RETO TÉCNICO

NIGHTWATCH

Javier Almeida

RECURSOS IMPLEMENTADOS EN AWS

- VPC
- SECURITY GROUPS
- IAM ROLE
- EC2
- S3

AWS VPC

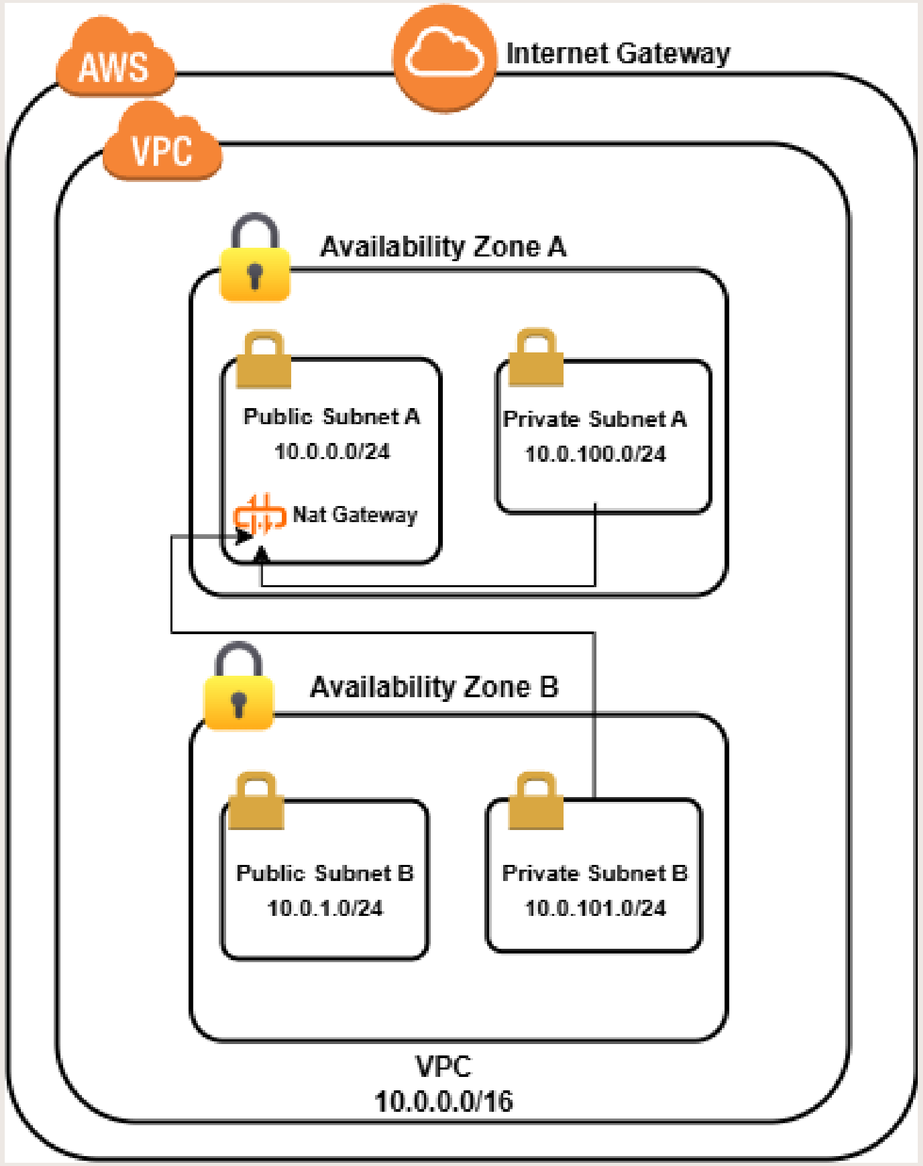
VPC_CIDR: 10.0.0.0/16. Rango amplio de direcciones IP privadas que permite el despliegue de múltiples recursos dentro de una infraestructura escalable.

Internet Gateway (IGW): Permite que las instancias en las subnets públicas tengan acceso directo a internet.

Nat Gateway (NGW): Facilita el acceso a internet para las instancias en subnets privadas sin exponerlas directamente, ubicado en una subnet pública y asociado a una Elastic IP.

Subnets públicas y privadas (2 de cada una): Separación lógica de recursos con alta disponibilidad, permitiendo escalar y distribuir servicios públicos y privados entre distintas zonas de disponibilidad.

Route Tables: Configuradas para enrutar el tráfico de internet desde las subnets públicas hacia el IGW, y desde las privadas hacia el NGW.



SECURITY GROUPS

PUBLIC_SG:

Grupo de seguridad diseñado para ser asociado a una Instancia EC2 pública. Permite el acceso entrante (ingress) desde internet por los siguientes puertos:

- **Puerto 22 (SSH)**: para conexión remota a la instancia.
- **Puerto 3000 (Grafana)**: dashboard de monitoreo.
- **Puerto 31080 (Prometheus)**: recopilación y visualización de métricas.
- **Puerto 30080 (Nginx)**: acceso al servidor web.

PRIVATE_SG:

Grupo de seguridad diseñado para ser asociado a una Instancia EC2 privada. Permite el acceso entrante (ingress) desde las ips asignadas por el `public_sg` por los siguientes puertos:

- **Puerto 22 (SSH)**: habilita acceso remoto desde la instancia pública (bastion host) hacia la instancia privada mediante túnel SSH.
- **Puerto 5432 (PostgreSQL)**: Permite la conexión a la base de datos de PostgreSQL a través de la Instancia pública.

IAM ROLE

Se crea un IAM Role llamado **grafana-ec2-role**
con el propósito de otorgar al servidor de Grafana los permisos necesarios para acceder a recursos de AWS.

Este rol permite:

- Recolectar métricas desde CloudWatch
- Obtener logs y eventos de los grupos de logs
- Enviar estos datos a S3 como parte del sistema de logging

Permisos utilizados:

CloudWatch (métricas):

- cloudwatch:DescribeAlarms
- cloudwatch:GetMetricData
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics

CloudWatch Logs:

- logs:DescribeLogGroups
- logs:GetLogEvents
- logs:DescribeLogStreams
- logs:FilterLogEvents

```
resource "aws_iam_role_policy" "grafana_full_policy" {
  name = "grafana-full-policy"
  role = aws_iam_role.grafana_ec2_role.id

  policy = jsonencode({
    Version = "2012-10-17",
    Statement = [
      {
        Effect = "Allow",
        Action = [
          "cloudwatch:DescribeAlarms",
          "cloudwatch:GetMetricData",
          "cloudwatch:GetMetricStatistics",
          "cloudwatch:ListMetrics"
        ],
        Resource = "*"
      },
      {
        Effect = "Allow",
        Action = [
          "s3:PutObject",
          "s3:GetObject",
          "s3:ListBucket"
        ],
        Resource = [
          "arn:aws:s3:::*",
          "arn:aws:s3:::*/*"
        ]
      },
      {
        Effect = "Allow",
        Action = [
          "logs:DescribeLogGroups",
          "logs:GetLogEvents",
          "logs:DescribeLogStreams",
          "logs:FilterLogEvents"
        ],
        Resource = "*"
      }
    ]
  })
}
```

AWS EC2

EC2 PÚBLICA:

La instancia EC2 pública fue creada con el tipo **t3.small**, con el objetivo de contar con los recursos necesarios para soportar los distintos servicios desplegados. Esta instancia cumple múltiples funciones, entre ellas la de bastion host para acceder de forma segura a la instancia privada.
Servicios y componentes alojados:

- **Paquetes instalados**: Python, Docker, K3s, cronie, nc, bind-utils, postgreSQL17
- **Servidor de Grafana** ejecutándose en contenedor Docker
- **Servidores de Nginx y Prometheus** desplegados dentro de **K3s** (Kubernetes ligero)
- **Sistema de logs** automatizado mediante scripts en **Bash** y **Python**, programados para ejecutarse diariamente a través de cronie (crontab)
- **Acceso remoto a la instancia privada** para tareas de administración o monitoreo

EC2 PRIVADA:

La instancia EC2 privada está dedicada a alojar el servidor de base de datos **PostgreSQL**. Se encuentra en una subred privada, sin acceso directo desde internet (utiliza el natgateway), y solo es accesible a través de la instancia pública (**bastion host**), lo que aumenta la seguridad del entorno.
Componentes y configuraciones:

- **PostgreSQL** ejecutándose en contenedor **Docker**
- **Paquetes instalados**: Docker, PostgreSQL
- **Acceso restringido** a través de **grupos de seguridad** que permiten conexiones únicamente desde la instancia pública

AWS S3

Se crea un bucket en Amazon S3 con el objetivo de proporcionar un espacio de almacenamiento confiable y escalable donde se guardarán los logs y respaldos generados por los scripts automatizados desde las instancias EC2.

Características y funcionalidades:

- Destino de backups diarios del servidor PostgreSQL (archivo .sql.gz)
- Almacenamiento de métricas y logs recolectados desde CloudWatch por el servidor de Grafana
- Acceso controlado mediante políticas de IAM asociadas al rol grafana-ec2-role
- Organización de los archivos por fecha para facilitar su consulta y trazabilidad