

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 <u>https://docs.aws.amazon.com/security-lake/latest/userguide/getting-started.html</u>
- 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		
O Disable		
O Enable		
Destination	under a particular profix, make c	uro that us
include a slash (/) after the name of the prefix. Otherwise, the prefix will be added to the name	e of your log files.	ure that you
s3://aws-security-data-lake-us-west-1	Browse S3	
Format: s3:// <bucket>/<optional-prefix-with-path></optional-prefix-with-path></bucket>		
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		
 Log object key format [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] 		
 Log object key format [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY] 	/[MM]/	
 Log object key format [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY] [DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] 	/[MM]/	
 Log object key format [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY] [DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] To speed up analytics and query applications, use this format. 	I/[MM]/	
 Log object key format [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY] [DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] To speed up analytics and query applications, use this format. Log object key example 	/[MM]/	

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.

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
0					
ternatives to root	user access key	/S Info			
Root user access keys are not	recommended				
Root user access keys are no	recommended				
Root user access keys are no We don't recommend that yo	t recommended u create root user access kevs.	Because you can't specify the ro	t user in a permissions policy.	vou can't limit its permissions.	which is a best
Root user access keys are no We don't recommend that yo	t recommended u create root user access keys.	Because you can't specify the roo	t user in a permissions policy, y	you can't limit its permissions,	which is a best
Root user access keys are no We don't recommend that yo practice.	t recommended u create root user access keys.	Because you can't specify the roo	t user in a permissions policy, y	you can't limit its permissions,	which is a best
Root user access keys are no We don't recommend that yo practice.	t recommended u create root user access keys.	Because you can't specify the roo	t user in a permissions policy, y	you can't limit its permissions,	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such	t recommended u create root user access keys. as an IAM role or a user in IAN	Because you can't specify the roo 1 Identity Center, which provide t	t user in a permissions policy, y	you can't limit its permissions, m credentials. Learn More 🗹	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such	t recommended u create root user access keys. as an IAM role or a user in IAN	Because you can't specify the roo 1 Identity Center, which provide t	t user in a permissions policy, y emporary rather than long-terr	you can't limit its permissions, m credentials. <u>Learn More</u> 🔀	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an ar	t recommended u create root user access keys. as an IAM role or a user in IAN ccess key, create an IAM user w	Because you can't specify the roo 4 Identity Center, which provide t /ith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More</u> 🔀 user. Learn More 🔀	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an ac	t recommended u create root user access keys. as an IAM role or a user in IAN ccess key, create an IAM user w	Because you can't specify the roo 1 Identity Center, which provide t rith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More</u> 🔀 user. <u>Learn More</u> 🔁	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an ac	t recommended u create root user access keys. as an IAM role or a user in IAM ccess key, create an IAM user w	Because you can't specify the roo 4 Identity Center, which provide t rith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More </u> Jiser. <u>Learn More </u>	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an ac	t recommended u create root user access keys. as an IAM role or a user in IAN cess key, create an IAM user w	Because you can't specify the roo I Identity Center, which provide t ith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More [2]</u> user. <u>Learn More [2]</u>	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an ac	t recommended u create root user access keys. as an IAM role or a user in IAM cess key, create an IAM user w	Because you can't specify the roo I Identity Center, which provide t rith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More [2]</u> Iser. <u>Learn More [2]</u>	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an are Continue to create access k	t recommended u create root user access keys. as an IAM role or a user in IAM cess key, create an IAM user w	Because you can't specify the roo 4 Identity Center, which provide t ith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More 2</u> user. <u>Learn More 2</u>	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an access keys Continue to create access keys	t recommended u create root user access keys. as an IAM role or a user in IAM cess key, create an IAM user w	Because you can't specify the roo I Identity Center, which provide t rith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More [2]</u> user. <u>Learn More [2]</u>	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an are Continue to create access k	t recommended u create root user access keys. as an IAM role or a user in IAM ccess key, create an IAM user w ey?	Because you can't specify the roo 4 Identity Center, which provide t yith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More [2]</u> user. <u>Learn More [2]</u>	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an access keys Continue to create access keys	t recommended u create root user access keys. as an IAM role or a user in IAM ccess key, create an IAM user w	Because you can't specify the roo 1 Identity Center, which provide t /ith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More (?</u> user. <u>Learn More</u> (?)	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an are Continue to create access k	t recommended u create root user access keys. as an IAM role or a user in IAM ccess key, create an IAM user w ey?	Because you can't specify the roo 4 Identity Center, which provide t iith an access key and apply least	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, m credentials. <u>Learn More [2]</u> user. <u>Learn More [2]</u>	which is a best
Root user access keys are no We don't recommend that yo practice. Instead, use alternatives such If your use case requires an are ontinue to create access k understand creating a root access	t recommended u create root user access keys. as an IAM role or a user in IAM cess key, create an IAM user w ey? ss key is not a best practice, b	Because you can't specify the roo 1 Identity Center, which provide t ith an access key and apply least ut I still want to create one.	t user in a permissions policy, y emporary rather than long-terr privilege permissions for that u	you can't limit its permissions, n credentials. <u>Learn More [2]</u> user. <u>Learn More [2]</u>	which is a best

- 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.



 Amazon 53 > Buckets > aves-security-data-lake-us-west-1-_____

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

 Objects
 Properties

 Permissions
 Metrics

 Management
 Access Points

- 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.

Even Send a	Event notifications 2 Edit Delete Create event notification					
	Name		Event types	Filters	Destination type	Destination
			All object create events	ext/	SQS queue	SecurityLake_us-west-1_MAIN_QUEUE_1_0
	permitted and an exception of the second s		All object create events	aws/	SQS queue	SecurityLake_us-west-1_MAIN_OUEUE_1_0

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

Amazon SQS > Queues > SecurityLake_us-west-1_MAIN_QUEUE_1_0 SecurityLake_us-west-1_MAIN_QUEUE_1_0	66	t Delete Purge Send and receive messages Start DLQ redrive
Details 🗤		
Name Ø SecurityLake_us-west-1_MAIN_QUEUE_1_0	Type Standard	AN
Encryption Amazon SQS key (ISE-SQS)	URL Ø https://bps.us-west-1.amazonaws.com	Dead-letter queue Enabled
► More		

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

kes C	२ Simple Queue service				×			
sqs		Searc	h results for 'Simpl	e Queue service				
ues	Services (90) Features (138)	Serv	rices	- C i A		See	all 90 results 🕨	
Na	Resources New Documentation (184,49	2)	SQS Managed M	essage Queues				
Se	Knowledge Articles (1,2) Marketplace (36)	61) 🧑	Simple Notifi SNS managed m	ication Servi essage topics fo	ce ☆ vr Pub/Sub			
Se	Blogs (11,780) Tutorials (59)		Amazon Sim	ple Email Se	rvice 😭			1
lick (Events (298) Create queue.		Email Sending a	nd Receiving Se	rvice			
nazon SQS >	Queues					e		
Queues (2 Q. Search (l) queues by prefix				C Edit	Delete Send and receive messa	jes Actions ¥	Create que
O Seco	Ne	Type V Standard	Created 2024-01-22T13:15=02:00	 Messages available 0 	 Messages in flight 0 	Encryption Amazon SQS key (SSE-SQS)	 Content-based deeler 	duplication
0 500	and she up were 1 MAN CORDE 1.0	Grandand	2024-01-22218-15-02-00		0	Amazona 505 km/858-5050		

- 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.



Event notifications 2 Send a notification when specific events occur in your bucket	Learn mare		Edit Delete	Create event notification
13. In the General confi • Event name • Prefix - option • Suffix - option	guration area, p al al	rovide the following:		
Event types Specify at least one event can choose one or more in	for which you want to receive not dividual events.	tifications. For each group, you can choose an ev	vent type for all events, or y	you
Object creation All object create ev s3:ObjectCreated:*	ents	Put s3:ObjectCreated:Put		
14. In Event types , sele	tt All object cre	s3:ObjectCreated:Post ate events.		
Event types Specify at least one event for which yo can choose one or more individual eve	u want to receive notifications. Fints.	or each group, you can choose an event type fo	r all events, or you	
Object creation				
All object create events s3:ObjectCreated:*		Put s3:ObjectCreated:Put		
	-	Post		

- 15. In **Destination**, select **SQS queue**.
- 16. In Specify SQS queue, select Choose from your SQS queue.
- 17. Select an SQS queue.



 Before Amazon S necessary permise Lambda function 	can publish messages to a de ions to call the relevant API to Learn more	stination, you must grant tl publish messages to an SN	ne Amazon S3 princij S topic, an SQS queu	pal the Je, or a
Destination hoose a destination to put Cambda function	sh the event. Learn more			
Run a Lambda function SNS topic Fanout messages to sys	rript based on S3 events. ems for parallel processing or direct	y to people.		
SQS queue Send notifications to an	QS queue to be read by a server.			
Pecify SQS queue Choose from your SO Enter SQS queue AR	S queues			
05 0000				

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 (2
Setup Instructions	
Enabled	
Log Type	
SQS Queve	
SQS Queue	
https://sqs.us-west-1.amazonaws.com	
Access Key	
Secret Key	
Test Save	
Testlog: 2024-01-2212:08:00 Starting AUS Security Lake test 2024-02-2212:04:04 UARN Confirmed SQS read access but no AUS Security Lake events exist in the queue	
Successful test. Remember to save your settings!	

- Optionally, click **Test** to verify the credentials.
 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.