AWS Free Tier Setup and Alerting

This guide walks you through setting up a Free Tier AWS account, configuring CloudTrail, setting up SNS for email alerts, and configuring EventBridge to trigger on the GetCallerIdentity API call made by the root user. It also includes instructions on how to test everything via the command line.

1. Set Up a Free Tier AWS Account

Create an AWS Account:

- Go to aws.amazon.com.
- Click "Create an AWS Account".
- Enter your Email Address, Password, and AWS Account Name.
- Click "Continue".

Provide Contact Information:

- Select "Personal" for account type.
- Fill in your Full Name, Phone Number, Country/Region, and Address.
- Accept the AWS Customer Agreement and click "Create Account and Continue".

Payment Information:

- Enter your Credit/Debit Card details.
- Click "Verify and Add". AWS may place a temporary hold (usually $1) for verification.

Identity Verification:

- Choose "Text Message (SMS)" or "Voice Call" for verification.
- Enter your phone number and complete the verification process.

Select a Support Plan:

- Choose "Basic Support – Free".
- Click "Complete Sign Up".

Sign In to the AWS Management Console:

- Go to aws.amazon.com and click "Sign In to the Console".
- Enter your credentials.

2. Set Up SNS to Send Email Alerts

Navigate to SNS:

- In the AWS Management Console, search for "SNS".

Create an SNS Topic:

- Click on "Topics".
- Click "Create topic".
- Type: Choose "Standard".
- Name: Enter a name (e.g., **APICallAlert**).
- Click "Create topic".

Subscribe to the SNS Topic:

- Click on the topic you just created.
- Click "Create subscription".

- Protocol: Select "Email".
- Endpoint: Enter your email address.
- Click "Create subscription".
- Check your email inbox for a confirmation email and click the "Confirm subscription" link.

Enable SNS Notification in CloudTrail:

- Go back to CloudTrail.
- Select your trail and click "Edit" in the "Trail settings" section.
- Scroll to the SNS section, select your SNS topic (APICallAlert), and enable SNS notification delivery.
- Save the changes.

3. Configure CloudTrail

Navigate to CloudTrail:

- In the AWS Management Console, search for "CloudTrail".

Create a New Trail:

- Click "Trails" in the left navigation pane.
- Click "Create trail".

Configure the Trail:

- Trail Name: Enter a name (e.g., MyCloudTrail).
- Storage Location: Choose "Create new S3 bucket" and enter a unique bucket name (e.g., my-cloudtrail-logs-uniqueid).
- Log Events: Ensure "Management events" is enabled with "Read/Write" events set to "All".
- Apply trail to all regions: Enable this option.

Advanced Settings:

- Log file SSE-KMS encryption: Leave unchecked (optional).
- Log file validation: Enable if desired.
- SNS: choose your previously created topic (**APICallAlert)**.

Create the Trail:

- Click "Create trail" and wait for it to set up.

4. Set Up EventBridge to Trigger on GetCallerIdentity for Root User

Navigate to EventBridge:

- In the AWS Management Console, search for "EventBridge".

Create a Rule:

- Click on "Rules".
- Click "Create rule".

Configure the Rule:

- Name: Enter a name (e.g., GetCallerIdentityAlert).
- Event Bus: Ensure "AWS default event bus" is selected.
- Rule Type: Choose "Rule with an event pattern".

Define the Event Pattern:

- Choose "Custom patterns (JSON editor)" and enter:

```
{
  "source": ["aws.sts"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventSource": ["sts.amazonaws.com"],
    "eventName": ["GetCallerIdentity"],
    "userIdentity": {
      "type": ["Root"]
    }
  }
}
```

Add SNS as the Target:

- Under Target, select "AWS service".
- Select a target: Choose "SNS topic".
- Topic: Select the SNS topic (APICallAlert).

Configure Permissions (If Prompted):

- Allow EventBridge to create a new role with permissions to publish to the SNS topic.

Create the Rule:

- Review the settings and click "Create rule".

5. Test the Setup via Command Line

Install AWS CLI (If Not Installed):

- Follow the instructions here for your OS.

Configure AWS CLI with Root Credentials:

- Open your terminal or command prompt.
- Run:
- aws configure
- Enter your root Access Key ID, Secret Access Key, Default region name (e.g., us-east-1), and Default output format (e.g., json).

Run the GetCallerIdentity Command:

- Execute:
- aws sts get-caller-identity

Check CloudTrail Logs:

- Go to the CloudTrail console.
- Check the Event history for the GetCallerIdentity event to confirm it has been logged.

Verify SNS Email Notification:

- Check your email inbox for an alert from SNS with details about the GetCallerIdentity API call.

Conclusion

You have successfully set up and tested your AWS Free Tier account with CloudTrail, SNS, and EventBridge to monitor GetCallerIdentity API calls. This setup helps detect unauthorized access attempts and enhances the security of your AWS environment.