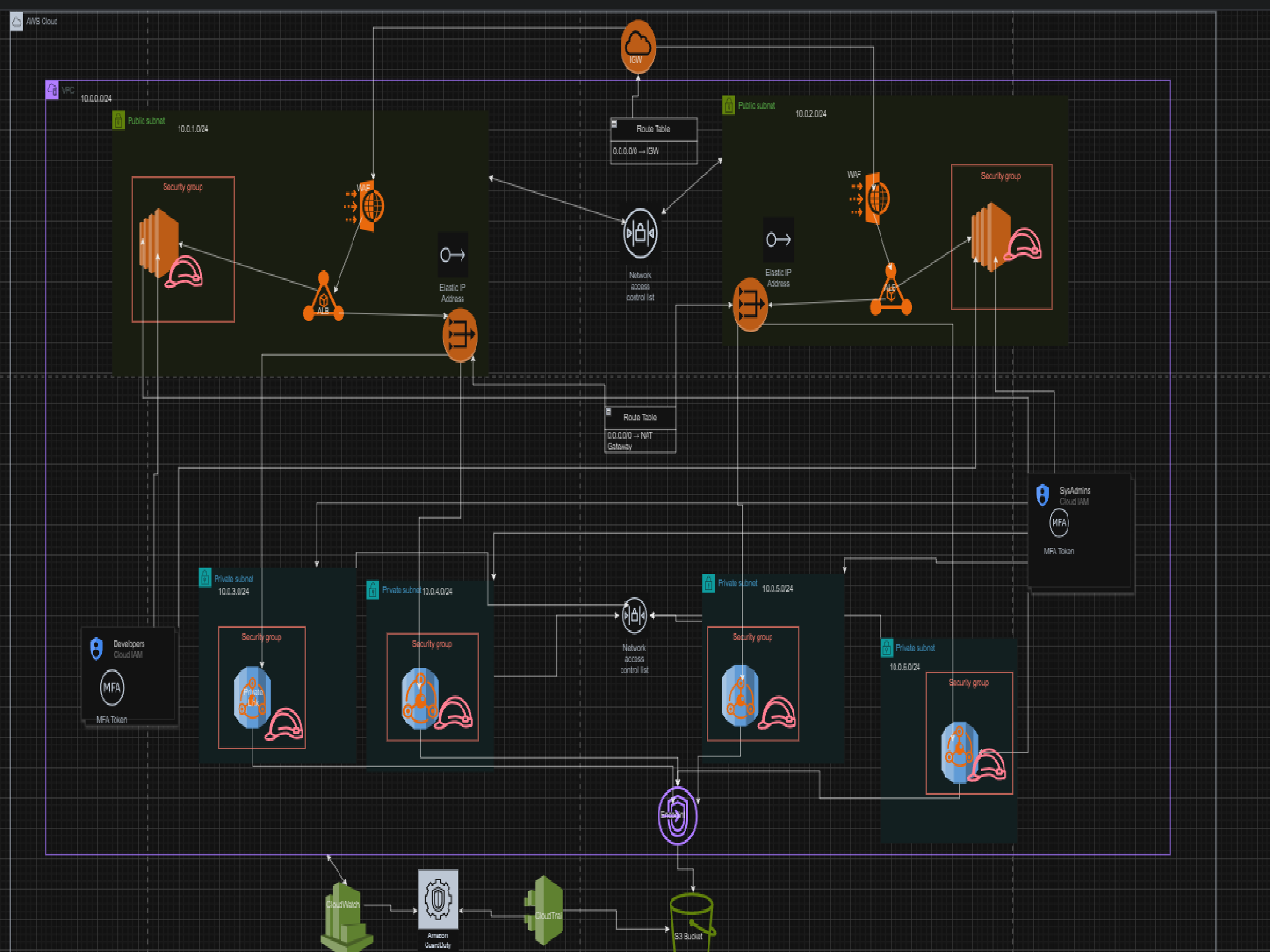
Secure AWS Environment

By: Chance Debbs

Summary

The goal of this project is to design and implement a secure and scalable cloud infrastructure on AWS. The architecture is designed to provide a reliable platform for hosting applications and services, ensuring that workloads are protected against threats while maintaining the flexibility to grow and adapt as demand increases. By leveraging AWS's global infrastructure, this project aims to show an environment that balances performance and operational efficiency.


AWS Cloud
VPC
10.0.0.0/24
Public subnet
10.0.1.0/24
Security group
WAF
ALB
Elastic IP Address
IGW
Route Table
0.0.0.0/0 → IGW
Network access control list
Public subnet
10.0.2.0/24
WAF
Elastic IP Address
ALB
Security group
Route Table
0.0.0.0/0 → NAT Gateway
SysAdmins
Cloud IAM
MFA
MFA Token
Developers
Cloud IAM
MFA
MFA Token
Private subnet
10.0.3.0/24
Security group
Private link
Private subnet
10.0.4.0/24
Security group
Network access control list
Private subnet
10.0.5.0/24
Security group
Private subnet
10.0.6.0/24
Security group
CloudWatch
Amazon GuardDuty
CloudTrail
S3 Bucket

Security

- **NACLs**:
  - Public Subnet: Allows HTTP/HTTPS traffic and restricted SSH.
  - Private Subnet: Allows traffic only from the public subnet.
- **Security Groups**:
  - Web Server: Allows inbound HTTP/HTTPS and restricted SSH.
  - Database: Allows inbound traffic only from the web server.
- **Web Application Firewall (WAF)**:
  - Protects the ALB from SQL injection and other web exploits.

Extra Security

Database Isolation:

Private RDS instances are not directly accessible from the internet.

Encryption:

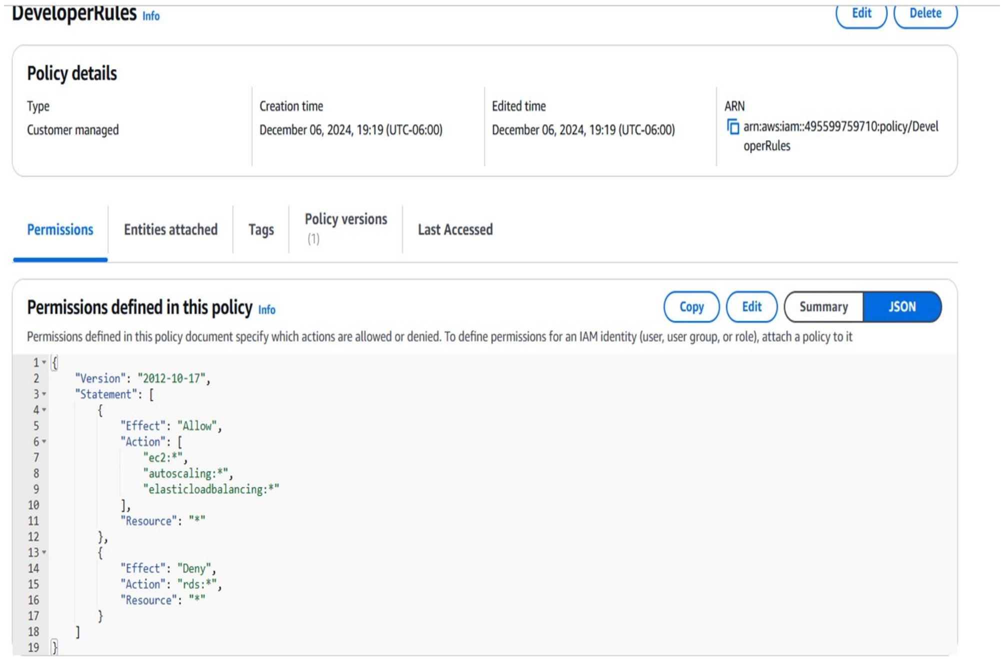
Data in transit is secured using HTTPS with TLS.

MFA:

Enforced developers and system admins to access the AWS environment.

IAM Roles and Policies

- IAM Roles were created to ensure secure and restricted access:
- - Developer: Access to EC2 only.
- - SysAdmin: Full access to EC2 and RDS.



DeveloperRules Info

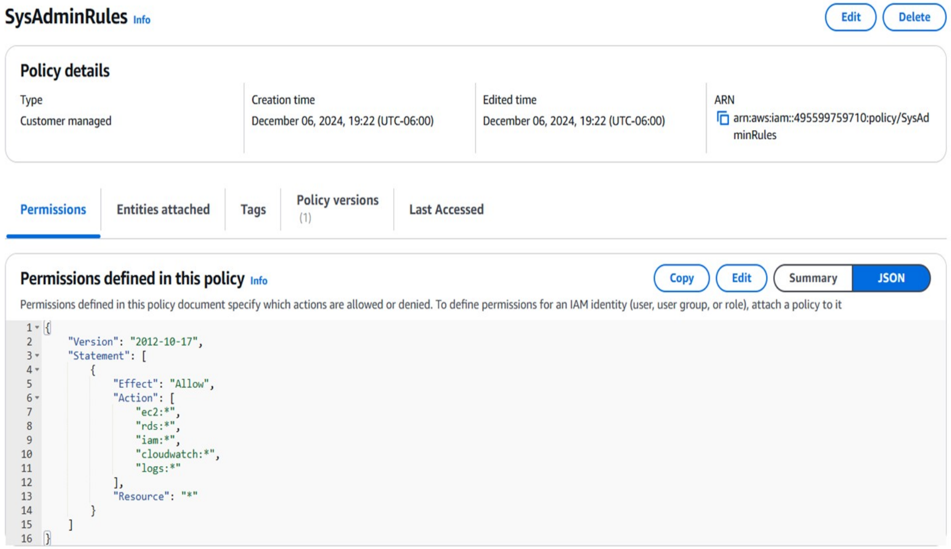
Policy details

Type	Creation time	Edited time	ARN
Customer managed	December 06, 2024, 19:19 (UTC-06:00)	December 06, 2024, 19:19 (UTC-06:00)	arn:aws:iam::495599759710:policy/DeveloperRules

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "autoscaling:*",
                "elasticloadbalancing:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "rds:*",
            "Resource": "*"
        }
    ]
}
```



SysAdminRules Info

Policy details

Type	Creation time	Edited time	ARN
Customer managed	December 06, 2024, 19:22 (UTC-06:00)	December 06, 2024, 19:22 (UTC-06:00)	arn:aws:iam::495599759710:policy/SysAdminRules

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "rds:*",
                "iam:*",
                "cloudwatch:*",
                "logs:*"
            ],
            "Resource": "*"
        }
    ]
}
```

PrivateLinks

Purpose:

- Enables secure, private access to RDS from resources within the VPC or external accounts.

Placement:

- PrivateLink is inside the private subnet associated with the RDS instance.

Benefits:

- Eliminates the need for public internet exposure.
- Ensures traffic between RDS and applications stays within the AWS network.

Monitoring and Logging

S3 Bucket:

- Stores CloudTrail logs securely with server-side encryption.

CloudWatch:

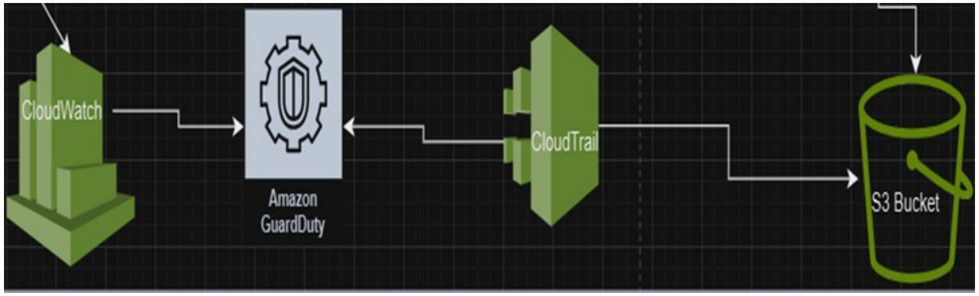
- Monitors EC2 instance performance, application logs, and system metrics.
- Configured alerts for anomalies and downtime.

CloudTrail:

- Captures all API activity and sends logs to an S3 bucket

Amazon Guard Duty:

- monitors for malicious activity or unauthorized behavior across your AWS environment by analyzing data from CloudTrail,



Elastic IP Address

- Used to provide static, public IP addresses for resources hosted in the public subnets.
- This ensures that the public IP address remains the same even if an instance or service is replaced or restarted.

VPC Endpoint

- VPC endpoint provides a secure and private connection between resources.
- eliminates the need for internet-based communication, ensuring data transfer remains with the AWS.
- Enhances security, reduces latency, and lowers data transfer costs.

NAT Gateway

- The NAT Gateway allows private subnets to securely access the internet for updates without exposing them directly. Configured with an Elastic IP for public communication.