

## Cyber Security AWS Cloud Home Lab Setup

### Amazon Simple Notification Service (SNS) - Topic and Subscription

#### APICallAlert1

Edit Delete Publish message

##### Details

<b>Name</b> APICallAlert1	<b>Display name</b> APICallAlert1
<b>ARN</b> arn:aws:sns:ap-southeast-2:586794447095:APICallAlert1	<b>Topic owner</b> 586794447095
<b>Type</b> Standard	

Subscriptions Access policy Data protection policy Delivery policy (HTTP/S) Delivery status logging Encryption Tags Integrations

##### Subscriptions (1)

Edit Delete Request confirmation Confirm subscription Create subscription

Q Search

< 1 >

ID	Endpoint	Status	Protocol
<div><div><input type="radio"/></div><div>79556ee7-e067-4a75-89aa-e4d1e88ae...</div></div>	nhussain06@yahoo.com	<div><div></div>Confirmed</div>	EMAIL

### AWS CloudTrail - Trail

#### CloudTrail1

Delete Stop logging

##### General details

Edit

<b>Trail logging</b> Logging	<b>Trail log location</b> aws-cloudtrail-logs-586794447095-70c8091c/AWSLogs/586794447095	<b>Log file validation</b> Enabled	<b>SNS notification delivery</b> arn:aws:sns:ap-southeast-2:586794447095:APICallAlert1
<b>Trail name</b> CloudTrail1	<b>Last log file delivered</b> March 02, 2025, 16:29:54 (UTC+11:00)	<b>Last file validation delivered</b> -	<b>Last SNS notification</b> March 02, 2025, 16:29:54 (UTC+11:00)
<b>Multi-region trail</b> Yes	<b>Log file SSE-KMS encryption</b> Not enabled		
<b>Apply trail to my organization</b> Not enabled			

### AWS EventBridge - Rule

#### GetCallerIdentityAlert

Edit Disable Delete CloudFormation Template

##### Rule details

<b>Rule name</b> GetCallerIdentityAlert	<b>Status</b> Enabled	<b>Event bus name</b> default	<b>Type</b> Standard
<b>Description</b> GetCallerIdentityAlert	<b>Rule ARN</b> arn:aws:events:ap-southeast-2:586794447095:rule/GetCallerIdentityAlert	<b>Event bus ARN</b> arn:aws:events:ap-southeast-2:586794447095:event-bus/default	

Event pattern Targets Monitoring Tags

##### Event pattern

Edit

```
1 {
2   "source": ["aws.sts"],
3   "detail-type": ["AWS API Call via CloudTrail"],
4   "detail": {
5     "eventSource": ["sts.amazonaws.com"],
6     "eventName": ["GetCallerIdentity"]
7   }
8 }
```

Copy

## Testing - Kali Linux

```
user1@kali: ~  
File Actions Edit View Help  
(user1@kali)-[~]  
$ aws configure  
AWS Access Key ID [None]: AKIAYRH5MWD32Z7OUBWG  
AWS Secret Access Key [None]: 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  
Default region name [None]: ap-southeast-2  
Default output format [None]: json  
(user1@kali)-[~]  
$ aws sts get-caller-identity  
{  
  "UserId": "AIDAYRH5MWD3U634SOS4U",  
  "Account": "586794447095",  
  "Arn": "arn:aws:iam::586794447095:user/user1"  
}
```

## Email Notification

● AWS Notification Message

Yahoo/Inbox ☆

● **APICallAlert1** [amazonaws.com](https://amazonaws.com) >  
From: no-reply@sns.amazonaws.com  
To: nhussain06@yahoo.com

Sun, 2 Mar at 5:00 pm ☆

```
{ "version": "0", "id": "95e40407-7f1c-0225-4684-3ae3b0959701", "detail-type": "AWS API Call via  
CloudTrail", "source": "aws.sts", "account": "586794447095", "time": "2025-03-02T06:00:41Z", "region": "ap-southeast-2", "resources":  
[], "detail": { "eventVersion": "1.08", "userIdentity":  
{ "type": "IAMUser", "principalId": "AIDAYRH5MWD3U634SOS4U", "arn": "arn:aws:iam::586794447095:user/user1", "accountId": "5867944  
47095", "accessKeyId": "AKIAYRH5MWD32Z7OUBWG", "userName": "user1", "eventTime": "2025-03-  
02T06:00:41Z", "eventSource": "sts.amazonaws.com", "eventName": "GetCallerIdentity", "awsRegion": "ap-southeast-  
2", "sourceIPAddress": "122.150.185.36", "userAgent": "aws-cli/2.23.6 md/awscrt#1.0.0.dev0 ua/2.0 os/linux#6.11.2-amd64  
md/arch#x86_64 lang/python#3.12.7 md/pyimpl#CPython cfg/retry-mode#standard md/installer#source md/distrib#kali.2024  
md/prompts#off md/command#sts.get-caller-identity", "requestParameters": null, "responseElements": null, "additionalEventData":  
{ "RequestDetails": { "awsServingRegion": "ap-southeast-2", "endpointType": "regional" }, "requestID": "22f75eb1-d017-42cc-84e0-  
b45db4a2c863", "eventID": "e3320f91-c328-4c3c-8382-  
bf2ec82c423c", "readOnly": true, "eventType": "AwsApiCall", "managementEvent": true, "recipientAccountId": "586794447095", "eventCate  
gory": "Management", "tlsDetails":  
{ "tlsVersion": "TLSv1.3", "cipherSuite": "TLS_AES_128_GCM_SHA256", "clientProvidedHostHeader": "sts.ap-southeast-  
2.amazonaws.com" } } } }
```

--  
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:  
<https://sns.ap-southeast-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:ap-southeast-2:586794447095:APICallAlert1:79556ee7-e067-4a75-89aa-e4d1e88ae1a2&Endpoint=nhussain06@yahoo.com>

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at  
<https://aws.amazon.com/support>