**AWS CloudFormation Documentation: Fully Featured VPC with Monitoring & Scheduling**

**Overview**

This CloudFormation template provisions a fully-featured **Virtual Private Cloud (VPC)** with public and private subnets, security groups, auto-scaling, monitoring, and scheduling. It includes built-in **alerting, flow logs, and NAT Gateway** for private subnet access.

**Features & Components**

**1. VPC and Subnets**

* **VPC:** Creates a VPC with CIDR 10.0.0.0/16, enabling DNS support.
* **Public Subnet:** 10.0.1.0/24 with public IP mapping.
* **Private Subnet:** 10.0.2.0/24 for internal workloads.

**2. Internet & NAT Gateway**

* **Internet Gateway (IGW):** Attaches to the VPC to enable public internet access.
* **NAT Gateway:** Allows private subnet instances to access the internet securely.

**3. Security Groups**

* **Public Security Group:** Allows HTTP/HTTPS traffic from anywhere (0.0.0.0/0).
* **Private Security Group:** Allows SSH (22) access only from an admin-defined IP.

**4. Routing Configuration**

* **Public Route Table:** Routes traffic through the Internet Gateway.
* **Private Route Table:** Routes traffic through the NAT Gateway for outbound access.

**5. Auto Scaling Group & EC2 Instances**

* **Launch Configuration:** Defines EC2 instances with t2.micro instance type.
* **Auto Scaling Group:**
  + Minimum instances: 1
  + Maximum instances: 5
  + Desired capacity: 2

**6. Monitoring & Logging**

* **VPC Flow Logs:** Captures traffic data and stores logs in CloudWatch.
* **CloudWatch & SNS Alerts:**
  + SNS topic is created for monitoring notifications.
  + Auto-scaling events (launch, terminate) trigger alerts.

**7. Scheduling Support**

* Parameters for **VPC Start & Stop Time** (VPCStartHour, VPCEndHour).
* Future integration with **AWS Lambda & CloudWatch Events** for automation.

**Parameters**

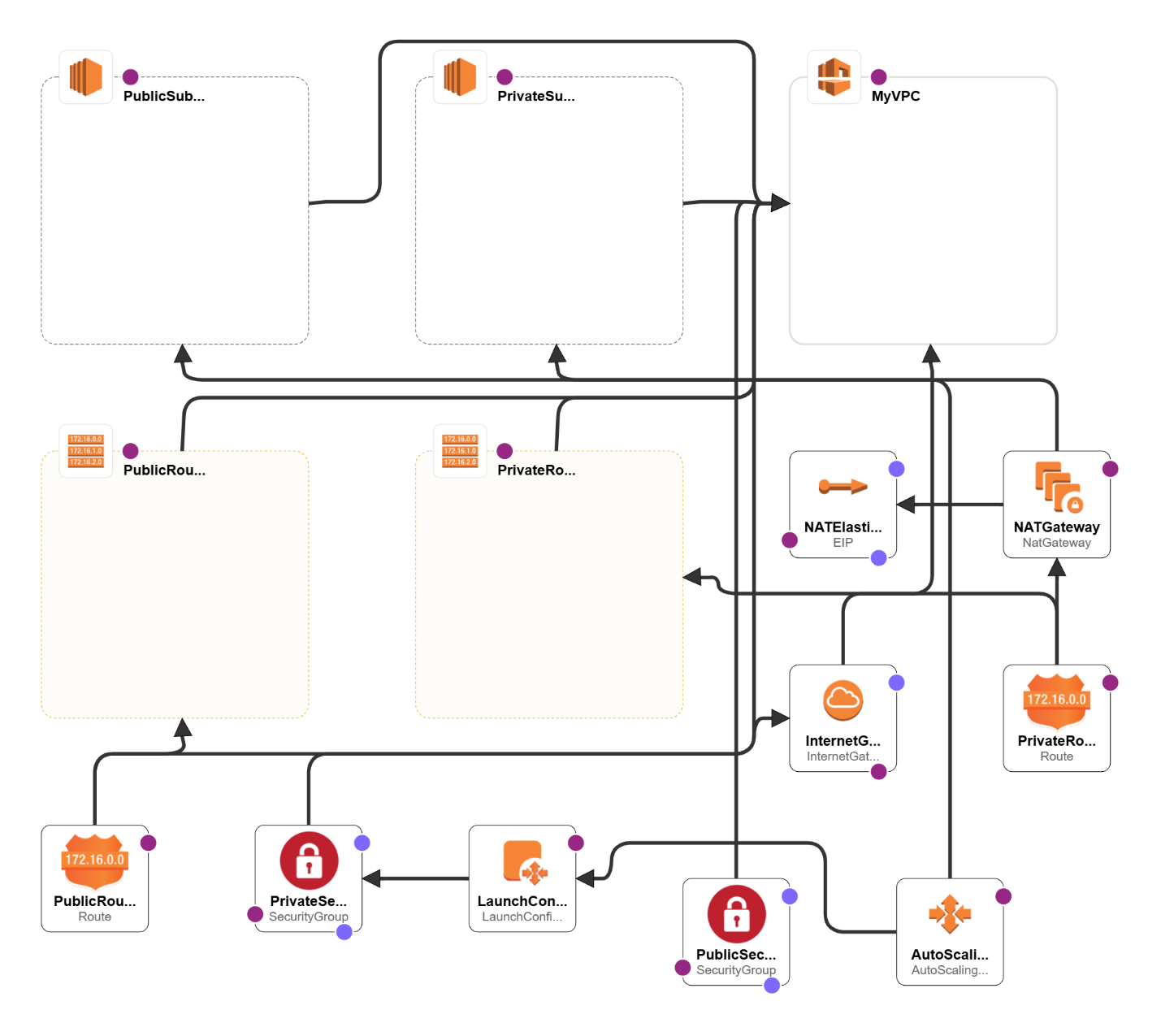
|  |  |  |
| --- | --- | --- |
| **Parameter** | **Description** | **Default** |
| VPCStartHour | Hour to start the VPC (24-hour format) | 9 |
| VPCEndHour | Hour to stop the VPC | 18 |
| AdminIP | Allowed admin IP for SSH | 0.0.0.0/0 |
| InstanceType | EC2 instance type | t2.micro |
| KeyPairName | SSH Key Pair Name | "" |
| AlertEmail | Email for monitoring alerts | Required |

**IAM Roles & Policies**

* **VPC Flow Logs IAM Role**
  + Allows logs:CreateLogStream and logs:PutLogEvents to store logs in CloudWatch.
* **Auto Scaling Notification Permissions**
  + Sends SNS alerts for scaling activities.

**Resources Created**

|  |  |
| --- | --- |
| Resource | Type |
| VPC | AWS::EC2::VPC |
| Public & Private Subnets | AWS::EC2::Subnet |
| Internet Gateway | AWS::EC2::InternetGateway |
| NAT Gateway | AWS::EC2::NatGateway |
| Security Groups | AWS::EC2::SecurityGroup |
| Auto Scaling Group | AWS::AutoScaling::AutoScalingGroup |
| VPC Flow Logs | AWS::EC2::FlowLog |
| SNS Topic | AWS::SNS::Topic |



**Future Enhancements**

✅ **Instance Scheduling Automation**: Use AWS Lambda + CloudWatch to stop/start EC2 based on VPCStartHour & VPCEndHour. ✅ **Application Load Balancer (ALB)**: Add an ALB for better load distribution. ✅ **CloudWatch Alarms**: Attach alarms for CPU usage, instance health, and networking issues. ✅ **RDS Integration**: Extend this template to include an Amazon RDS database.

**Outputs**

|  |  |
| --- | --- |
| Output | Description |
| SNSTopicArn | ARN of the SNS Topic for monitoring alerts |
| VPCId | ID of the created VPC |
| PublicSubnetId | ID of the Public Subnet |
| PrivateSubnetId | ID of the Private Subnet |

**Deployment Instructions**

1. Navigate to the **AWS CloudFormation Console**.
2. Click on **Create Stack** > **With new resources**.
3. Upload the CloudFormation YAML file.
4. Enter the **required parameters** (AlertEmail, KeyPair, etc.).
5. Click **Next** and then **Create Stack**.
6. Wait for the deployment to complete (~5 minutes).
7. Monitor resources in **AWS Management Console**.

**Conclusion**

This CloudFormation template provides a **scalable, secure, and automated VPC environment** with monitoring and scheduling capabilities. Future enhancements can include **ALB, RDS, and automation scripts** for cost optimization and better workload management.