Runbook for SSM Run Command Project

Objective:

This project will guide you through using AWS Systems Manager (SSM) Run Command to automate configuration and validation of EC2 instances. The project involves creating an S3 bucket, uploading scripts, setting up SNS for notifications, and using SSM to execute scripts on EC2 instances.

Scenario and Solution Implementation

Scenario:

Imagine you are working for a client who has recently moved their infrastructure to AWS. They have multiple EC2 instances running various applications. However, they face challenges with inconsistent configurations and lack of automated validation, leading to frequent issues and manual intervention.

Your task is to automate the configuration and validation of these EC2 instances using AWS Systems Manager (SSM) Run Command. You will use scripts to ensure consistent configurations across instances, validate the setups, and provide automated reports.

Solution Steps:

A. Download and Review the Script

1. **Download `S3_insanitycheck.sh`** and open it in a text editor to understand its functionality.
2. **Script Breakdown**:
    - Collects system details.
    - Validates specific configurations like SELinux status, NFS mounts, McAfee installation, etc.
    - Outputs results to a log file.

B. Create AWS Resources : Run the below command to create the necessary resources from the CLI or you can create them manually from the console

1. **Create an S3 Bucket**:

```
aws s3 mb s3://<your-bucket-name>
```

2. **Upload the Script to S3**:

```
aws s3 cp /path/to/S3_insanitycheck.sh s3://<your-bucket-name>/
```

3. **Create a Folder in the S3 Bucket**:

```
aws s3api put-object --bucket <your-bucket-name> --key log/
```

4. **Create an SNS Topic**:

```
aws sns create-topic --name <your-topic-name>
```

   - Copy the topic ARN and update the `ssm-runcommand-doc.json` file.

5. **Subscribe to the SNS Topic**:

```
aws sns subscribe --topic-arn <your-topic-arn> --protocol email
--notification-endpoint <your-email@example.com>
```

C. Set Up IAM Role for EC2

1. **Create an IAM Role with Policies**:
   - Attach policies: `AmazonSSMFullAccess`, `AmazonS3FullAccess`, and `AmazonSNSFullAccess` (`or admin Access for demo purposes`)
   -
2. **Launch EC2 Instances**:
   - Launch two Amazon Linux 2 instances with the IAM role attached.
   - Tag instances with `Name: Webservers`.

D. Create and Execute SSM Document

1. **Create SSM Run Command Document**:
   - Go to AWS Systems Manager Console.
   - Navigate to `Shared Resources> Documents` > `Create Document`.
   - select `Command or Session`
   - Name the document `EC2InsanityDemoCheck` and leave Target type `empty or` specify the resource type as `EC2`.
   - Copy the content of shared `ssm-runcommand-doc.json` into the content JSON editor. Replace the default content
   - Click on `Create document`

2. **Update the JSON Document (if not done already)**:
   - Replace placeholders with your S3 bucket name, script path, and SNS topic ARN.
3. **Execute the Run Command**:
   - Use the SSM console to run the command on the tagged EC2 instances.
   - Monitor the command output and check the log files in the S3 bucket.

E. Validate the Setup

1. **Check Log Files**: Ensure logs are correctly uploaded to the S3 bucket.
2. **SNS Notifications**: Verify you receive notifications via email.