How to route CloudTrail S3 notifications through SNS

Version 2.0

January 24, 2020

expel

Contents

Overview

Amazon S3 notifications can't be configured for more than one Simple Queue Service (SQS) queue per bucket. This poses a problem for customers who want to hook Expel up to their CloudTrail bucket if they are already sending notifications to an SQS queue for internal reasons. In this document, we show how a customer can route S3 notifications through SNS (simple notification service) to a different SQS queue that Expel can poll from.

Pre-requisites

1. **A trail must already be configured to send CloudTrail events to an S3 bucket**
2. **An IAM (Identity and Access Management) Role or User must be created for Expel to authenticate with**

Information to record

Field	Description
S3 bucket ARN (Amazon Resource Name)	The unique identifier for the S3 bucket where CloudTrail events are being sent
SQS queue ARN	The unique identifier for the SQS queue that Expel will use to consume S3 notifications
SQS queue URL	The URL for the SQS queue that Expel will use to consume S3 notifications
SNS topic ARN	The unique identifier for the SNS topic that will be used to route S3 notifications to the SQS queue

Steps

Step 1: Create a new SNS topic

Note: Make sure to create the SNS topic in the same region as the S3 bucket CloudTrail events are being sent to!

A. Navigate to Services > Simple Notification Service and click **Create Topic** (Figure 1)

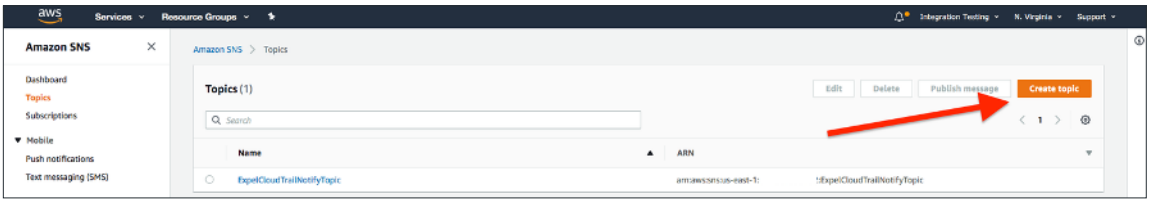

Figure 1

B. On the next screen, create a **Topic Name** (Figure 2)

Figure 2

C. Under **Access Policy**, choose **Advanced** (Figure 3)

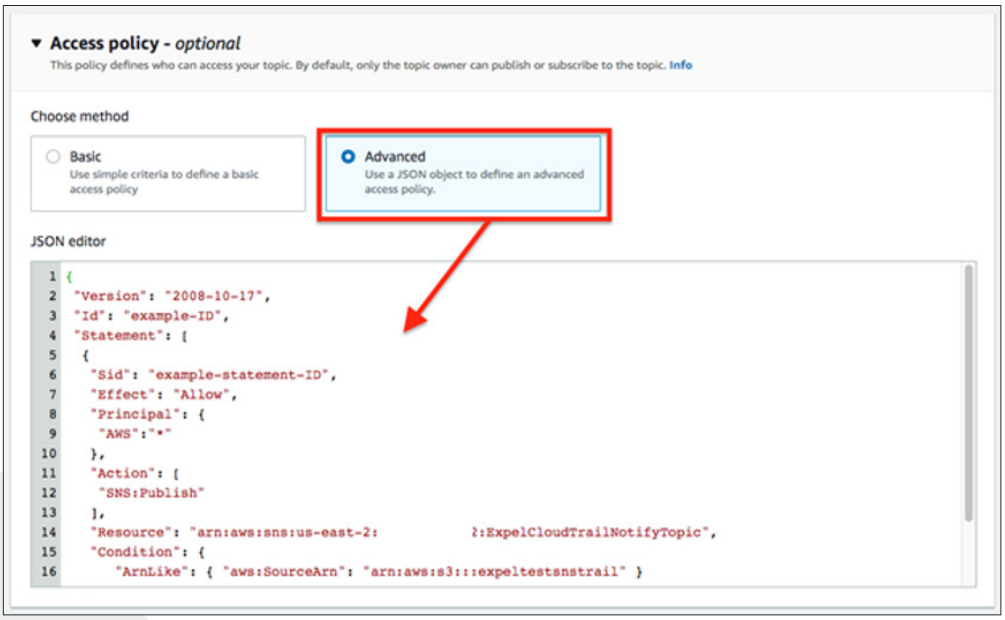

Figure 3

D. In the JSON editor, paste the below policy substituting the **YOUR_TOPIC_ARN** and **YOUR_S3_ARN** fields with your values. This policy allows S3 to publish notifications to the topic for your CloudTrail bucket (Figure 4)

SNS Topic Access Policy

```
{
 "Version": "2008-10-17",
 "Id": "expel-topic-policy-ID",
 "Statement": [
  {
   "Sid": "expel-statement-ID",
   "Effect": "Allow",
   "Principal": {
    "AWS":"*"
   },
   "Action": [
    "SNS:Publish"
   ],
   "Resource": "YOUR_TOPIC_ARN",
   "Condition": {
      "ArnLike": { "aws:SourceArn": "YOUR_S3_ARN" }
   }
  }
 ]
}
```

Figure 4

E. Press **Create Topic** to finish this step

Step 2: Create an SQS queue for S3 notifications

In this step, we'll create a new SQS queue for S3 notifications. Expel will poll notifications from this queue to know when new CloudTrail data has been added.

Note: Make sure you create the SQS queue in the same region as the SNS topic and S3 bucket!

A. Navigate to **Services > Simple Queueing Service** and press **Create New Queue** (Figure 5)

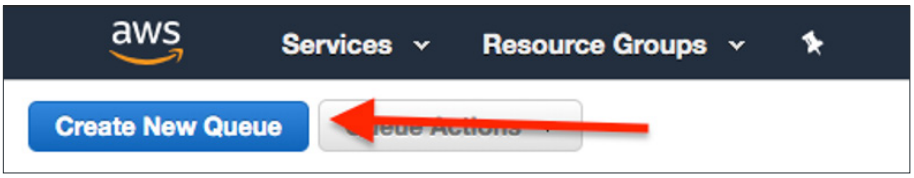

Figure 5

B. On the next screen, name the new queue, choose **Standard Queue**, and press **Quick Create Queue** (Figure 6)

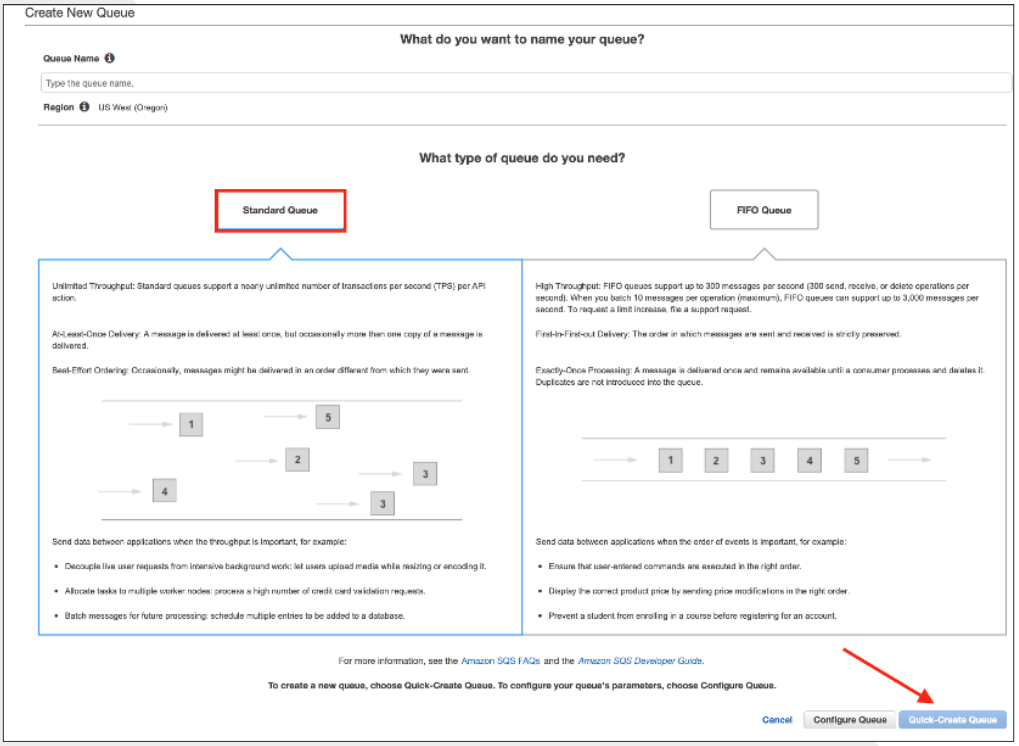

Figure 6

C. Once the queue has been created, we need to modify the Queue policy to allow our SNS topic to write to it. Select the queue and navigate to **Permissions**. Click **Add Permission** (Figure 7)

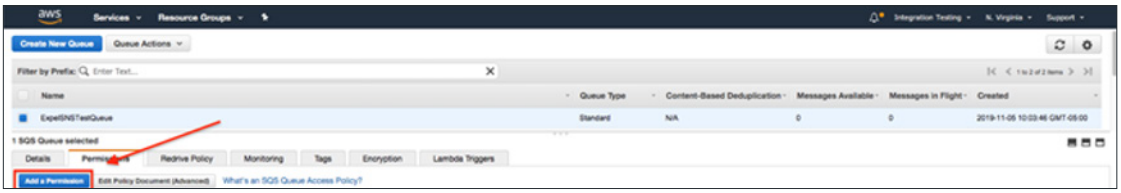

Figure 7

D. On the next screen, fill out the required fields to grant the SNS Topic SendMessage permissions on the SQS queue (Figure 8)

Field	Value
Effect	Allow
Principal	Everybody (*)
Actions	SendMessage
Qualifier	None
Condition	StringEquals
Key	aws:SourceArn
Value	< Your SNS Topic ARN >

Figure 8

E. When done, the form should look similar to below (Figure 9)

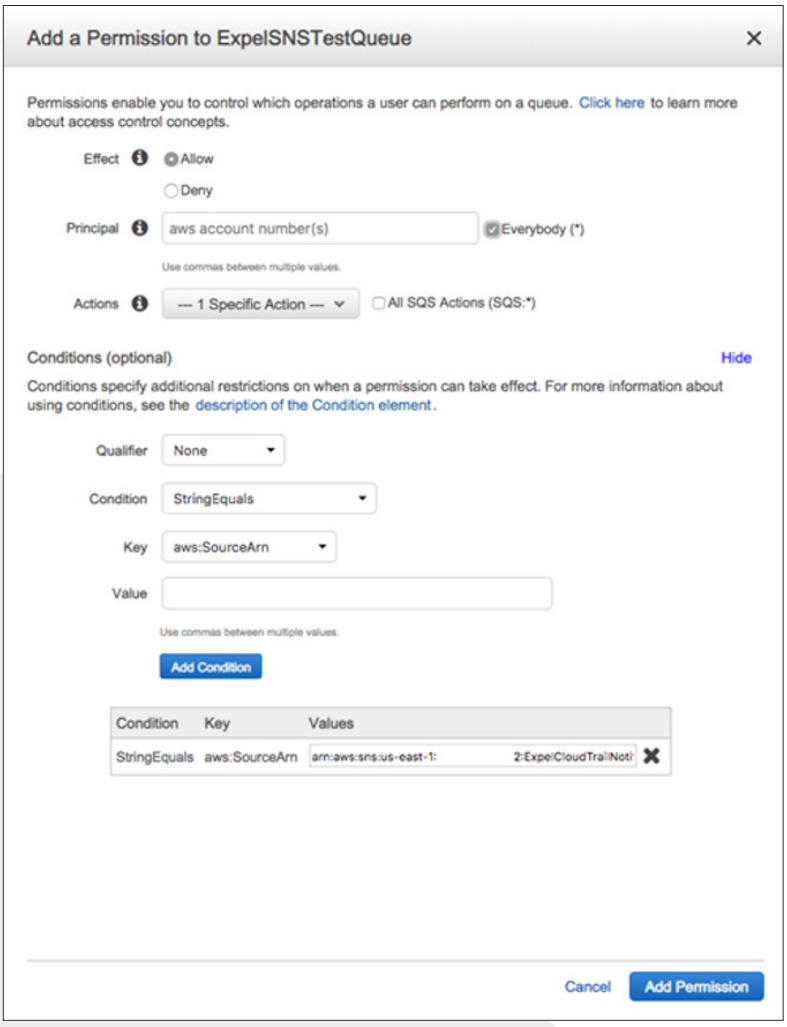

Figure 9

F. Press **Add Permission** to finish this step. The SQS policy should look similar to below (Figure 10)

SQS Permission Policy

```
{
  "Version": "2012-10-17",
  "Id": "YOUR_QUEUE_ARN/SQSDefaultPolicy",
  "Statement": [
    {
      "Sid": "Sid1572965666162",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "YOUR_SQS_QUEUE_ARN",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "YOUR_SNS_TOPIC_ARN"
        }
      }
    }
  ]
}
```

Figure 10

Step 3: Subscribe SQS queue to SNS topic

Now that we've created a SNS topic and SQS queue we need to configure SNS to send events to the SQS queue.

A. Navigate to **Services > Simple Notification Service** and press **Create subscription** (Figure 11)

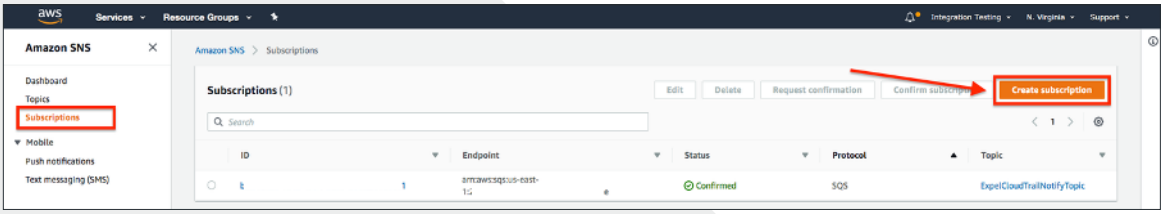

Figure 11

B. On the next screen, enter the required fields to configure the subscription (Figure 12)

Field	Value
Topic ARN	Your SNS Topic ARN
Protocol	Select Amazon SQS
Endpoint	Your SNS Queue ARN
Enable raw message delivery	Checked

Figure 12

Note: Checking "enable raw message delivery" ensures SNS doesn't add extra metadata headers to the message when it sends to SQS. Please check this!

C. Press **Create subscription** to finish this step (Figure 13)

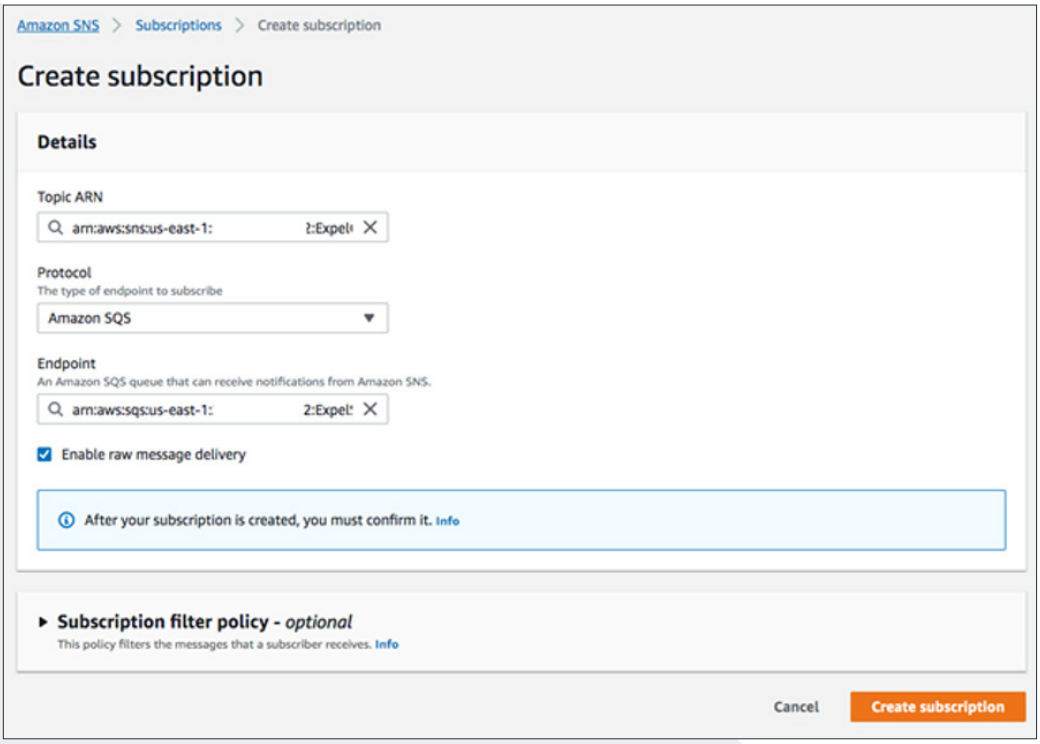

Figure 13

Step 4: Enable S3 event notifications to SNS topic

In this step, we'll configure the CloudTrail S3 bucket to send SNS notifications when CloudTrail adds logs to the bucket.

A. Navigate to **Services > S3 > Your S3 CloudTrail Bucket**

B. Open **Properties** for your S3 bucket and navigate to **Events**. Press **+Add notification** (Figure 14)

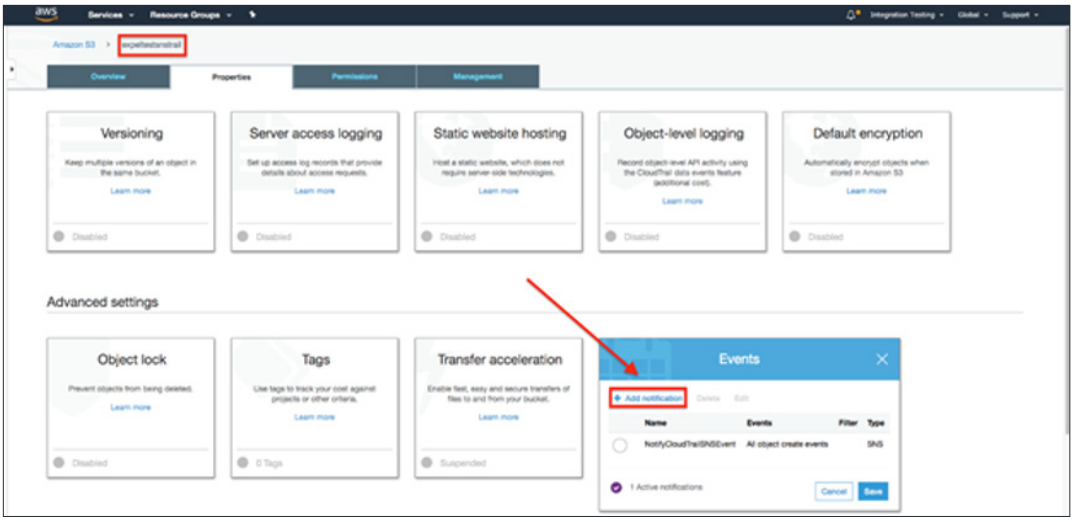

Figure 14

C. On the next screen (Figure 15):

a. Create a name for your notification rule

b. Select **All object create events**

c. Send to **SNS topic**

d. Select your SNS topic we created earlier

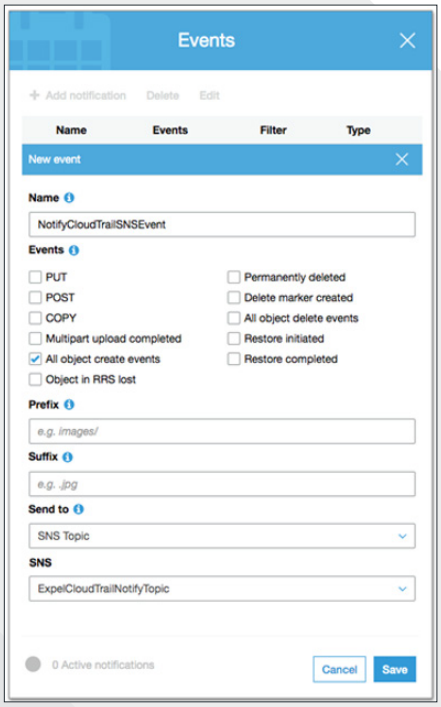

Figure 15

D. Press **Save** to finish this step

Step 5: Grant Expel IAM User or Role access to SQS queue

At this point we have configured S3 notifications ➔ SNS topic ➔ SQS queue. The final step involves granting the existing Expel IAM Role (or User) access to poll events from the SQS queue and the S3 bucket.

A. Navigate to **Services > IAM > Expel User or Role**

B. Create and add a new inline policy to the Expel User or Role. The policy should grant the permissions below:

- **SQS Permissions**
  - DeleteMessage
  - DeleteMessageBatch
  - ReceiveMessage
- **S3 Permissions**
  - GetObject
- **Expel Permissions**

```
{
    “Version”: “2012-10-17”,
    “Statement”: [
    {
            “Action”: [
            “sqs:DeleteMessage”,
            “sqs:DeleteMessageBatch”,
            “sqs:ReceiveMessage”
            ],
            “Effect”: “Allow”,
            “Resource”: “YOUR_SQS_QUEUE_ARN”
    },
    {
            “Action”: [
            “s3:GetObject”
            ],
            “Effect”: “Allow”,
            “Resource”: “YOUR_S3_BUCKET_ARN/*”
    }
    ]
}
```

C. Congratulations! You've configured S3 notifications to a SQS queue via SNS. Contact your Expel *Engagement Manager* for details on how to finish onboarding.

That's it! Give yourself a pat on the back — you're done!

If you have any issues, concerns, questions or feedback,
please don't hesitate to contact Expel at devicehealth@expel.io.