Quintrix

Amazon Connect Integration

WEEK 8 – QA RECORDINGS PART 2

PROPRIETARY & CONFIDENTIAL

1095 Morris Ave, SUITE 101, Union NJ 07083
646-762-0305 | INFO@QUINTRIXSOLUTIONS.COM

Amazon Connect – Monitor Calls

Monitor live conversations

Managers and agents in training can monitor live conversations between agents and customers. To set this up, you need to add the Set recording behavior block to your voice/chat contact flow, assign managers and trainees the appropriate permissions, and then show them how to monitor the conversations.

Amazon Connect – Monitor Calls

Set up live monitoring for voice and/or chat

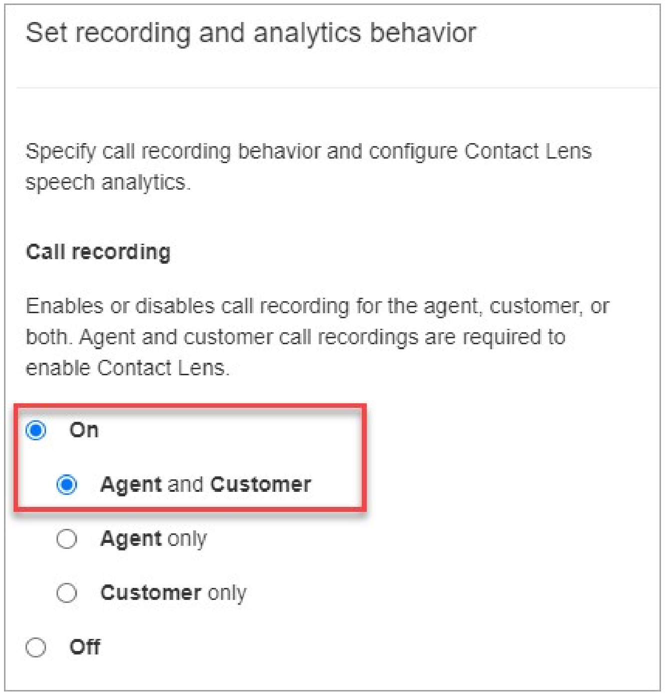
1. Add the Set recording and analytics behavior block to your contact flow. Do this to monitor calls, chats, or both.

To enable monitoring of voice and/or chat conversations, in the block's properties choose Agent and Customer.

2. Choose whether to record the conversations you monitor.

Although you need to add the Set recording behavior block to your contact flow, you don't need to record voice and/or chat conversations for monitoring to work. By default when you set up your instance, Amazon S3 buckets are created to store call recordings and chat transcripts. The existence of these buckets enables call recording and chat transcripts at the instance level.

To not record the calls or chats you're monitoring, disable the Amazon S3 buckets.



Set recording and analytics behavior

Specify call recording behavior and configure Contact Lens speech analytics.

Call recording

Enables or disables call recording for the agent, customer, or both. Agent and customer call recordings are required to enable Contact Lens.

● **On**

  ● **Agent** and **Customer**

  ○ **Agent** only

  ○ **Customer** only

○ **Off**

Amazon Connect – Monitor Calls

Assign permissions to monitor live conversations

For managers to monitor live conversations, you assign them the CallCenterManager and Agent security profiles. To allow agent trainees to monitor live conversations, you may want to create a security profile specific for this purpose.

To assign a manager permissions to monitor a live conversation

1. Go to Users, User management, choose the manager, and then choose Edit.

2. In the Security Profiles box, assign the manager to the CallCenterManager security profile. This security profile also includes a setting that makes the icon to download recordings appear in the results of the Contact search page.

3. Assign the manager to the Agent security profile so they can access the Contact Control Panel (CCP), and use it to monitor the conversation.

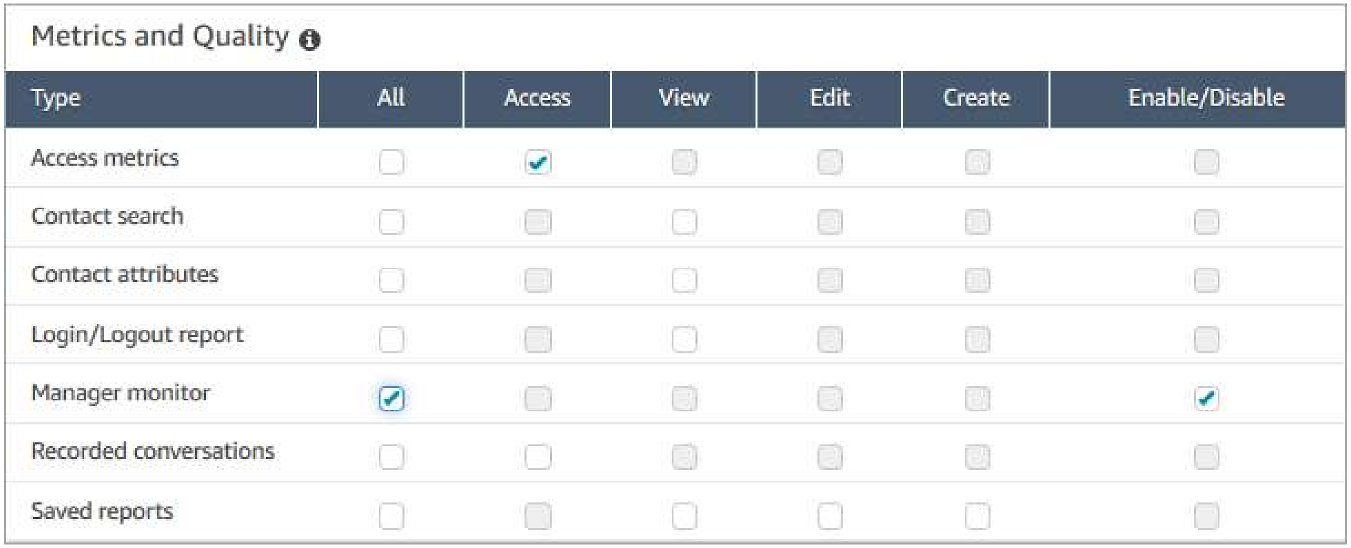
4. Choose Save.

Amazon Connect – Monitor Calls

To create a new security profile for monitoring live conversations

1. Choose Users, Security profiles.
2. Choose Add new security profile.
3. Expand Analytics, then choose Access metrics and Manager monitor**.**

Access metrics is needed so they can access the real-time metrics report, which is where they choose which conversations to monitor.



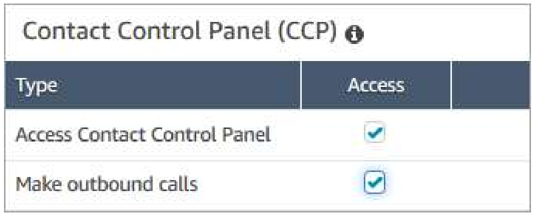
Metrics and Quality

Type	All	Access	View	Edit	Create	Enable/Disable
Access metrics	□	☑	□	□	□	□
Contact search	□	□	□	□	□	□
Contact attributes	□	□	□	□	□	□
Login/Logout report	□	□	□	□	□	□
Manager monitor	☑	□	□	□	□	☑
Recorded conversations	□	□	□	□	□	□
Saved reports	□	□	□	□	□	□

Amazon Connect – Monitor Calls

To create a new security profile for monitoring live conversations

4. Expand Contact Control Panel, then choose Access Contact Control Panel and Make outbound calls.



Contact Control Panel (CCP)

Type	Access	
Access Contact Control Panel	☑	
Make outbound calls	☑	

These permissions are needed so they can monitor the conversation through the Contact Control Panel.

5. Choose Save.

Amazon Connect – Monitor Calls

Monitor live conversations with contacts

Tip - Call barge-in is not currently supported. That is, if you're listening to a conversation, your microphone stays muted.

1. Check that the Set recording and analytics behavior block is in the contact flow you want to monitor. It has to be there whether you're monitoring calls or chats. In the block's Properties, choose Agent and Customer.

2. Log in to your Amazon Connect instance with a user account that is assigned the CallCenterManager security profile, or that is enabled for the Manager monitor permission.

3. Open the Contact Control Panel (CCP) by choosing the phone icon in the top-right corner of your screen. You'll need the CCP open to connect to the conversation.

Amazon Connect – Monitor Calls

Monitor live conversations with contacts

4. To choose the agent conversation you want to monitor, in Amazon Connect choose Analytics, Real-time metrics, Agents.

5. To monitor voice conversations: Next to the names of agents in a live voice conversation, you'll see a headset icon. Choose the icon to start monitoring the conversation.

When you're monitoring a conversation, the status in your CCP changes to Monitoring.

6. To monitor chat conversations: For each agent you'll see the number of live chat conversations they're in. Click on the number. Then choose the conversation you want to start monitoring.

When you're monitoring a conversation, the status in your CCP changes to Monitoring.

7. To stop monitoring the conversation, in the CCP choose End call or End chat.

When the agent ends the conversation, monitoring stops automatically.

Amazon Connect – Monitor Calls

Review recorded conversations

Managers can review past conversations between agents and customers. To set this up, you need to set up recording behavior, assign managers the appropriate permissions, and then show them how to access the recorded conversations.

When is a conversation recorded? A conversation is recorded only when the contact is connected to an agent. The contact is not recorded before then, when they are connected to the IVR. If the call is transferred externally, the call recording stops when the agent drops from the call.

Tip - When call recording is enabled, the recording is placed in your S3 bucket shortly after the contact is disconnected. Then the recording is available for you to review it using the steps in this article.

You can also access the recording from the customer's contact record. The recording is available in the contact record, however, only after the contact has left the After Contact Work (ACW) state.

Amazon Connect – Monitor Calls

How do I manage access to recordings? Use the Recorded conversations (unredacted) security profile permission to manage who can listen to recordings, and access the corresponding URLs that are generated in S3.

Review recordings/transcripts of past conversations

These are the steps that a manager does to review past recordings/transcripts of conversations.

1. Log in to Amazon Connect with a user account that has permissions to access recordings.

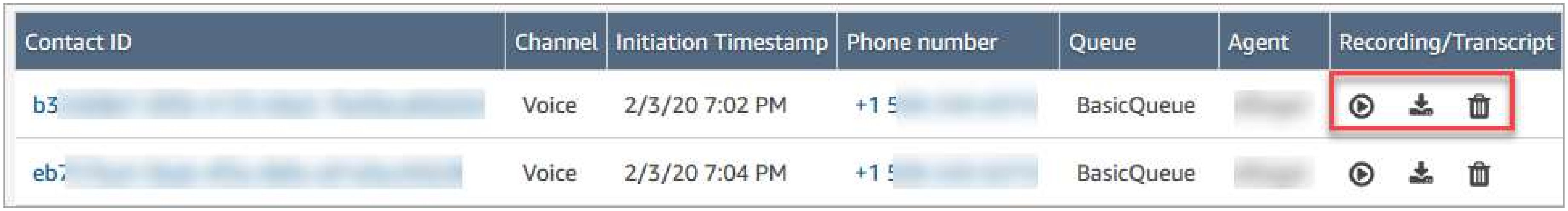
2. In Amazon Connect choose Analytics, Contact search.

3. Filter the list of contacts by date, agent login, phone number, or other criteria. Choose Search.

Tip - We recommend using the Contact ID filter to search for recordings. This is the best way to ensure you get the right recording for the contact. Many recordings have the same name as the contact ID, but not all.

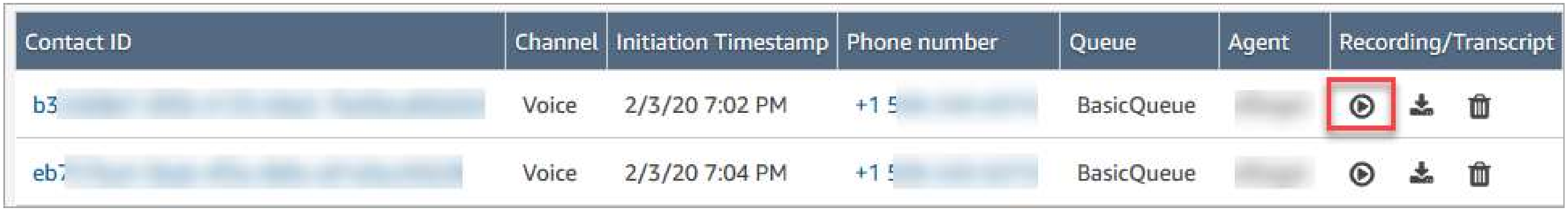
Amazon Connect – Monitor Calls

4. Conversations that were recorded have icons in the Recording/Transcript column. If you don't have the appropriate permissions, you won't see these icons.



Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

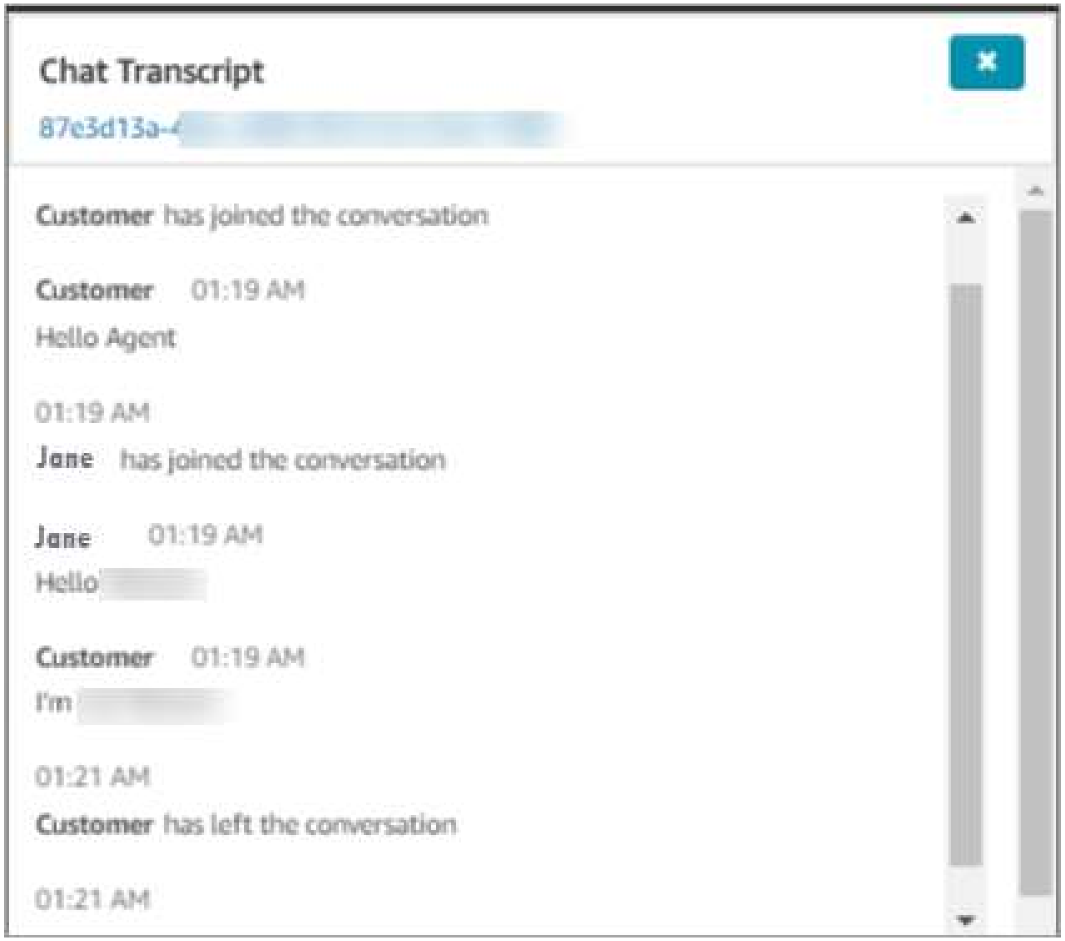
5. To listen to a recording of a voice conversation, or read the transcript of a chat, choose the Play icon.



Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

Amazon Connect – Monitor Calls

6. The following image shows a sample chat transcript.



Chat Transcript

87e3d13a-4[redacted]

Customer has joined the conversation

Customer 01:19 AM
Hello Agent

01:19 AM
Jane has joined the conversation

Jane 01:19 AM
Hello [redacted]

Customer 01:19 AM
I'm [redacted]

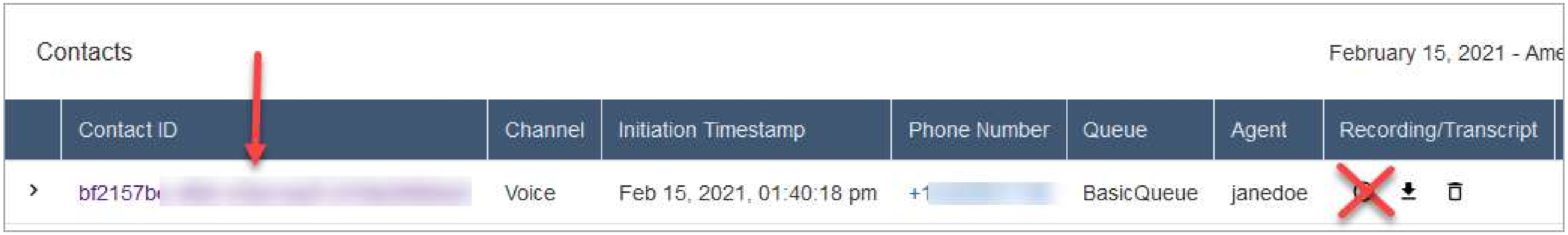
01:21 AM
Customer has left the conversation

01:21 AM

Amazon Connect – Monitor Calls

Pause, rewind, or fast-forward a recording

1. Instead of choosing the Play icon, choose the contact ID to open the contact record..



Contacts

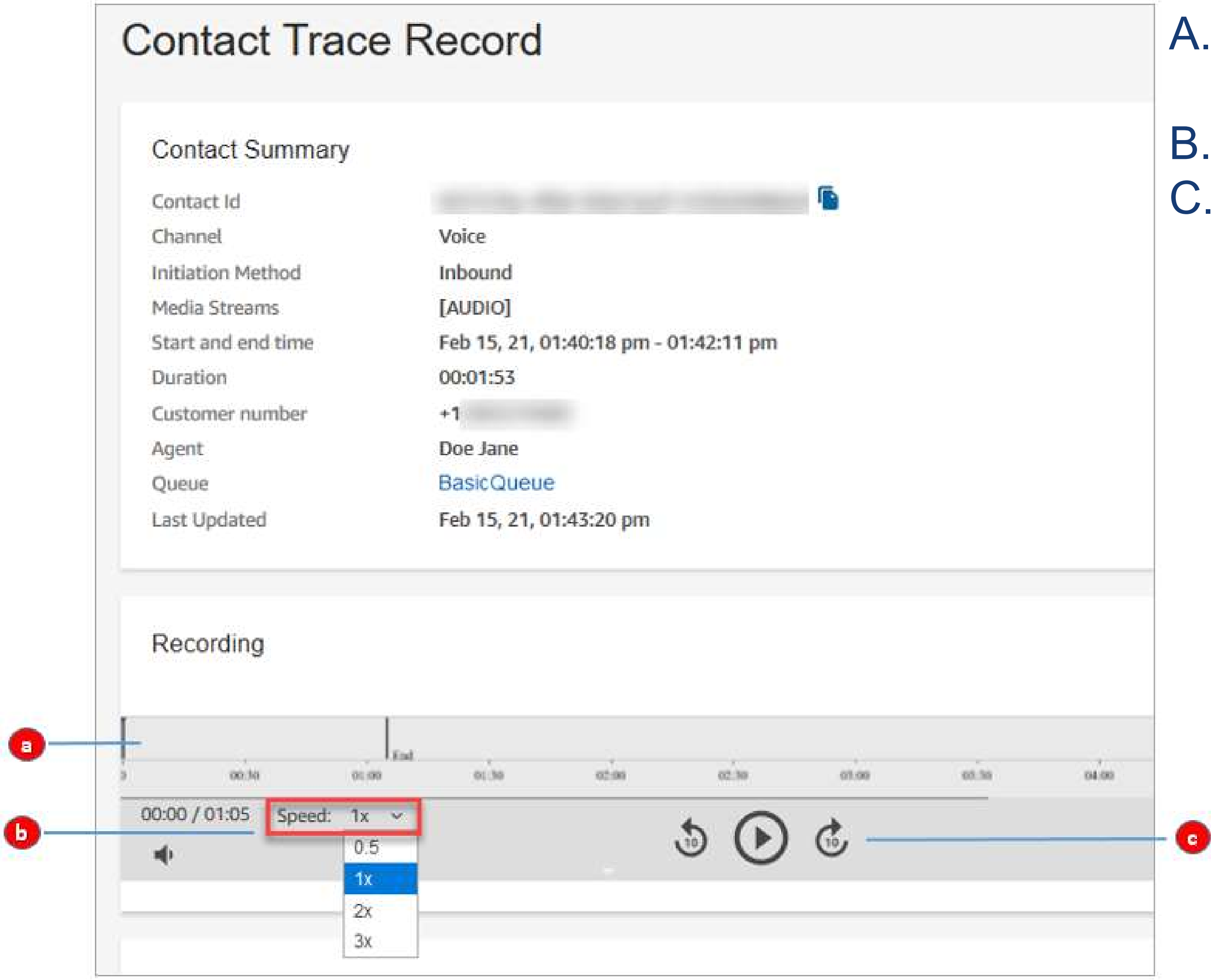
February 15, 2021 - Ame

	Contact ID	Channel	Initiation Timestamp	Phone Number	Queue	Agent	Recording/Transcript
›	bf2157b[redacted]	Voice	Feb 15, 2021, 01:40:18 pm	+1[redacted]	BasicQueue	janedoe	▶ ⬇ 🗑

Amazon Connect – Monitor Calls

Pause, rewind, or fast-forward a recording

2. On the Contact record page, there are more controls to navigate the recording.



Contact Trace Record

Contact Summary

Contact Id	[redacted]
Channel	Voice
Initiation Method	Inbound
Media Streams	[AUDIO]
Start and end time	Feb 15, 21, 01:40:18 pm - 01:42:11 pm
Duration	00:01:53
Customer number	+1 [redacted]
Agent	Doe Jane
Queue	BasicQueue
Last Updated	Feb 15, 21, 01:43:20 pm

Recording

A. Click or tap to the time you want to investigate.
B. Adjust the playing speed.
C. Play, pause, skip backwards or forwards in 10 second increments.

Amazon Connect – Monitor Calls

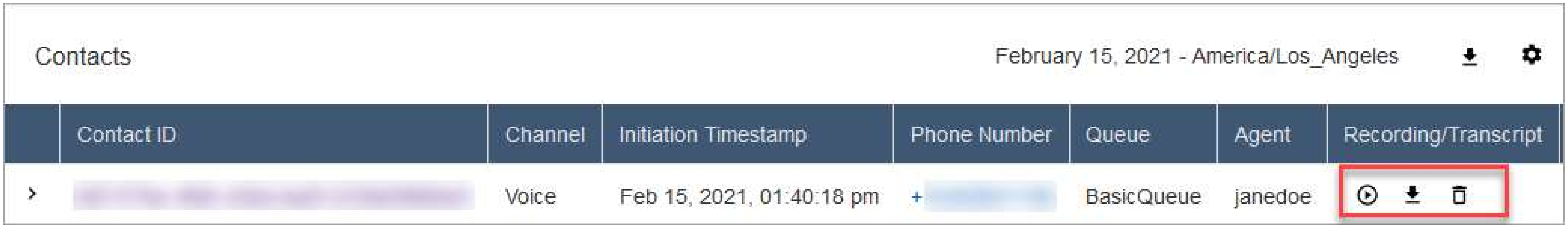
Troubleshoot problems pausing, rewinding, or fast-fowarding

If you are unable to pause, rewind or fast-forward recordings on the Contact search page, one possible reason could be that your network is blocking HTTP range requests. Work with your network administrator to unblock HTTP range requests.

Amazon Connect – Monitor Calls

Assign permissions to review recordings of past conversations

Assign the CallCenterManager security profile so a user can listen to call recordings or review chat transcripts. This security profile also includes a setting that makes the icon to download recordings appear in the results of the Contact search page.

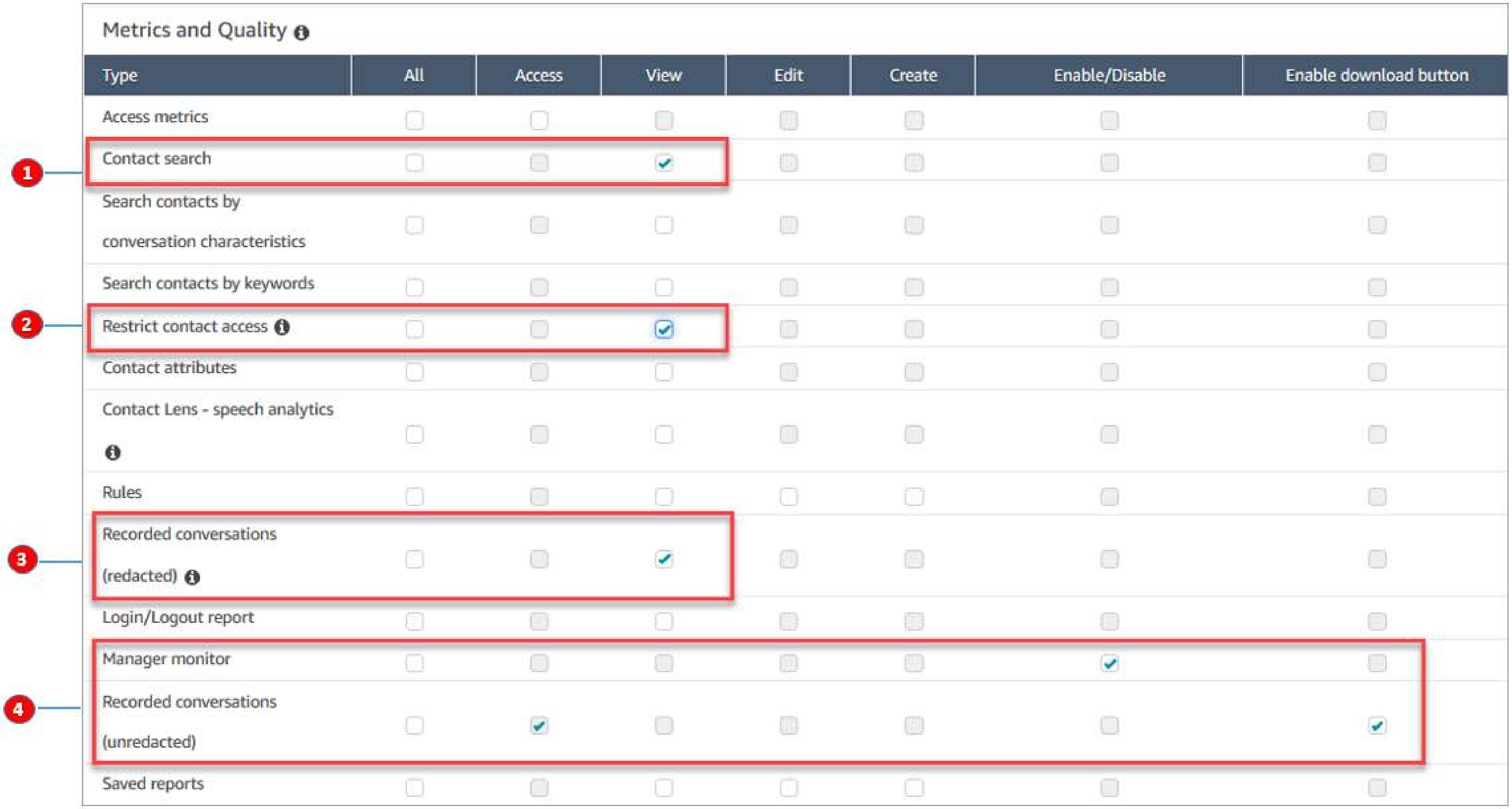


Contacts February 15, 2021 - America/Los_Angeles ⬇ ⚙

	Contact ID	Channel	Initiation Timestamp	Phone Number	Queue	Agent	Recording/Transcript
›	[redacted]	Voice	Feb 15, 2021, 01:40:18 pm	+[redacted]	BasicQueue	janedoe	▶ ⬇ 🗑

Amazon Connect – Monitor Calls

Or, assign the following individual permissions.



Metrics and Quality

Type	All	Access	View	Edit	Create	Enable/Disable	Enable download button
Access metrics	□	□	□	□	□	□	□
Contact search	□	□	☑	□	□	□	□
Search contacts by conversation characteristics	□	□	□	□	□	□	□
Search contacts by keywords	□	□	□	□	□	□	□
Restrict contact access	□	□	☑	□	□	□	□
Contact attributes	□	□	□	□	□	□	□
Contact Lens - speech analytics	□	□	□	□	□	□	□
Rules	□	□	□	□	□	□	□
Recorded conversations (redacted)	□	□	☑	□	□	□	□
Login/Logout report	□	□	□	□	□	□	□
Manager monitor	□	□	□	□	□	☑	□
Recorded conversations (unredacted)	□	☑	□	□	□	□	☑
Saved reports	□	□	□	□	□	□	□

Amazon Connect – Monitor Calls

1. Contact search: This permission is required so users can access the Contact search page, which is where they can search contacts so they can listen to recordings and review transcripts.

2. Restrict contact access: Manage access to results on the Contact search page based on their agent hierarchy group.

For example, agents who are assigned to AgentGroup-1 can only view contact trace records (CTRs) for contacts handled by agents in that hierarchy group, and any groups below them. (If they have permissions for Recorded conversations, they can also listen to call recordings and view transcripts.) Agents assigned to AgentGroup-2 can only access CTRs for contacts handled by their group, and any groups below them.

Managers and others who are in higher level groups can view CTRs for contacts handled by all the groups below them, such as AgentGroup-1 and 2.

For this permission, All = View since View is the only action granted.

Amazon Connect – Monitor Calls

Note - When you change a the hierarchy group of a user, it may take a couple of minutes for their contact search results to reflect their new permissions.

3. Recorded conversations (redacted): If your organization uses Contact Lens for Amazon Connect, you can assign this permission so agents access only those call recordings and transcripts in which sensitive data has been removed.

The redaction feature is provided as part of Contact Lens for Amazon Connect. For more information, see Use sensitive data redaction.

4. Manager monitor: This permission allows users to monitor live conversations and listen to recordings.

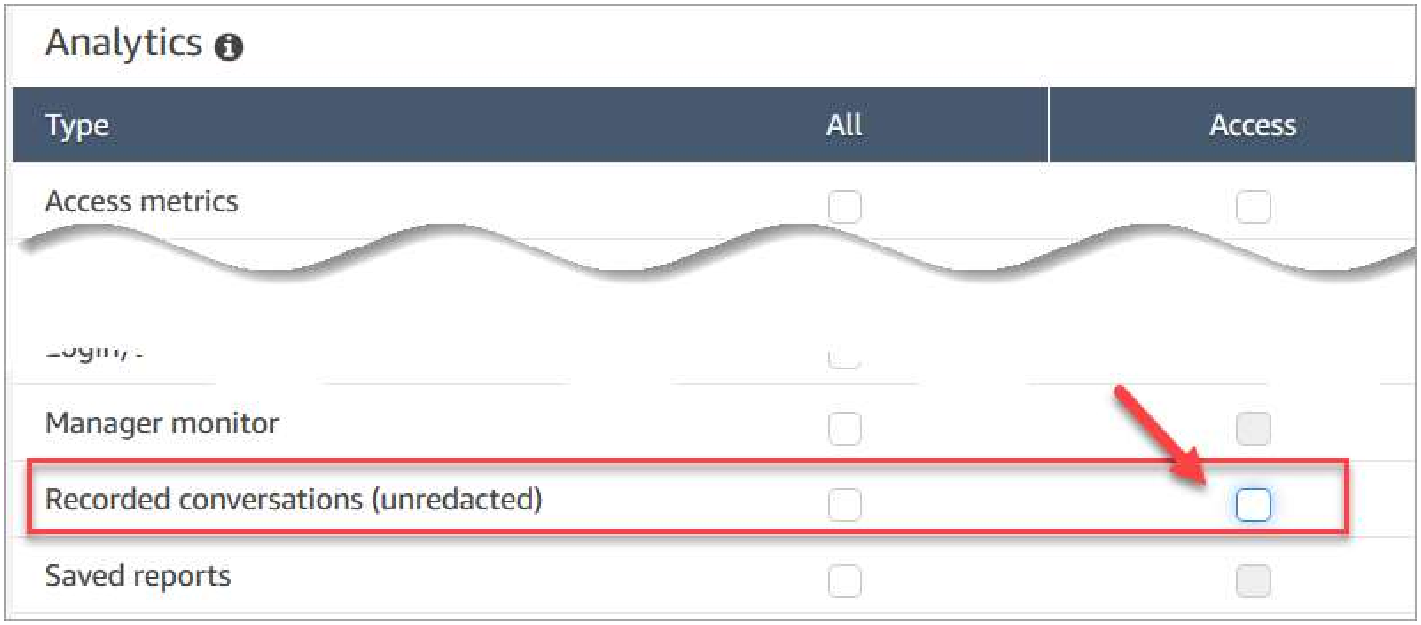
Tip - Be sure to assign managers to the Agent security profile so they can access the Contact Control Panel (CCP). This enables them can monitor the conversation through the CCP.

Amazon Connect – Monitor Calls

5. Recorded conversations (unredacted): If your organization isn't using Contact Lens for Amazon Connect, use this permission to manage who can listen to recordings, access the corresponding URLs that are generated in S3, and delete recordings.

Note the following:

- To restrict access to recordings, ensure users do not have Analytics - Recorded conversations (unredacted) - Access permissions, as shown in the following



Analytics

Type	All	Access
Access metrics	□	□
Manager monitor	□	□
Recorded conversations (unredacted)	□	□
Saved reports	□	□

Amazon Connect – Monitor Calls

- If users do not have Recorded conversations permission—or they're not logged in to Amazon Connect—they cannot listen to the call recording or access the URL in S3, even if they know how the URL is formed.

- The Enable download button permission controls only whether the download button appears in the user interface. It does not control access to the recording.

- To enable a user to delete recordings, choose the Delete permission. By default, the Enable download button permission is granted too so the user can delete recordings through the user interface.

Amazon Connect – Monitor Calls

Download recordings/transcripts of past conversations

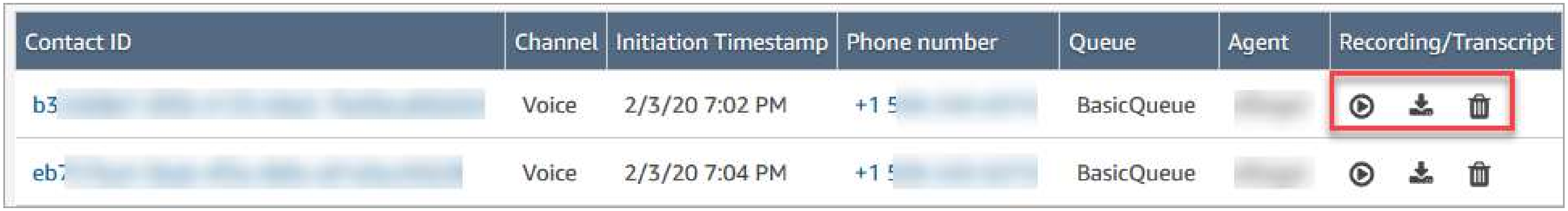
These are the steps that a manager does to download past recordings/transcripts of conversations.

1. Log in to Amazon Connect with a user account that has permissions to access recordings.

2. In Amazon Connect choose Analytics, Contact search.

3. Filter the list of contacts by date, agent login, phone number, or other criteria. Choose Search.

4. Conversations that were recorded have icons in the Recording/Transcript column. If you don't have the appropriate permissions, you won't see these icons.

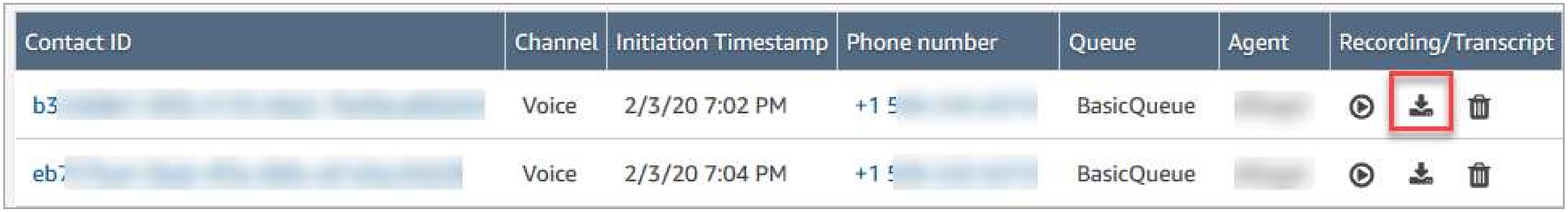


Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

Amazon Connect – Monitor Calls

Download recordings/transcripts of past conversations

5. Choose the Download icon.

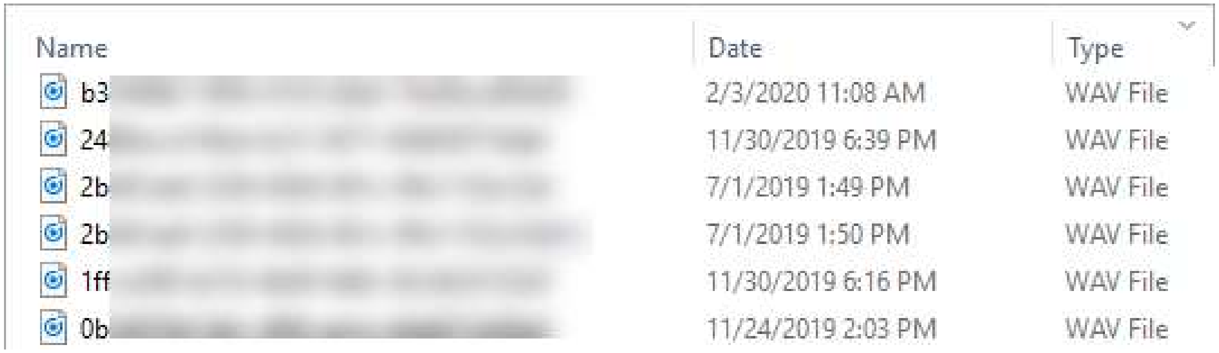


Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

Amazon Connect – Monitor Calls

Download recordings/transcripts of past conversations

6. The recording is saved automatically to your Downloads folder as a .wav file.



Name	Date	Type
b3[redacted]	2/3/2020 11:08 AM	WAV File
24[redacted]	11/30/2019 6:39 PM	WAV File
2b[redacted]	7/1/2019 1:49 PM	WAV File
2b[redacted]	7/1/2019 1:50 PM	WAV File
1ff[redacted]	11/30/2019 6:16 PM	WAV File
0b[redacted]	11/24/2019 2:03 PM	WAV File

The name of the file is the contact ID.

Tip - You may hear only the agent, only the customer, or both the agent and customer in the recording. This is determined by how the Set recording and analytics behavior block is configured.

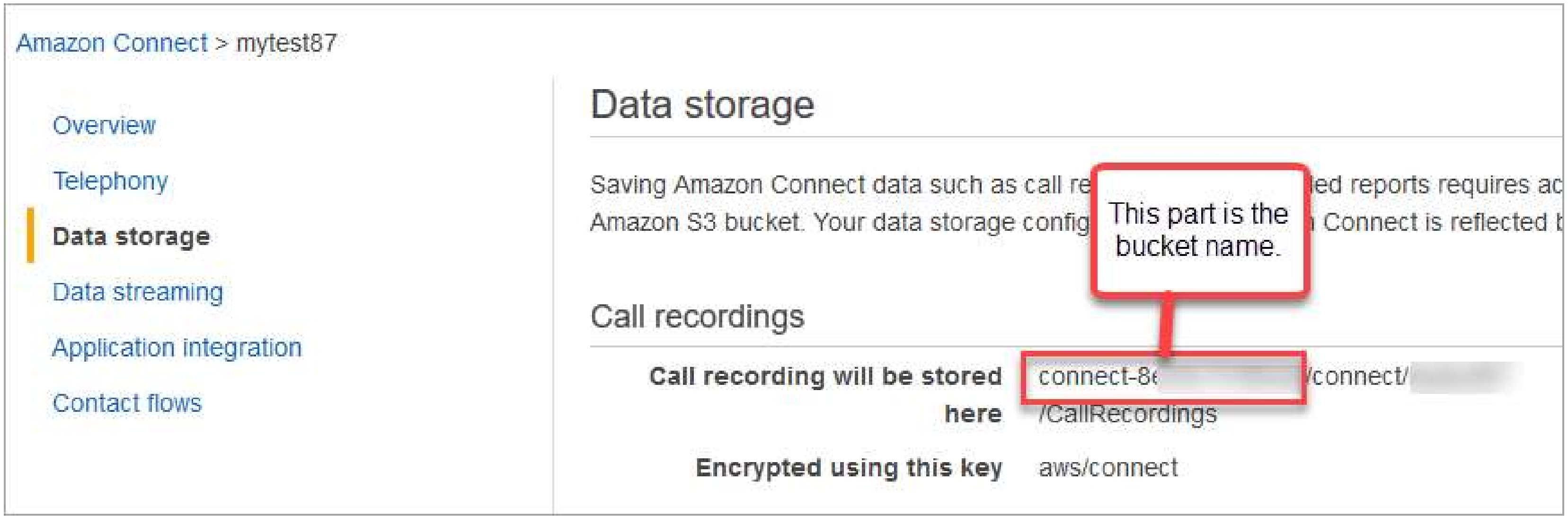
Amazon Connect – Monitor Calls

Track who deleted or listened to recordings

You need an AWS account to do these steps.

Set up logging

1. If you have multiple instances and buckets, look up the name of the Amazon S3 bucket for your instance. Go to the Amazon Connect console, choose the instance alias, and choose Data storage.



Data storage

Saving Amazon Connect data such as call re led reports requires ac
Amazon S3 bucket. Your data storage config Connect is reflected t

This part is the bucket name.

Call recordings

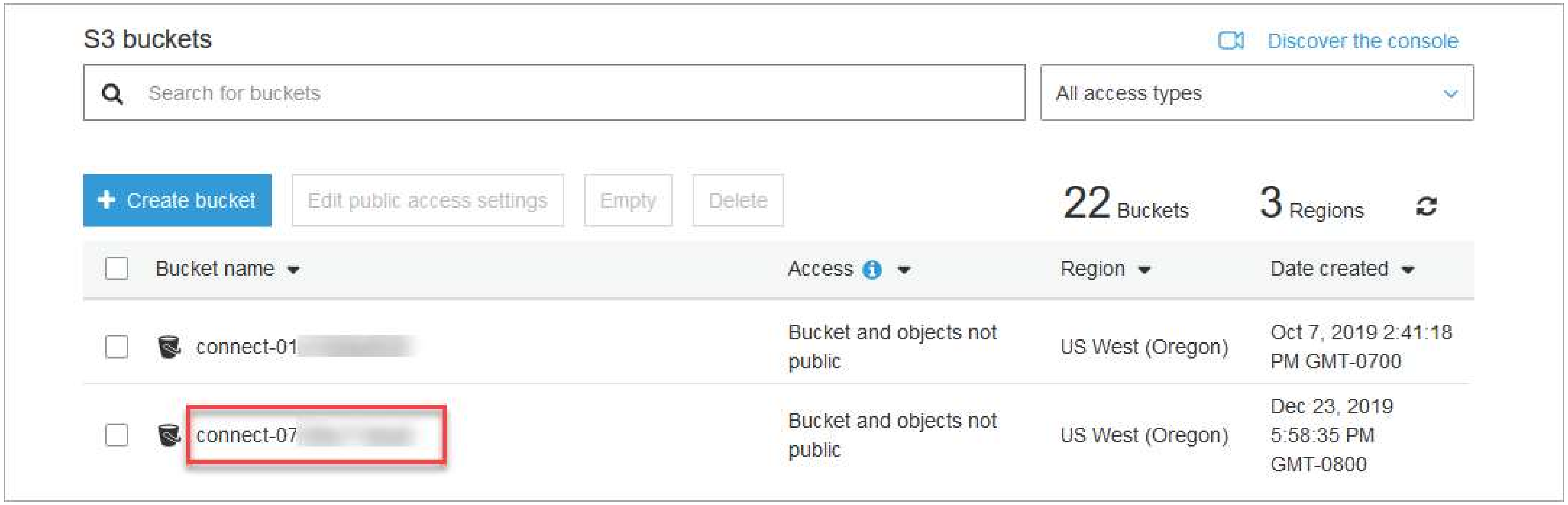
Call recording will be stored here connect-8[redacted]/connect/[redacted]
/CallRecordings

Encrypted using this key aws/connect

Amazon Connect – Monitor Calls

2. Go to the Amazon S3 console.

3. Choose the Amazon S3 bucket where your recordings are stored.



□	Bucket name	Access	Region	Date created
□	connect-01[redacted]	Bucket and objects not public	US West (Oregon)	Oct 7, 2019 2:41:18 PM GMT-0700
□	connect-07[redacted]	Bucket and objects not public	US West (Oregon)	Dec 23, 2019 5:58:35 PM GMT-0800

Amazon Connect – Monitor Calls

4. Choose the Properties tab.

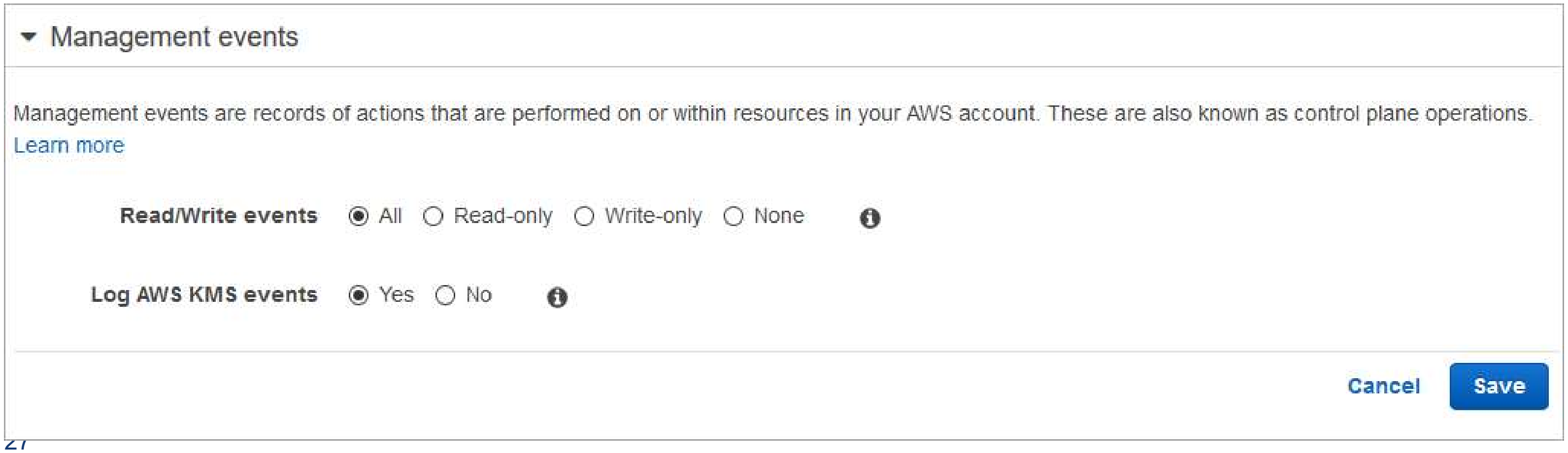
5. Choose Object-level logging and then choose View CloudTrail trails.

It opens the AWS CloudTrail console.

6. In the navigation menu, choose Trails and then choose the trail name.

7. In the upper right corner, toggle Logging to ON, if it's not on already.

8. Under Management events, choose the edit icon. To log only who deletes recordings, you set this to Write-only. To also log who listens to recordings, set to All. Choose Save.



▾ Management events

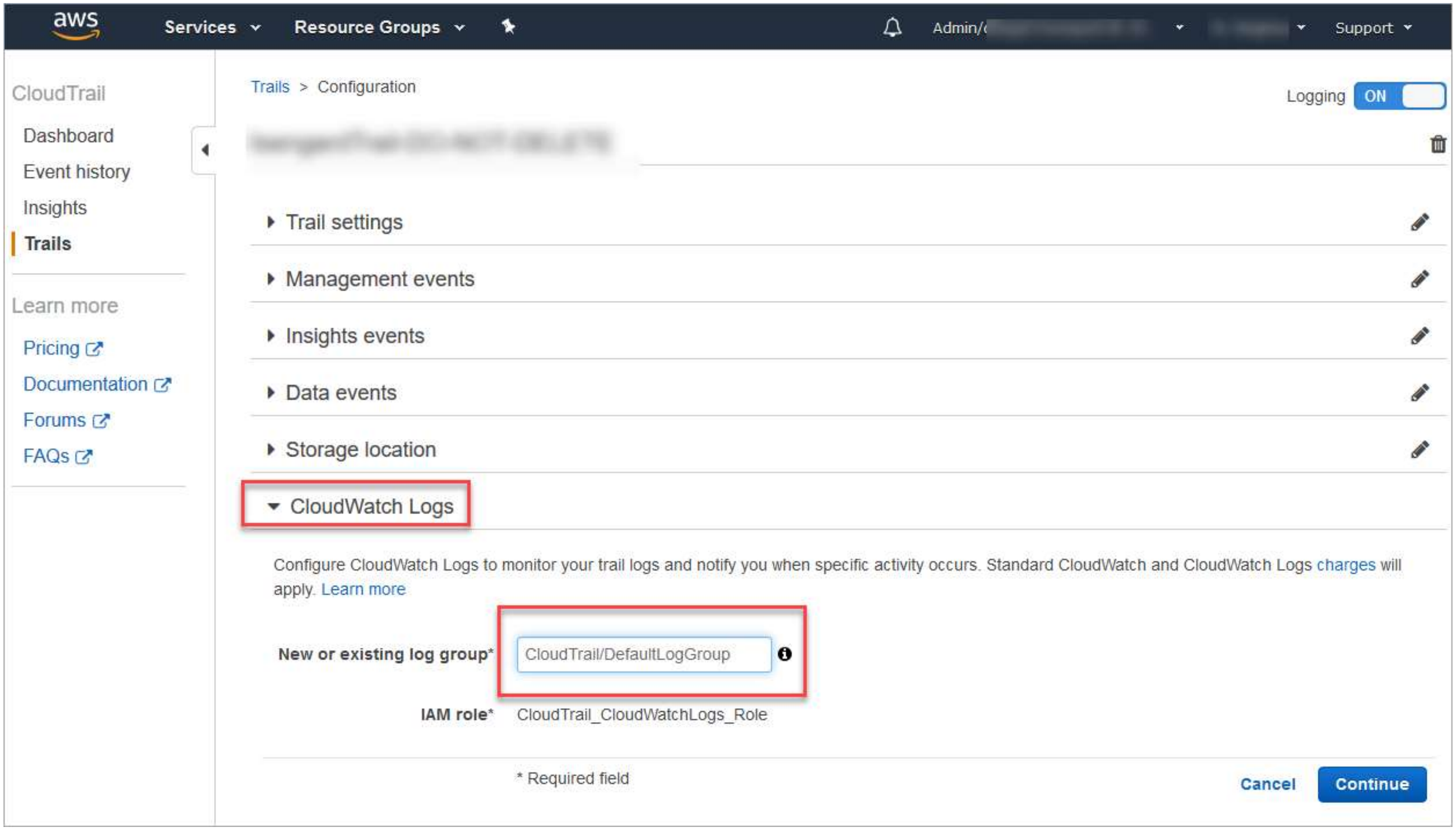
Management events are records of actions that are performed on or within resources in your AWS account. These are also known as control plane operations. Learn more

Read/Write events ● All ○ Read-only ○ Write-only ○ None

Log AWS KMS events ● Yes ○ No

Amazon Connect – Monitor Calls

9. Under CloudWatch Logs choose the edit icon. Either accept the default name for your log group (CloudTrail/DefaultLogGroup), or specify a new name. Choose Continue.



Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges will apply. Learn more

New or existing log group* CloudTrail/DefaultLogGroup

IAM role* CloudTrail_CloudWatchLogs_Role

* Required field

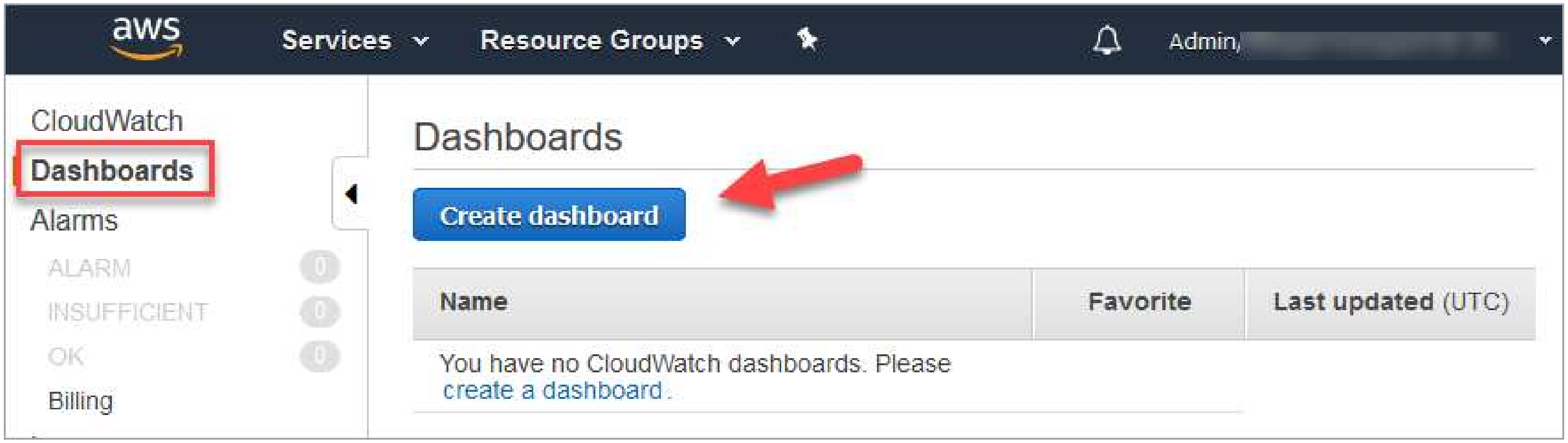
Amazon Connect – Monitor Calls

10. Choose Allow. You can now close the AWS CloudTrail console.

Find who deleted or listened to recordings

1. Go to the Amazon CloudWatch console.

2. Choose Create dashboard.



You have no CloudWatch dashboards. Please create a dashboard.

Amazon Connect – Monitor Calls

3. Enter a name, such as CloudTrail-logging.
4. On the Add to this dashboard dialog box, choose Query results. Choose Configure.
5. In the Select log groups, use the drop-down arrow to choose the log group for your instance, such as CloudTrail/DefaultLogGroup.
6. In the query box, delete the current query, and then copy and paste the one shown below instead. This query will find all API events where the recording was deleted:

```
fields @timestamp, @message
| filter eventSource ='s3.amazonaws.com'
| filter eventName = 'DeleteObject'
```

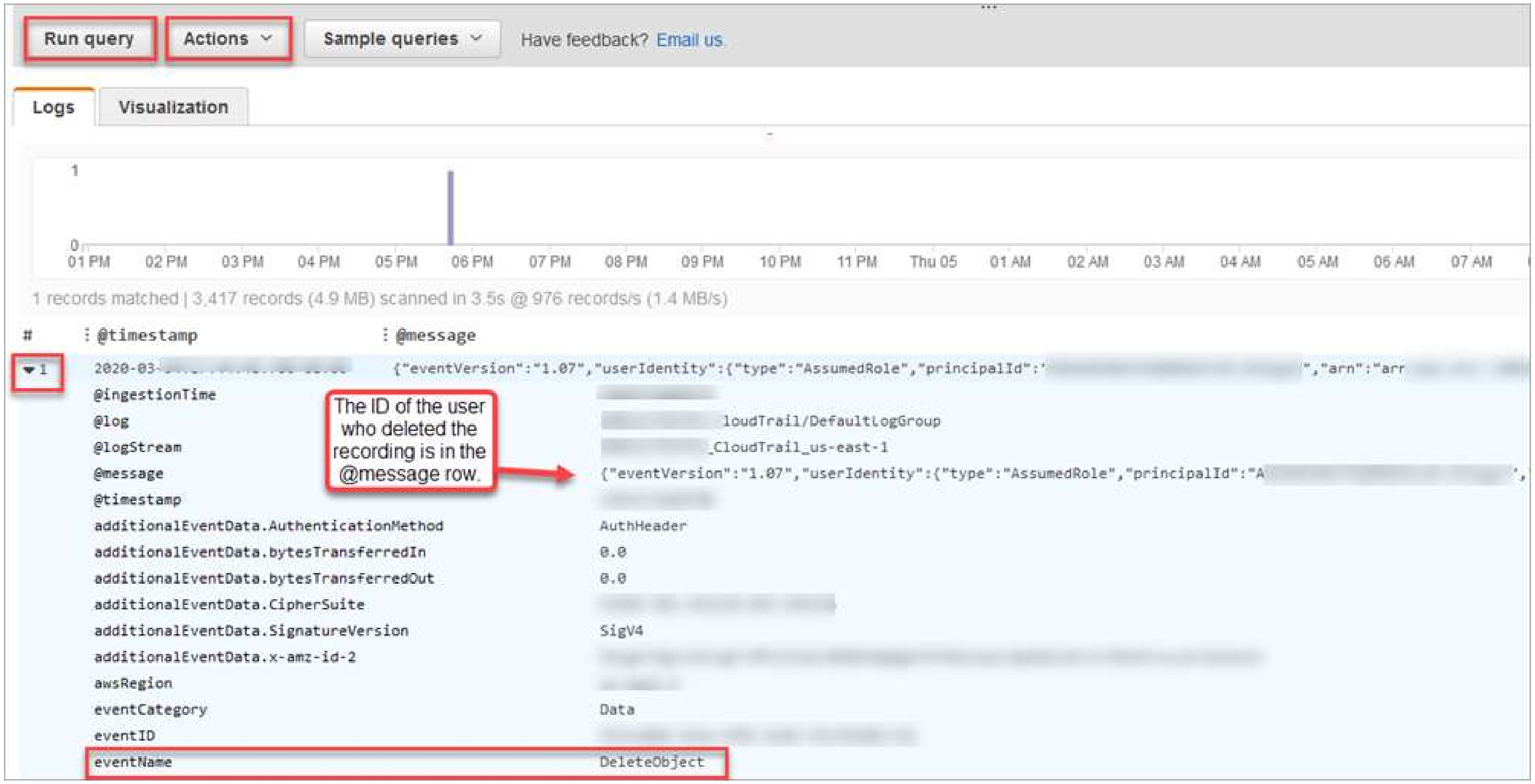
Amazon Connect – Monitor Calls

7. In the time box, choose how far back you want to search.

8. Choose Run query.

It returns all of the events that are named DeleteObject.

9. Next to the event, choose the arrow. It expands to show you detailed information about the event, including the ID of the user who deleted the recording.



1 records matched | 3,417 records (4.9 MB) scanned in 3.5s @ 976 records/s (1.4 MB/s)

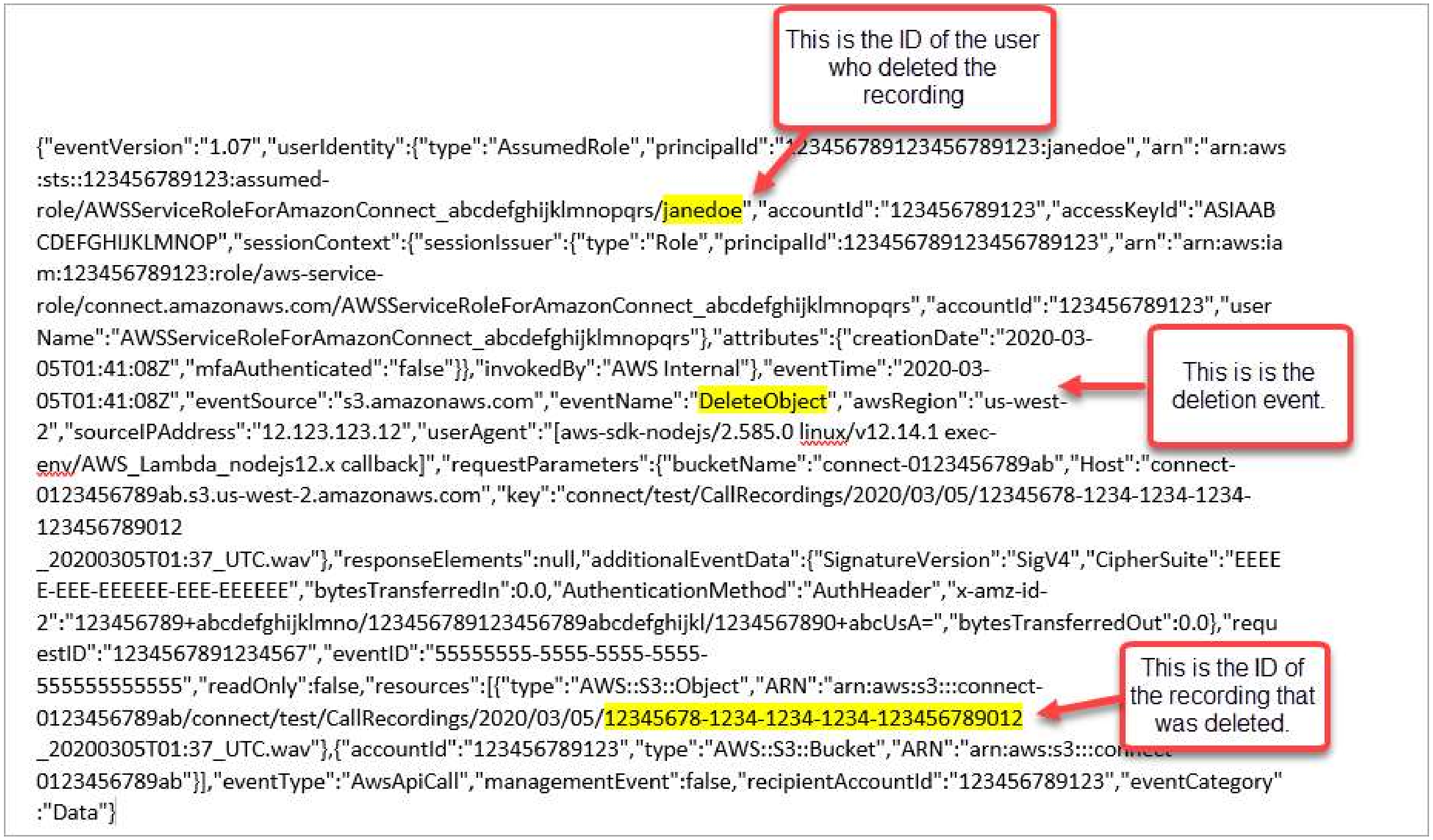
```
#     @timestamp                        @message
▾1    2020-03-[redacted]                {"eventVersion":"1.07","userIdentity":{"type":"AssumedRole","principalId":"[redacted]","arn":"arr[redacted]
      @ingestionTime                            [redacted]
      @log                                      [redacted]loudTrail/DefaultLogGroup
      @logStream                                [redacted]_CloudTrail_us-east-1
      @message                                  {"eventVersion":"1.07","userIdentity":{"type":"AssumedRole","principalId":"A[redacted]",
      @timestamp                                [redacted]
      additionalEventData.AuthenticationMethod  AuthHeader
      additionalEventData.bytesTransferredIn    0.0
      additionalEventData.bytesTransferredOut   0.0
      additionalEventData.CipherSuite           [redacted]
      additionalEventData.SignatureVersion      SigV4
      additionalEventData.x-amz-id-2            [redacted]
      awsRegion                                 [redacted]
      eventCategory                             Data
      eventID                                   [redacted]
      eventName                                 DeleteObject
```

The ID of the user who deleted the recording is in the @message row.

Amazon Connect – Monitor Calls

10. If a lot of records are returned, choose the Actions arrow, and then choose Download query results (CSV). The data is exported to Excel. From there you can format the spreadsheet so it's easier for you to search and see the names of the users who deleted recordings.

The following image shows what the @message column looks like in the CSV file.



```
{"eventVersion":"1.07","userIdentity":{"type":"AssumedRole","principalId":"123456789123456789123:janedoe","arn":"arn:aws
:sts::123456789123:assumed-
role/AWSServiceRoleForAmazonConnect_abcdefghijklmnopqrs/janedoe","accountId":"123456789123","accessKeyId":"ASIAAB
CDEFGHIJKLMNOP","sessionContext":{"sessionIssuer":{"type":"Role","principalId":123456789123456789123","arn":"arn:aws:ia
m:123456789123:role/aws-service-
role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect_abcdefghijklmnopqrs","accountId":"123456789123","user
Name":"AWSServiceRoleForAmazonConnect_abcdefghijklmnopqrs"},"attributes":{"creationDate":"2020-03-
05T01:41:08Z","mfaAuthenticated":"false"}},"invokedBy":"AWS Internal"},"eventTime":"2020-03-
05T01:41:08Z","eventSource":"s3.amazonaws.com","eventName":"DeleteObject","awsRegion":"us-west-
2","sourceIPAddress":"12.123.123.12","userAgent":"[aws-sdk-nodejs/2.585.0 linux/v12.14.1 exec-
env/AWS_Lambda_nodejs12.x callback]","requestParameters":{"bucketName":"connect-0123456789ab","Host":"connect-
0123456789ab.s3.us-west-2.amazonaws.com","key":"connect/test/CallRecordings/2020/03/05/12345678-1234-1234-1234-
123456789012
_20200305T01:37_UTC.wav"},"responseElements":null,"additionalEventData":{"SignatureVersion":"SigV4","CipherSuite":"EEEE
E-EEE-EEEEEE-EEE-EEEEEE","bytesTransferredIn":0.0,"AuthenticationMethod":"AuthHeader","x-amz-id-
2":"123456789+abcdefghijklmno/123456789123456789abcdefghijkl/1234567890+abcUsA=","bytesTransferredOut":0.0},"requ
estID":"1234567891234567","eventID":"55555555-5555-5555-5555-
555555555555","readOnly":false,"resources":[{"type":"AWS::S3::Object","ARN":"arn:aws:s3:::connect-
0123456789ab/connect/test/CallRecordings/2020/03/05/12345678-1234-1234-1234-123456789012
_20200305T01:37_UTC.wav"},{"accountId":"123456789123","type":"AWS::S3::Bucket","ARN":"arn:aws:s3:::connect-
0123456789ab"}],"eventType":"AwsApiCall","managementEvent":false,"recipientAccountId":"123456789123","eventCategory"
:"Data"}
```

This is the ID of the user who deleted the recording

This is is the deletion event.

This is the ID of the recording that was deleted.

Amazon Connect – Monitor Calls

11. If you're also logging who listened to recordings, update the query to search for the eventName GetBucketLocation.

```
fields @timestamp, @message
| filter eventSource ='s3.amazonaws.com'
| filter eventName = 'GetBucketLocation’
```

Tips - Mirroring CloudTrail logs to CloudWatch is useful but optional. Mirroring the CloudWatch log allows you to use CloudWatch Insight to search the events easily.

If you have a large contact center, you may not want to use object logging because it generates many logs that are stored in your Amazon S3 bucket.

Another option is to write an AWS Lambda function to process the CloudTrail events. You can also search the logs manually.

Amazon Connect – Monitor Calls

Search for recordings by contact ID

To find a recording of a specific contact, you only need the contact ID. You don't need to know the date range, agent, or any other information about the contact.

Tip - We recommend using the contact ID to search for recordings.

Even though many call recordings for specific contact IDs may be named with the contact ID prefix itself (for example, 123456-aaaa-bbbb-3223-2323234.wav), there is no guarantee that the contact IDs and name of the contact recording file always match. By using Contact ID for your search on the Contact search page, you can find the correct recording by referring the audio file on the contact's record.

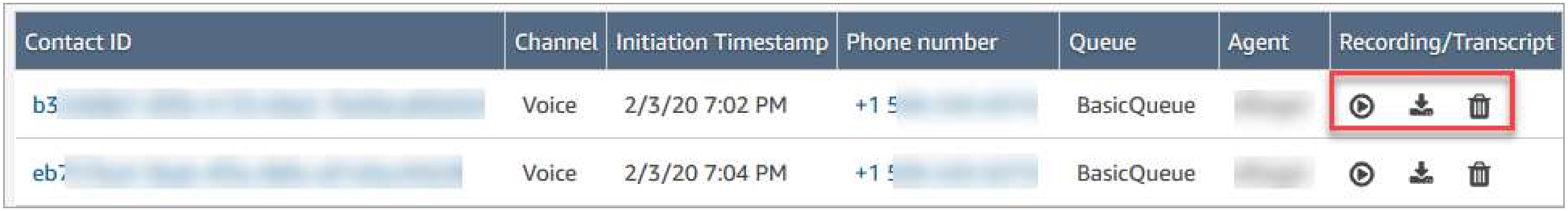
Amazon Connect – Monitor Calls

1. Log in to Amazon Connect with a user account that has permissions to access recordings.

2. In Amazon Connect choose Analytics, Contact search.

3. In the Contact ID, enter the contact ID, and then choose Search.

4. Conversations that were recorded have icons in the Recording/Transcript column. If you don't have the appropriate permissions, you won't see these icons.



Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⤓ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⤓ 🗑

Some layout options

1.4 Million
unfilled computing jobs by 2020[1]

75 Percent
of companies face disruption[2]

$116 Billion
lost productivity per year[3]

Current Options Are Not Solving the Problem

STAFFING AGENCY	CAMPUS HIRING	VISA TALENT	INTERNAL TRAINING	BOOTCAMPS
Do not help with shortage	Not enterprise ready	High compliance & legal costs; delays	Not core competency; bureaucratic	Demand-supply mismatch; fragmented

Quintrix

Sources: (1) Bureau of Labor Statistics. (2) Gartner. (3) CIO Magazine.