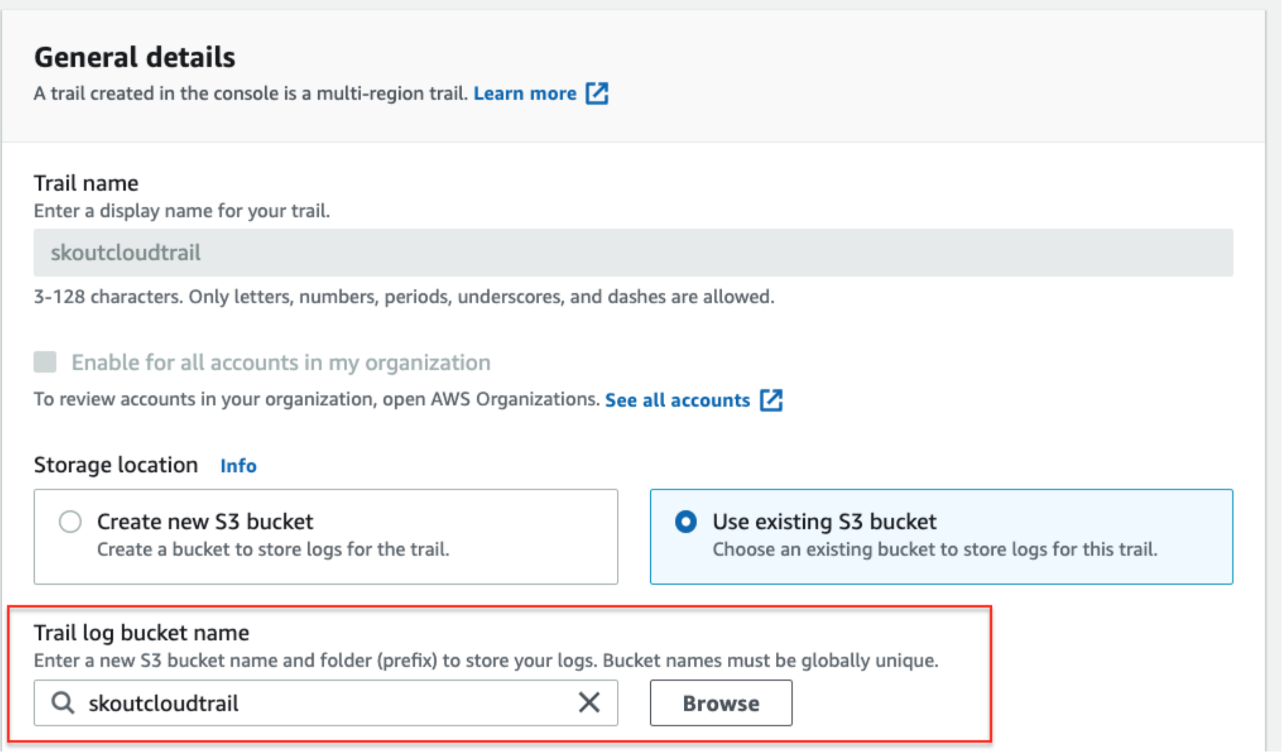
Integrating AWS Cloudtrail with XDR Dashboard

https://campus.barracuda.com/doc/96767287/

The steps below outline integration between AWS CloudTrail and XDR Monitoring. AWS CloudTrail service helps monitor governances, compliance, and operational and risk auditing of AWS accounts. Customers who are looking to monitor their AWS environment should follow the implementation instructions listed below to enable XDR to monitor their AWS environment in real time.

To integrate AWS Cloudtrail

1. If your Trail isn't set up, follow this link to set up a trail within cloudtrail: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.htm
2. Ensure the trail is logging to a S3 Bucket. If you edit the trail, you can see the name of the bucket it's writing log files to. Take note of the S3 Bucket Name:



General details

A trail created in the console is a multi-region trail. Learn more

Trail name

Enter a display name for your trail.

skoutcloudtrail

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

□ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Storage location Info

○ Create new S3 bucket
Create a bucket to store logs for the trail.

● Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

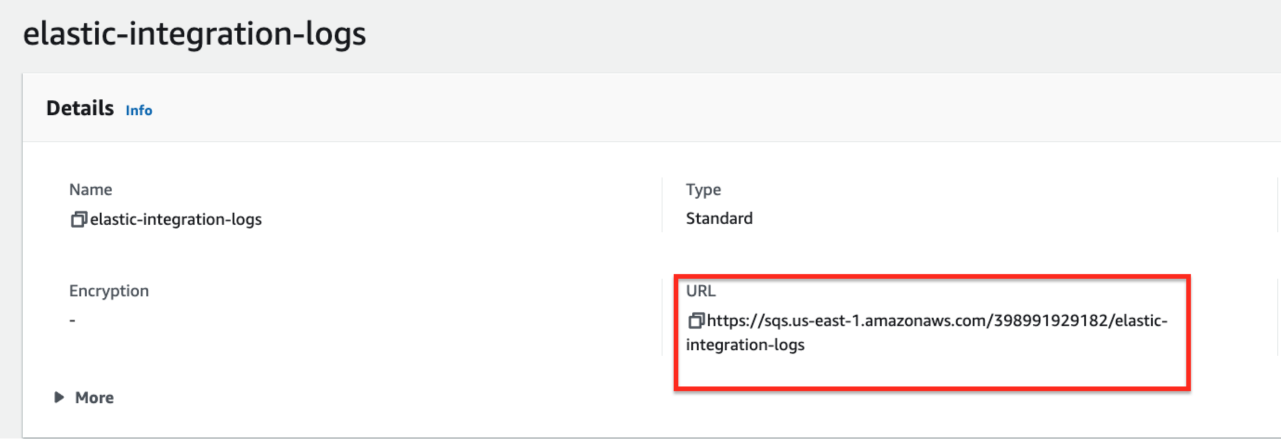
Trail log bucket name

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

skoutcloudtrail

3. Set up an SQS Queue and use this template for its access policy:
   Replace with the ARN of the SQS queue you just made
   Replace with the name of the S3 Bucket that your CloudTrail is writing logs to
   Afterwards hit save and then take note of the URL of the SQS Queue

```
{
    "Version": "2012-10-17",
    "Id": "__default_policy_ID",
    "Statement": [
       {
           "Sid": "__owner_statement",
           "Effect": "Allow",
           "Principal": "*",
           "Action": "SQS:*",
           "Resource": "<SQS-queue-ARN>",
           "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:<bucket-name>"
                }
           }
       }
   ]
}
```



elastic-integration-logs

Details Info

Name
elastic-integration-logs

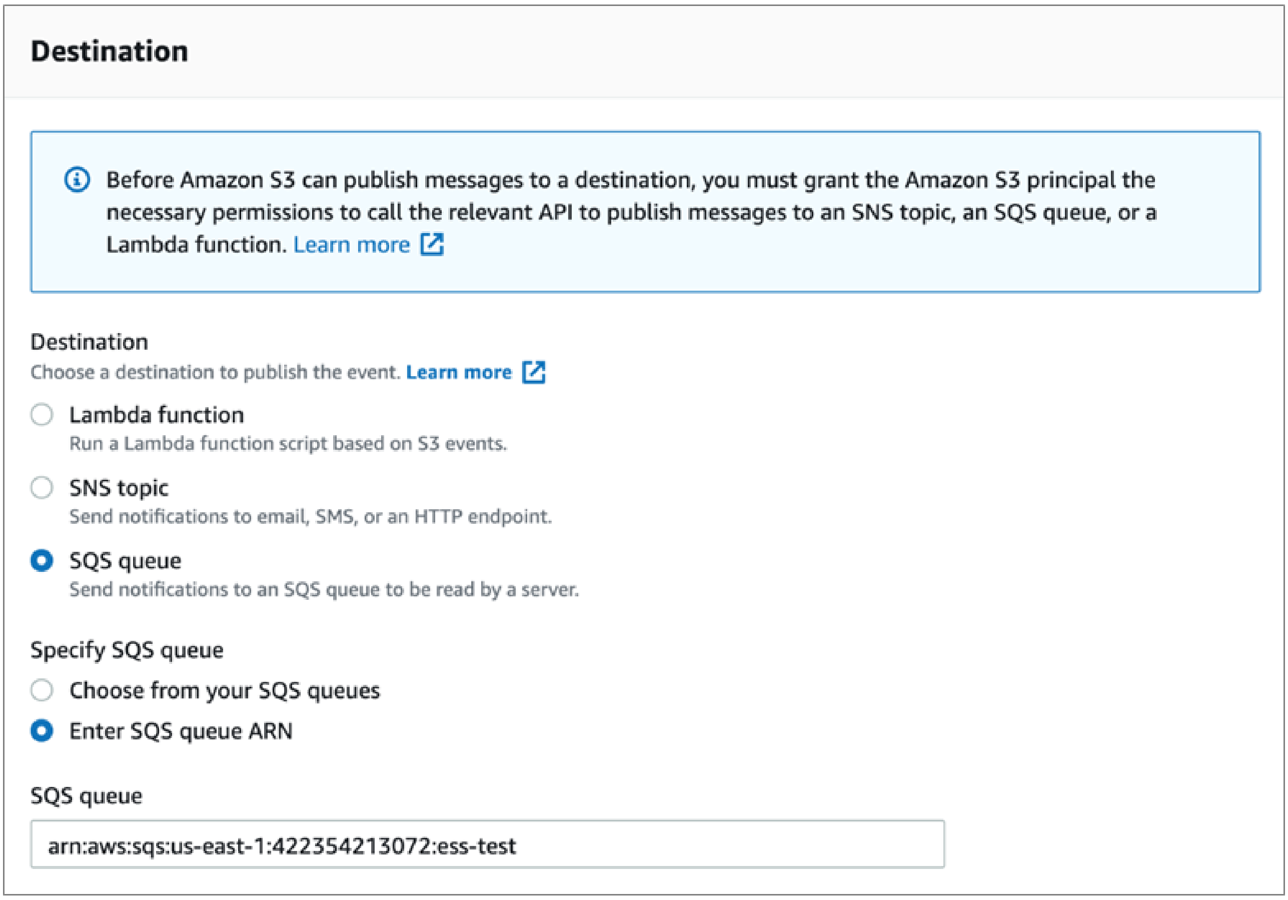
Type
Standard

Encryption
-

URL
https://sqs.us-east-1.amazonaws.com/398991929182/elastic-integration-logs

▶ More

4. Navigate to the S3 Bucket that your cloudtrail is writing logs to.
   Click **Properties** > Scroll down to **Event Notifications** and click **Create event notification**.
   Type a name for the event name.
   In **Event Types**, select everything to monitor all Cloudtrail updates.
   For the **Destination**, enter the SQS queue you made.



Destination

ⓘ Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. Learn more

Destination

Choose a destination to publish the event. **Learn more**

○ Lambda function
Run a Lambda function script based on S3 events.

○ SNS topic
Send notifications to email, SMS, or an HTTP endpoint.

● SQS queue
Send notifications to an SQS queue to be read by a server.

Specify SQS queue

○ Choose from your SQS queues

● Enter SQS queue ARN

SQS queue

arn:aws:sqs:us-east-1:422354213072:ess-test

5. For XDR to receive AWS SQS messages, an access key id and secret access key will need to be generated. A user permissioned in IAM with a role only allowed to read access from SQS queues:
   - Setting up a new user in IAM – https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-setting-up.html
   - SQS IAM permissioning JSON’s (Only need the SQS Send Message permission, first example) –https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-examples-of-sqs-policies.html
6. Once completed, provide XDR the following information -
   - **Queue Url**: https://sqs.us-east-1.amazonaws.com/123/test-queue
   - **Access key id**
   - **Secret Access Key**

Figures