
Integrating Amazon Security Lake

<https://campus.barracuda.com/doc/104366130/>

The steps below outline integration between Amazon Security Lake and Barracuda XDR monitoring. Amazon Security Lake helps you analyze security data so that you can get a complete understanding of your security posture across the entire organization. With Amazon Security Lake, you can also improve the protection of your workloads, applications, and data.

Prerequisites

To integrate Amazon Security Lake, you must have the following:

- A functioning Amazon Security Lake instance. See <https://docs.aws.amazon.com/security-lake/latest/userguide/getting-started.html>
- Server Access Logging enabled on Amazon S3 Security. See the *To enable Server Access Logging enabled on Amazon S3 Security procedure* below.

To enable Server Access Logging enabled on Amazon S3 Security

1. In **Amazon S3 Security**, navigate to **Buckets** > *[your bucket]*, where *[your bucket]* is the name of your bucket.
2. Click the **Properties** tab.
3. In **Server access logging**, select the **Enable** check box.
4. In **Destination**, enter the path to your bucket.
5. In **Log Object key Format**, select a format.

Server access logging

Log requests for access to your bucket. [Learn more](#)

Server access logging

Disable

Enable

Destination

Specify a destination bucket in the US West (N. California) us-west-1 Region. To store your logs under a particular prefix, make sure that you include a slash (/) after the name of the prefix. Otherwise, the prefix will be added to the name of your log files.

s3://aws-security-data-lake-us-west-1-

Format: s3://<bucket>/<optional-prefix-with-path>

Destination Region

US West (N. California) us-west-1

Destination bucket name

aws-security-data-lake-us-west-1-

Destination prefix

Log object key format

[DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]

[DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]

To speed up analytics and query applications, use this format.

Log object key example

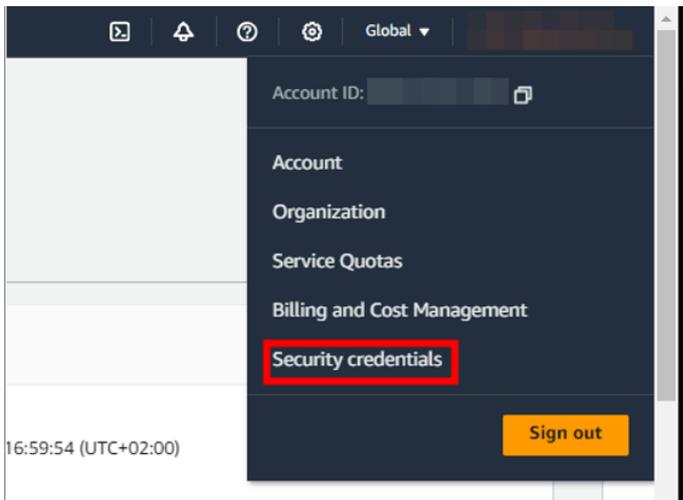
aws-security-lake-2023-07-01-10-12-56-[UniqueString]

6. Click **Save Changes**.

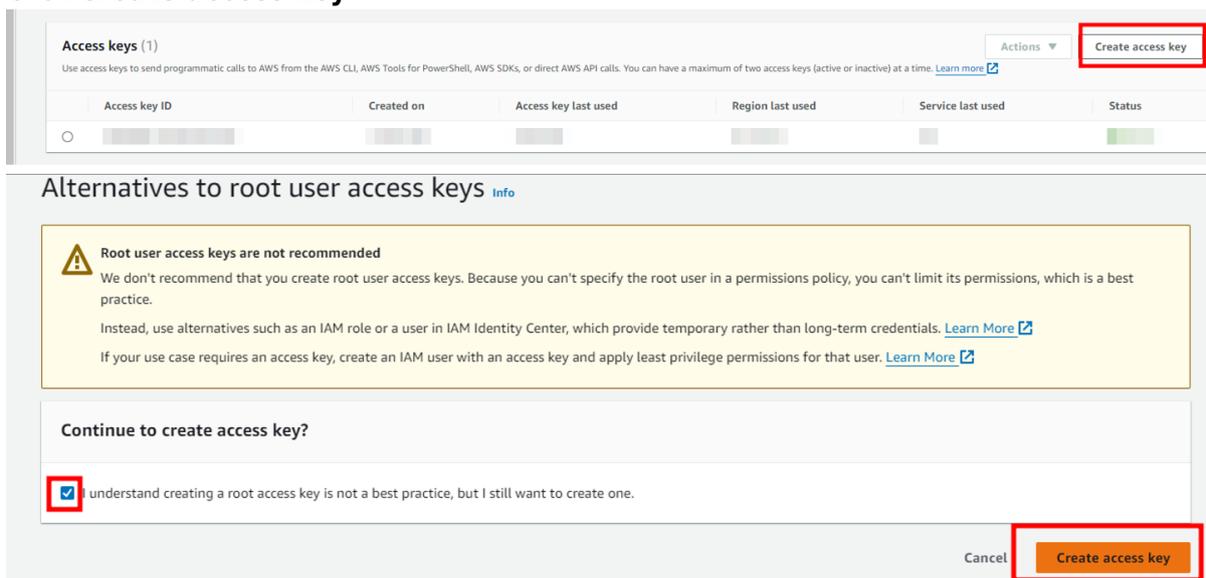
7. Proceed to the *To enable the Amazon Security Lake integration for an S3 Bucket* procedure.

To create and save access keys for integration

1. In **Amazon S3**, in the profile menu in the top right corner of the window, click **Security Credentials**.



2. In the **Access keys** section, click **Create access key**.
3. Select the **I understand creating a root access key is not a best practice, but I still want to create one** check box.
4. Click **Create access key**.

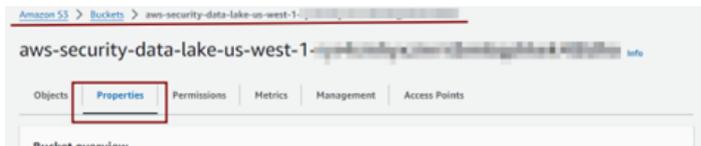


5. Copy and save your **Access key** and **Secret access key**.
6. Click **Done**.

To integrate Amazon Security Lake via Simple Queue Service (Optional)

You don't need to perform this procedure to integrate Amazon Security Lake unless you want to use Simple Queue Service.

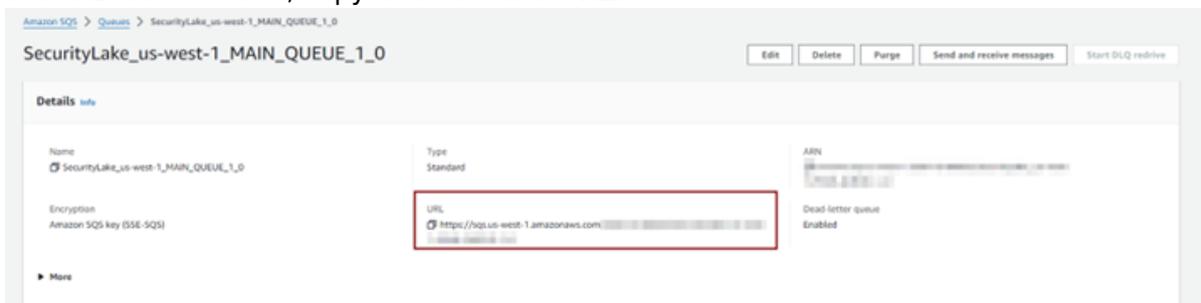
1. In **Amazon S3 Security**, navigate to **Buckets** > *[your bucket]*, where *[your bucket]* is the name of your bucket.
2. Click the **Properties** tab.



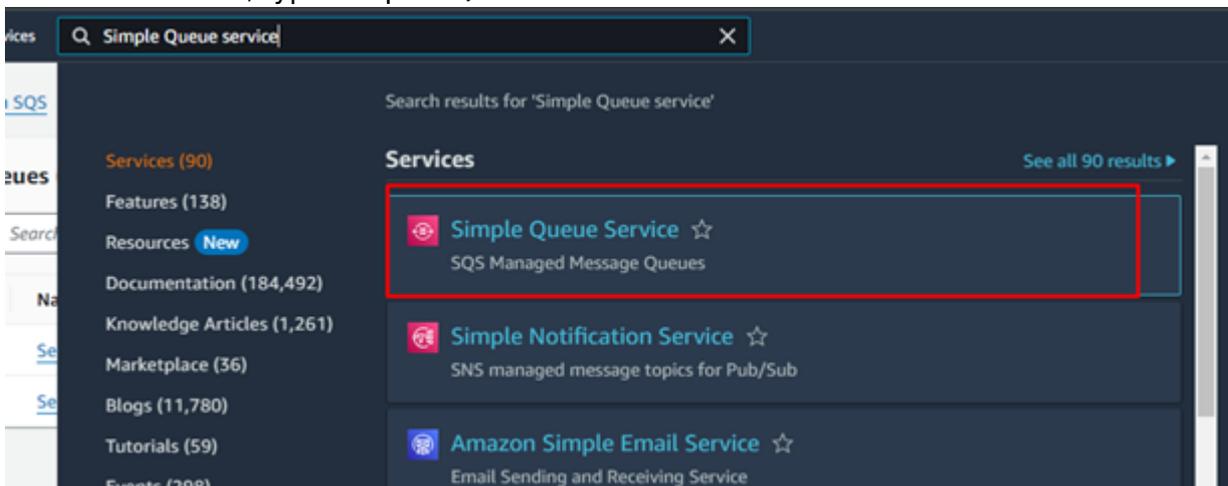
3. In the **Event notifications** area, do one of the following:
4. If there are no event notifications, proceed to step 7.
5. If there is an event notification, click a link in the **Destination** column on the right.



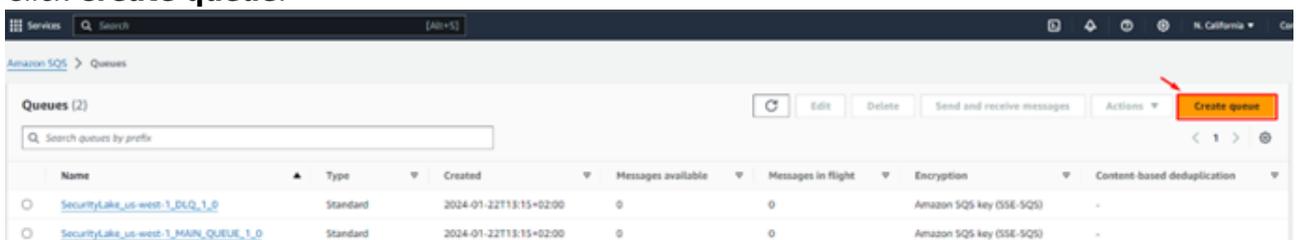
6. In the Details section, copy and save the **URL**.



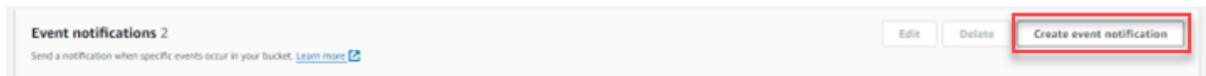
7. In the **Search** bar, type Simple Queue Service and hit **Return**.



8. Click **Create queue**.

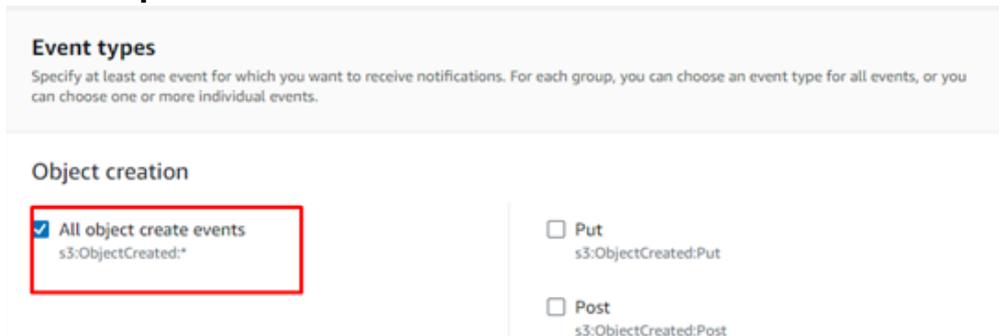


9. Select your options, then click **Create queue**.
10. Navigate to **Buckets** > [your bucket], where [your bucket] is the name of your bucket.
11. Click the **Properties** tab.
12. In the **Event notifications** area, click **Create event notification**.

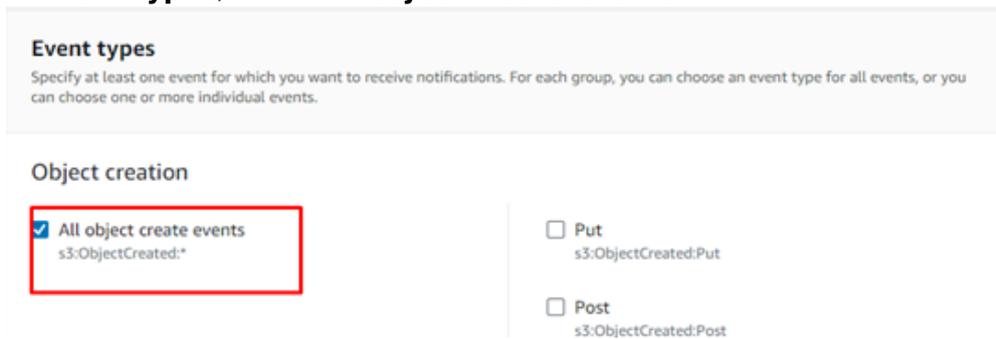


13. In the **General configuration** area, provide the following:

- **Event name**
- **Prefix - optional**
- **Suffix - optional**



14. In **Event types**, select **All object create events**.



15. In **Destination**, select **SQS queue**.

16. In **Specify SQS queue**, select **Choose from your SQS queue**.

17. Select an SQS queue.

Destination

i 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
Fanout messages to systems for parallel processing or directly to people.

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

security-lake-queue

Cancel Save changes

18. Click **Save Changes**.

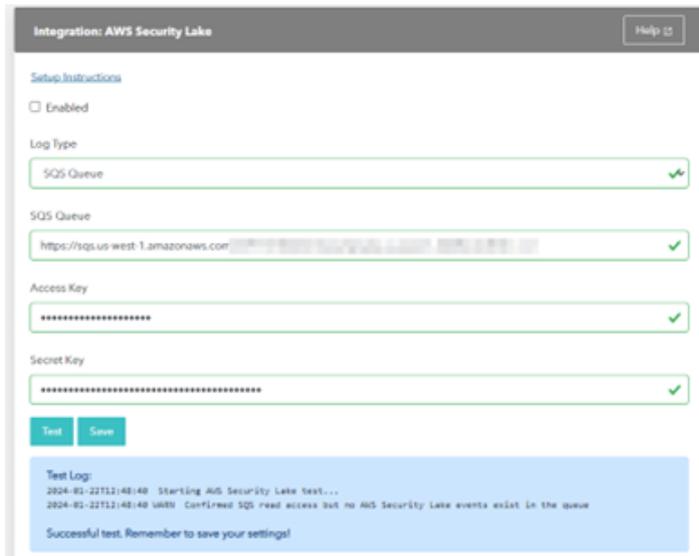
19. Proceed to the *To enable the Amazon Security Lake integration for an SQS Queue* procedure below.

To enable the Amazon Security Lake integration for an S3 Bucket

1. In **Barracuda XDR Dashboard**, navigate to **Administration > Integrations**.
2. On the **AWS Security Lake** card, click **Setup**.
3. Select the **Enabled** check box.
4. In **Log Type**, select **S3 Bucket**.
5. In **AWS Bucket**, paste the path to your Amazon Bucket.
6. In **Access Key**, paste your access key.
7. In **Secret Key**, paste your secret key.
8. Optionally, click **Test** to verify the credentials.
9. Select the **Enable** check box.
10. Click **Save**.

To enable the Amazon Security Lake integration for an SQS Queue

1. In **Barracuda XDR Dashboard**, navigate to **Administration > Integrations**.
2. On the **AWS Security Lake** card, click **Setup**.
3. Select the **Enabled** check box.
4. In **Log Type**, select **SQS Queue**.
5. In **SQS Queue**, paste the SQS queue you set up in the previous procedure.
6. In **Access Key**, paste your access key.
7. In **Secret Key**, paste your secret key.



Integration: AWS Security Lake Help

Setup Instructions

Enabled

Log Type

SQS Queue ✓

SQS Queue

https://sqs.us-west-1.amazonaws.com/... ✓

Access Key

***** ✓

Secret Key

***** ✓

Test Save

Test Log:

```
2024-02-22T12:48:40 Starting AWS Security Lake test...
2024-02-22T12:48:40 INFO Confirmed SQS read access but no AWS Security Lake events exist in the queue
Successful test. Remember to save your settings!
```

8. Optionally, click **Test** to verify the credentials.
9. Select the **Enable** check box.
10. Click **Save**.

Figures

1. S3BucketSettings.png
2. Access keys.png
3. CreatedAccessKeys.png
4. PropertiesTab.png
5. EventNotifications.png
6. URL.png
7. Search.png
8. CreateQueue.png
9. EventNotification2.png
10. EventNotification4.png
11. EventNotification4.png
12. EventNotification5.png
13. SQS Queue.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.