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.

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: acl-04693d8452e77de5a
2. rule_number
    - Type: Integer
    - Description:The rule number (in this case, Rule No. 100)
    - Required:true
    - Default:100

Logic Flow

1. Pre-Creation Validation
    - Validate AWS credentials
    - Validate NACL ID
    - Validate Rule Number
2. Post-Creation Configuration
    - Verify Rule Application
3. Error Handling Scenarios
    - Invalid NACL ID
    - Insufficient Permissions

Success Criteria

- Rule No. 100 is successfully applied to the NACL for inbound traffic.
- 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