AWS EC2 Security Group Update

Standard Operating Procedure (SOP)

Overview

This SOP outlines the process for programmatically updating an EC2 Security Group by establishing port
80 using Python. It includes the steps for adding or removing inbound/outbound rules and e nsuring that 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: i-046f7716bf623f91f
    - Validation Rules: Must be a valid instance ID.

2. region
    - type: string
    - description: region associated with ec2 route table
    - required: true
    - default: us-east-1

3. security_group_id
    - type: string
    - description: The security group ID associated with the EC2 instance
    - required: true
    - default: sg-03ebb2cfca10fa9f2

Logic Flow

1. Pre-Creation Validation

    - Validate AWS credentials
    - Validate EC2 instance ID
    - Validate Security Group ID

2. Post-Creation Configuration

    - Verify Route Addition

3. Error Handling Scenarios

    - Invalid instance ID
    - Insufficient Permissions

4. Logic Explanation

    - Modify the inbound rule of the EC2 security group to allow custom TCP traffic on port 80 using Boto3, ensuring proper confirmation messages at each step. Update the corresponding records in ServiceNow via the ServiceNow API, logging each operation's output using print statements. Implement robust exception handling with appropriate raise statements to manage errors effectively.

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