Virtual server based DMZ web service using VPC

Overview

In order to build web hosting infrastructure that provides a high level of availability and scalability in a legacy environment, it was necessary to install complex solutions. The capacity also had to be estimated according to peak times. This led to an increase in lead times and operating costs, which had a negative impact on service and profit margins.

Now, Samsung Cloud Platform provides web service infrastructure fast and only as much as needed based on customer-specific networks (**VPC**) that enable immediate Internet communications, highly scalable computing services, and security offerings for web services. This document introduces the architecture of a DMZ web service based on virtual servers using **VPC** in Samsung Cloud Platform.

Architecture Diagram

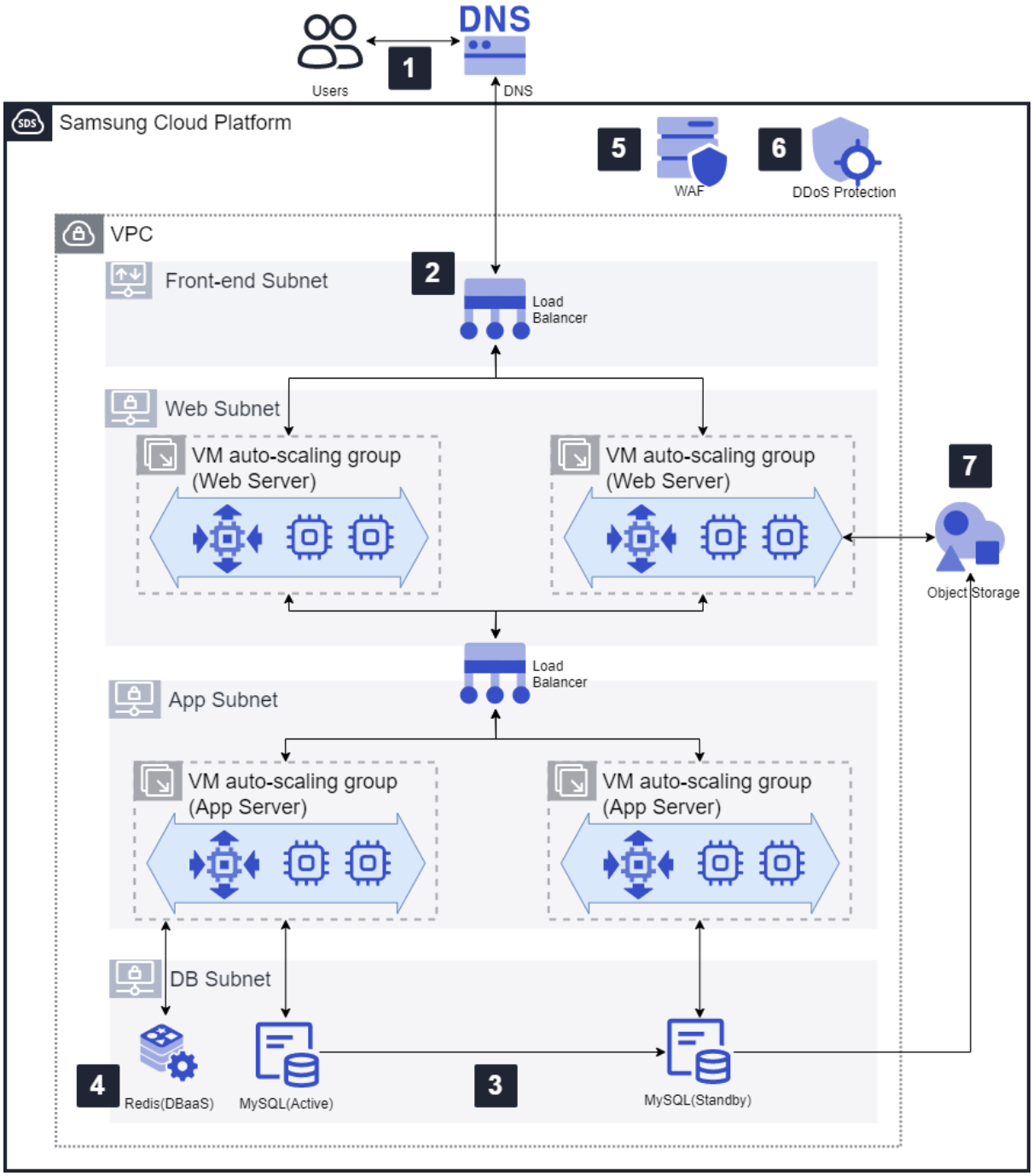

Figure 1. Example of DMZ web service architecture using Samsung Cloud Platform

1. In **DNS** service, set the domain name to be open externally and connected to the service IP of the **Load Balancer**. **Load Balancer** service IP is allocated in a **VPC** with Internet access.
2. **Load Balancer** improves service reliability by distributing web request traffic to multiple **VM Auto-Scaling** groups.

3. Relational databases need redundant configuration to increase availability. You can choose from 7 types of relational database engines.
4. You can reduce the response time of frequent requests by using the NoSQL database service as a cache of the relational database.
5. **WAF** service protects web servers from attack traffic such as XSS or SQL injection.
6. **DDoS Protection** service automatically responds to external DDoS attacks.
7. **Object Storage** can be used to store static contents such as images and videos, or for database backup purposes.

Use Cases

A. Providing public web services through **VPC**

Public web services can be configured through a public IP provided by **VPC**. With **DNS** service, you can easily register the domain name for the corresponding public IP.

B. Securing web security by applying security solutions and security group policies

In order to ensure the security of web servers open to the Internet, you can configure security solutions as a service. The **WAF** service monitors website traffic to detect and block attacks. The **DDoS Protection** service detects and blocks DDoS attacks that intensively flood traffic to web servers to disable the service. You can protect your infrastructure from external attacks by setting up security groups with minimal policies allowed.

Pre-requisites

None

Limitations

A service request is required when applying for **DDoS Protection** service and requesting policies.

Considerations

A. Security

When configuring the security policy, you can apply a separate security policy by separating the **Load Balancer** that requires direct access from the Internet and the security group for the internal infrastructure that does not require direct access.

You can control network access of unnecessary hosts by setting allow rules for each subnet in the **Firewall** service or for each virtual server in the **Security Group** service.

B. Serverless

In the future, you can consider a transition to a serverless web application using **Cloud Functions** service and **API Gateway** service.

Related Products

- VPC
- DNS
- Load Balancer
- Security Group
- Firewall
- Virtual Server
- VM Auto-Scaling
- MySQL(DBaaS)
- WAF
- DDoS Protection
- Object Storage
- Cloud Functions

Related Documents

- Web hosting