AWS EC2 Security Group Update

Standard Operating Procedure (SOP)

Overview

This SOP outlines the process for programmatically updating an EC2 Security Group using Python. It includes the steps for adding or removing inbound/outbound rules and ensuring t hat the security group is configured correctly for the desired access.

Platform

AWS

Code Language

Python

Required Dependencies

- boto3
- AWS SDK for Python

Credentials Required

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_REGION

Input Parameters

1. instance_id
    - Type: String
    - Description: The EC2 instance ID to associated with the Internet gateway.
    - Required: true
    - Default: null
    - Validation Rules: Must be a valid instance ID.

2. cidr_block
    - type: string

- description: The CIDR block to allow traffic from (e.g., 0.0.0.0/0 for all IPs)
- required: true
- default: none
- validation rules: Must be in valid CIDR format (e.g., 0.0.0.0/0 for all IPs)

3. region
    - type: string
    - description: region associated with ec2 route table
    - required: true
    - default: null

Logic Flow

1. Pre-Creation Validation

    - Validate AWS credentials
    - Validate EC2 instance ID
    - Validate Security Group ID
    - Validate Protocol and Port Range
        - Ensure the provided protocol is valid (tcp, udp, icmp), and the port range is within the acceptable range (e.g., 0-65535 for TCP/UDP).
    - Validate Rule Actions and Directions
        - Ensure that the rule action (allow or deny) and direction (inbound or outbound) are specified correctly.
    - Validate CIDR Block
        - Ensure that the CIDR block is valid (e.g., 0.0.0.0/0 for all IPs).

2. Post-Creation Configuration

    - Verify Route Addition
    - Log Action

3. Error Handling Scenarios

    - Invalid Security Group ID
    - Invalid Protocol/Port Range
    - Invalid CIDR Block
    - Insufficient Permissions

Success Criteria

- The security group is successfully updated with the specified rule.
- The rule appears in the security group's list of inbound or outbound rules.
- Action is logged for auditing purposes.

Monitoring Considerations

- Verify Route Addition
- Audit Logs
- Monitor Security Group Metrics

Tags

- aws
- security-group
- security
- networking
- ec2