AWS Network ACL(NACL) Inbound Rule Update

Standard Operating Procedure (SOP)

Overview

This SOP outlines the process for programmatically allowing a specific inbound rule (Rule No. 100) in a Network Access Control List (NACL) on AWS using Python.

2. 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. **network_acl_id**
   Type: String
   Description:The unique ID of the Network Access Control List (NACL)
   Required:true
   Default:null

   Validation Rules**:**
   - Must be a valid NACL ID (e.g., acl-xxxxxxxx).

2. **rule_number**
   Type: Integer
   Description:The rule number (in this case, Rule No. 100)

Required:true
Default:100

Validation Rules:

- Integer value between 1 and 32766

Logic Flow

1. Pre-Creation Validation

    - Validate AWS credentials
    - Validate NACL ID
    - Validate Rule Number
    - Validate CIDR Block
    - Validate Traffic Direction (Inbound/Outbound)

2. Post-Creation Configuration

    - Verify Rule Application
    - Log Action

3. Error Handling Scenarios

    - Invalid NACL ID
    - Invalid Rule Number
    - Invalid CIDR Block
    - Insufficient Permissions

Success Criteria

- Rule No. 100 is successfully applied to the NACL for inbound traffic.
- CIDR block is configured correctly.
- Action is logged for auditing purposes.
- Rule appears in the NACL's inbound rules list.

Monitoring Considerations

- Verify Rule Addition
- Audit Logs
- Monitor NACL Metrics

Tags

- Aws
- Nacl
- Security
- networking