1.AWS Infrastructure Design Document

📘 AWS Infrastructure Design Document – English Version

Source:

🟦 1. Project Overview

Item	Details
Project Name	AWS Migration Project for SME Corporate Website
Author	Fuma
Created	2025/11/22
Version	v1.0

🎯 Purpose

Migrate the existing on-premise environment to AWS to improve **availability** and **maintainability**.

🧩 Background

The current on-premise servers suffer from:

- Hardware aging
- Unstable access
- Operational issues with backups

To address these risks, AWS is introduced to achieve **high availability** and **cost efficiency**.

🏁 Scope

- Web/DB environment build
- Data migration

- Monitoring configuration
- Backup design

👥 Intended Users

General public website for corporate customers and business partners.

💰 Target Cost

20,000–25,000 JPY/month

🟨 2. Requirements Definition

💻 Functional Requirements

- Public website hosting (HTTPS via ALB)
- Database (RDS MySQL)
- File storage (S3)
- Monitoring (CloudWatch)
- Log collection (CloudWatch Logs)

⚙️ Non-Functional Requirements

Category	Requirement
Availability	Multi-AZ configuration for both Web and DB layers
Cost	≤ 25,000 JPY per month
Scalability	Capable of introducing CI/CD in the future
Security	IAM least privilege, SG separation, TLS enabled

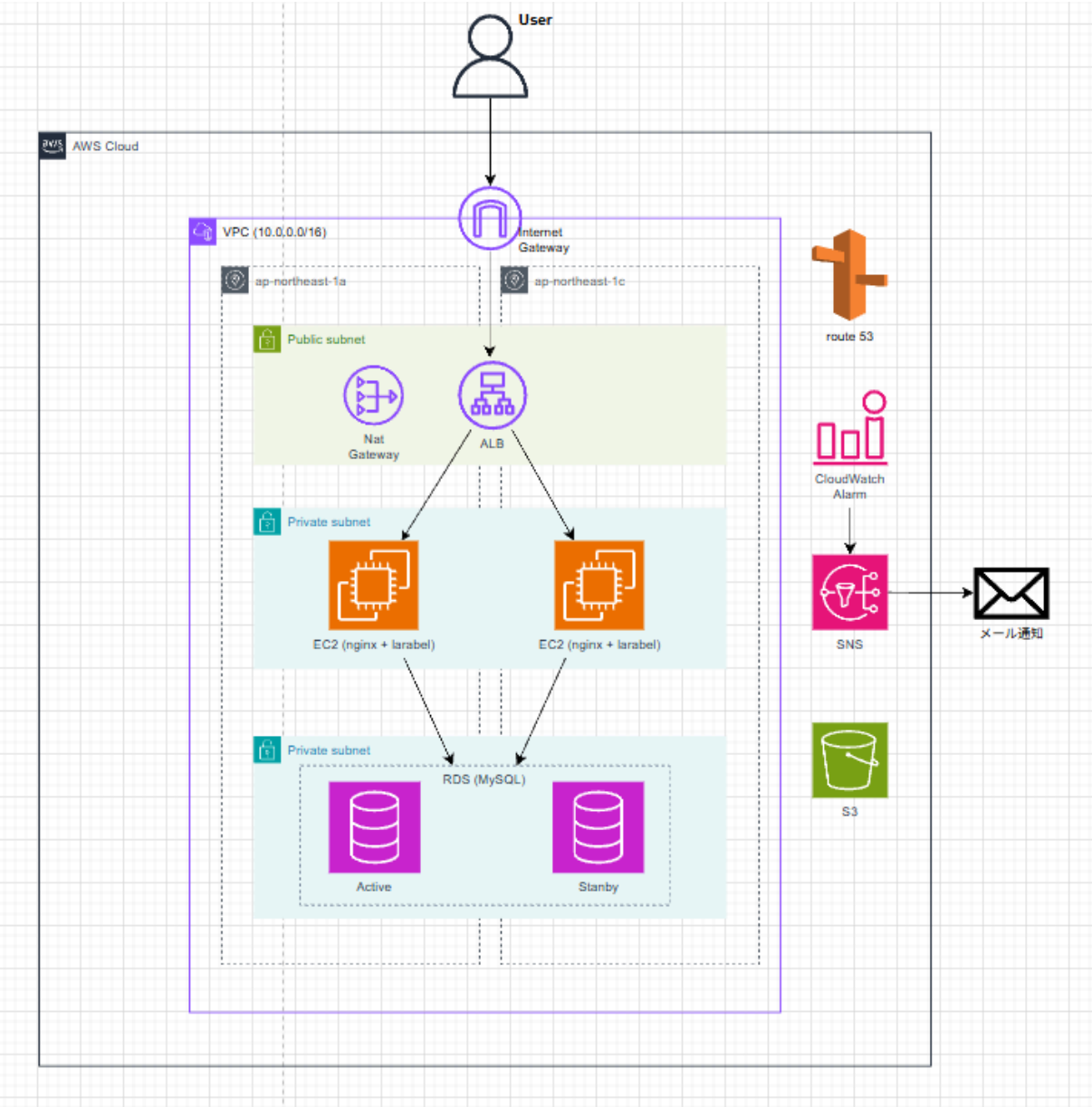
🟧 3. Client Confirmation Items (Assumed)

No	Question	Proposed Answer
1	S3 Versioning / Lifecycle policy?	Enable versioning, transition to IA after 90 days
2	Manual RDS snapshots needed?	Enable automated backups + propose manual snapshots as needed
3	OS & middleware patching method?	Manual updates, propose SSM Patch Manager
4	Range of log collection_	Metrics + Nginx/Laravel logs collected via CloudWatch
5	NAT Gateway redundancy required?	Single NATGW for cost efficiency, HA as optional proposal
6	CI/CD introduction plan?	Consider CodePipeline introduction in the future

🟨 4. System Architecture (Summary)

🧩 Architecture Components

- **VPC:** 10.10.0.0/16
- **Public Subnets:** ALB, NATGW
- **Private Subnets (App):** EC2 Web/AP
- **Private Subnets (DB):** RDS MySQL
- **Additional Services:** S3, Route53, CloudWatch



🟦 5. Detailed Architecture

5.1 VPC / Network Configuration

VPC

- **CIDR:** 10.10.0.0/16
- The network is segmented into Public, Private-App, and Private-DB layers.

Subnets

Layer	CIDR	Purpose
Public Subnet 1a	10.10.0.0/24	ALB, NAT Gateway
Public Subnet 1c	10.10.1.0/24	ALB, redundancy
Private-App 1a	10.10.10.0/24	EC2 Web/AP
Private-App 1c	10.10.11.0/24	EC2 redundancy
Private-DB 1a	10.10.20.0/24	RDS Primary
Private-DB 1c	10.10.21.0/24	RDS Standby

Routing

- Public Routes: 0.0.0.0/0 → Internet Gateway
- Private-App / DB Routes: 0.0.0.0/0 → NAT Gateway

Purpose

- Ensure **high availability**, **secure separation**, and **controlled outbound traffic**.

5.2 ALB Configuration

Key Points

- **Internet-facing ALB** deployed in Public Subnets.
- Handles HTTPS traffic with ACM certificate.
- HTTP → HTTPS automatic redirect.

Implemented Items

- Created ALB
- Created Target Group (HealthCheck path: `/`)
- Registered EC2 instances
- Set HTTPS listener (443)
- Configured redirect from HTTP (80)

5.3 EC2 Configuration

EC2 Instances

- **Amazon Linux 2023** × 2 (Private Subnets)
- **Purpose:** Web server + PHP application runtime

Installed Components

- git
- PHP-FPM
- Nginx
- mariadb client
- firewalld disabled for ALB use

Validation

- Nginx + PHP-FPM integration
- Web response test (Hello page)
- Yum update via NAT Gateway

5.4 RDS Configuration

RDS MySQL

- **Type:** db.t3.micro
- **Mode:** Multi-AZ
- **Storage:** General Purpose SSD
- **Subnet Group:** Private-DB 1a/1c
- **Parameter Groups:** Custom adjustments applied

Validation

- DB connectivity test (`mysql -h <endpoint> -u <user> -p`)
- Basic CRUD operations
- Failover behavior confirmed (auto-switching)

Backup

- Automated backup: **7 days**
- Encryption: Enabled

🟧 6. Security Configuration

6.1 Security Groups

ALB Security Group

Protocol	Port	Source
HTTPS	443	0.0.0.0/0
HTTP (redirect only)	80	0.0.0.0/0

EC2 Security Group

Protocol	Port	Source
HTTP	80	ALB SG
HTTPS	443	ALB SG
SSH	22	SSM only (no public access)

RDS SG

Protocol	Port	Source
MySQL	3306	EC2 SG

6.2 IAM

Principles Used

- **Least privilege**
- IAM Roles attached to:
  - EC2 (S3 + CloudWatch Logs access)
  - RDS monitoring

- ALB logging

SSM

- EC2 connected via **SSM Session Manager**, not SSH公開鍵
- Strengthens security and removes need for public IP

🟨 7. Monitoring & Logging Design

7.1 CloudWatch Metrics

EC2

- CPUUtilization (>80%)
- StatusCheckFailed
- NetworkIn/Out

RDS

- CPUUtilization
- FreeStorageSpace
- DatabaseConnections

ALB

- HTTP 5XX errors
- HealthyHostCount
- TargetResponseTime

7.2 CloudWatch Alarms + SNS

Alarms Configured

- EC2 CPU > 80% for 5 min
- RDS CPU > 80%
- ALB 5XX errors > threshold

- Unhealthy hosts detected

Notifications

- SNS email notifications
- Operation team notified on threshold breach

7.3 Logging

ALB Access Logs

- Stored in S3 bucket
- Lifecycle rules:
  - 30 days → Standard-IA
  - 90 days → Glacier

EC2 Logs

- Nginx access/error logs → CloudWatch Logs
- PHP-FPM logs → CloudWatch Logs

🟩 8. Cost Estimation

Monthly AWS Cost

Service	Monthly Cost (USD)
EC2 ×2	19.86 × 2 = **39.72**
RDS (Multi-AZ)	**43.48**
NAT Gateway	**45.26**
ALB	**17.97**
S3	**1.25**
Route53	**0.80**
CloudWatch	**1.50**
Total	**149.98 USD / month**

Annual Cost

- **1,799.76 USD / year**

🟪 9. Cost Optimization Proposals

Item	Current	Improvement	Expected Reduction
NAT Gateway	45.26 USD	Switch to SSM-only access	**−45 USD**
RDS	Multi-AZ	Single-AZ (if allowed)	**−20〜25 USD**
EC2	2 units	Min=1, Max=2 AutoScaling	**−20 USD**
ALB	17.97 USD	Stop during low-traffic	**−5〜10 USD**

Optimized Total

50〜70 USD/month possible for dev/staging.

🟫 10. Operations Design

Backup

- RDS automated backup: 7 days
- Manual snapshots before major changes
- S3 versioning enabled

Patching

- EC2: Manual yum update
- RDS: Auto minor version upgrades
- Optional: SSM Patch Manager

Deployment

- Current: Manual (git pull)
- Future proposal:
  - CodePipeline
  - CodeBuild
  - Blue/Green deployment

Monitoring Process

- Receive SNS notifications
- Check CloudWatch dashboard
- Investigate EC2/RDS metrics
- Check ALB logs in S3 if needed

🟧 11. Risk Management

Identified Risks

1. NAT Gateway cost spikes
2. ALB access log cost accumulation
3. Increasing DB connections
4. EC2 high CPU
5. Security misconfiguration

Mitigation

- Cost alarms
- Limit access logs retention
- AutoScaling plan
- Security Group review
- SSM-only policy

🟨 12. Future Improvements

- Introduce CI/CD pipelines
- IaC using Terraform or CloudFormation
- WAF introduction
- AutoScaling Group for EC2
- RDS Proxy for performance

- Improved monitoring dashboards

🟦 13. Summary

- Fully built **high-availability 3-tier architecture**
- Suitable for small–medium corporate websites
- Includes ALB, EC2, RDS Multi-AZ, NATGW, S3, Route53, CloudWatch
- Cost: **149.98 USD/month** (optimized to 50〜70 USD possible)
- Documentation + monitoring + operations design complete
- Ready for real-world production deployment