alternative Network Diagram – Option 2



# Alternative Architecture Description

In the alternative architecture a bastion host is introduced into its own subnet which is restricted to only SSH traffic from outside, webserver will not allow SSH traffic from outside but will only from the bastion server.

Only bastion server can log into ec2 instances on webserver or db server.

# Security Considerations

Security is an important considered and needs to be kept in forefront on all architecture and design. The two architectures laid out in the document are predominantly different in terms of acceptance of security risk and standard an organization puts in place.

In the First Architecture, SSH traffic is coming into webserver which is potential issues

In the Second Architecture, SSH traffic from outside is only going to the bastion server and can jump from this host to other internal hosts.

# Other Architectures

* Bastion server can be placed in its VPC with public subnet and using VPC peering to access the other instance, while the Web traffic can go to into webserver.
* Instead of the creating DB server on EC2 an RDS can be created.

# Cloudformation & Automation

## Logical Architecture Diagrams



## Architecture Description

Database and webserver are installed on the same EC2 instance which is in a subnet inside a VPC. A Internet gateway is attached to the VPC with a route and a network ACL, Network ACL will allow in and out traffic for the following ports for http, SSH and ephemeral ports protocols.

Webserver and database is sitting behind a security group that controls the http, ssh protocols.

## Automation

I have automated the installation of webserver and mysql database and setting up the database by the provided parameters using shell scripting in the User data properties of the EC2 instance.