PRODUCT DOCUMENTATION

SETTING UP ELEMENTAL LIVE AS THE CONTRIBUTION ENCODER FOR MEDIACONNECT

CONTENTS

© 2019 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.

With AWS Elemental Live 2.14.4 GA and later, you can set up a MediaConnect flow as the output from Elemental Live. In this setup, Elemental Live is the contribution encoder for an AWS Elemental MediaConnect flow. You can choose to encrypt the output during delivery to MediaConnect.

ASSUMPTIONS

- This article assumes you know how to use the AWS Console, AWS IAM, and AWS Elemental MediaConnect, and that you have access to the user guides for the AWS services: What Is AWS Elemental MediaConnect? - AWS Elemental MediaConnect, What Is IAM? - AWS Identity and Access Management , and What Is AWS Secrets Manager? - AWS Secrets Manager .
- This article assumes that you have already set up permissions for MediaConnect. So you have created at least one AWS user and given permissions to those users so that they can use the features of MediaConnect. Specifically, for the purposes of this procedure, the user can create a MediaConnect flow. You have also set up MediaConnect as a trusted entity with Secrets Manager; see this section in the AWS Elemental MediaConnect User Guide: Step 4. Set Up AWS Elemental MediaConnect as a Trusted Entity - AWS Elemental MediaConnect.
- This article does not assume that you have set up Elemental Live with permissions in AWS. Setting up those permissions is one of the steps in this article.

STEP A: CREATE A ROLE IN AWS IAM AND ATTACH POLICIES

You must use the IAM (Identity & Access Management) service to set up Elemental Live as an AWS user (the "Elemental Live user") and give it permissions so that it can communicate with Secrets Manager and MediaConnect. You must:

- Create policies that contain specific permissions.
- Create the "Elemental Live user" in your AWS account. The user must be in the same AWS account as the user who is operating AWS Elemental MediaConnect.
- Associate the Elemental Live user with those policies, which gives the user the permissions of those policies.

CREATE A POLICY FOR ELEMENTAL LIVE TO MAKE REQUESTS TO MEDIACONNECT

Elemental Live must have permissions on MediaConnect. Follow this procedure to set up these permissions:

1. Log into the AWS console and go to the IAM console.
2. On the left menu, choose Policies. Use the filters to determine if there is already a policy with a name similar to "ElementalAccessToMediaConnect".

© 2019 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.

3. If the policy does not exist, choose Create policy. Click the Visual editor tab and create the policy using the IAM policy generator. This generator lets you choose the service from a list and then choose operations from a list:
   - Service: MediaConnect.
   - Actions:Under List, click DescribeFlow.
   - Resources: If your organization does not have strict rules about accessing containers on MediaConnect, you can ignore this section; you will have access to all flows. Otherwise, follow your internal policies to identify specific flows.
   - Give the policy a name such as "ElementalAccessToMediaConnect"

For detailed instructions on creating a policy, see Creating IAM Policies - AWS Identity and Access Management.

CREATE A POLICY FOR ELEMENTAL LIVE TO MAKE REQUESTS TO SECRETS MANAGER

If you plan to encrypt the output from Elemental Live when you send it to MediaConnect, then Elemental Live must have permissions on AWS Secrets Manager. Follow this procedure to set up these permissions:

1. Log into the AWS console and go to the IAM console. Choose Policies and look for a policy that gives MediaConnect the permissions for Secrets Manager. If you or someone else previously followed the procedure in Step 3. Set Up a Policy for AWS Elemental MediaConnect - AWS Elemental MediaConnect, then this policy will be called "SecretsManagerReadSecrets".
2. If this policy exists, make sure it contains the following actions:
   - DescribeSecret
   - GetResourcePolicy
   - GetSecretValue
   - ListSecretVersionIds
3. Also make sure that the resources section gives access to the ARN of the secret that you will use. Read the information in IAM Policy Examples for Secrets in AWS Secrets Manager - AWS Elemental MediaConnect. You may need to edit the policy to include the ARN for this secret in the resources section.
4. If the policy does not exist, follow the procedure in Step 3. Set Up a Policy for AWS Elemental MediaConnect - AWS Elemental MediaConnect to create the policy.

CREATE A USER

1. Log into the AWS console and go to the IAM console.
2. If the user does not exist or it does exist but you want to create separate users for each Elemental product, choose Add User. (Note that you may want separate users for separate *products*, but there is probably no need to create a separate user for each Elemental *node*.) Follow the prompts to add the user with this information:

© 2019 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.

- Give the user a name such as "ElementalUser".
- For Access type, choose Programmatic access. Do not choose Console access.
- In permissions, choose Attach existing policies directly. Attach the policies you created above. For example, "ElementalAccessToMediaConnect" and "SecretsManagerReadSecrets".
- Ignore tags.

3. Create the user and choose Close.
4. Choose the user by clicking the name, for example, click ElementalUser.
5. Choose the Security tab.
6. Click "Create Access Key".
7. On the Create access key dialog, choose to download the .csv file. Save the file in a safe place, so that you have a permanent record of the access key ID and the Secret access key.
   The Access key ID looks like this:AKIAIOSFODNNYEXAMPLE
   The Secret access key looks like this:
   wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
8. Give the Access key ID and the Secret access key to the Elemental Live operator.
   Do *not* give the username and password to the operator.
9. How it works: You have created an AWS user with the permissions required to make requests to MediaConnect and optionally to Secrets Manager. When the Elemental Live user sets up the output with MediaConnect as the destination, they will enter the Access key ID and Secret access key. When the Elemental Live event is running, Elemental Live sends these two IDs to the AWS services, instead of sending the user name and password. These IDs provide authorization for the Elemental Live node to make requests to the AWS services.

STEP B: SET UP FOR ENCRYPTION (OPTIONAL)

If you are encrypting the Elemental Live output, you must generate an encryption key and set it up in Secrets Manager. In this scenario, Secrets Manager is effectively acting as the key server for the encryption key. The Secrets Manager serves the key to Elemental Live so it can encrypt and to MediaConnect to it can decrypte. In this scenario, encryption/decryption is supported with a static SHA-256 encryption key and using the AES-256, AES-192, or AES-128 algorithm.
Perform the following steps according to the security policies and procedures for your organization.

1. Use a suitable tool for generating a SHA-256 encryption key from a seed that you specify. AWS does not provide a generation tool. Note that you need only one key, even if you are creating two flows.

© 2019 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.

2. Save the key to the AWS Secrets Manager, as described in Encryption in Transit - AWS Elemental MediaConnect. You must assign a name to the secret, for example, "key_sports". Save the key in the same region as the flow you plan to create.
3. Make a note of the ARN for this secret. You need this ARN when you create the MediaConnect flow. It looks like the following example, where "key_sports" is the name you assigned to the secret.

   arn:aws:secretsmanager:us-west-2:111122223333:secret:key_sports-3i8QE0

STEP C: CREATE THE MEDIACONNECT FLOWS

You must follow this procedure before you create the Elemental Live outputs because Live needs data that is generated by this procedure.

1. Create one or two MediaConnect flows. (Create two flows if your have set up Elemental Live for output redundancy using output locking. If you have not set up redundant outputs, create one flow.)
2. Follow the procedure in https://docs.aws.amazon.com/mediaconnect/latest/ug/flows-create.html in the *AWS Elemental MediaConnect User Guide.*
3. Complete Availability Zone and Name as appropriate. These fields do not relate to using Elemental Live as the source.
4. In the Source section, follow the steps for setting up a standard source. Specifically:
   - Protocol: Zixi push.
   - Whitelist CIDR block: This is the IP address (in CIDR format) of the Elemental node that will be delivering to this flow. It must be a public facing IP address. Speak to your organization's administrator for a value to enter here.
   - Stream ID: You must enter a value when Elemental Live is the source.
5. If you are encrypting the video, check Enable in the Decryption section and complete the fields as described in the MediaConnect documentation. Specifically:
   - Decryption type: Always Static key.
   - Role ARN: The role that has been set up for MediaConnect to be a trusted entity with Secrets Manager. See this section of the AWS Elemental MediaConnect User Guide: Step 4. Set Up AWS Elemental MediaConnect as a Trusted Entity - AWS Elemental MediaConnect. You must specify this role ARN here so that MediaConnect can obtain the encryption key.
     To fine the ARN for the role, go to the IAM console, choose Roles, click the name of the role, and look at the Role ARN field in the Summary.
     The role ARN looks like this:
     arn:aws:iam::111122223333:role/MediaConnectASM
   - Secret ARN: The ARN you obtained in step A, for example:
     arn:aws:secretsmanager:us-west-2:111122223333:secret:key_sports-3i8QE0

© 2019 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.

- Decryption algorithm: Specify the algorithm that you want to use. Elemental Live will be instructed to use this algorithm to encrypt. MediaConnect will read this information and use this algorithm to decrypt.

6. When you create each flow, MediaConnect creates an ARN for that flow. The ARNs look like the following, where "curling_finals_A" and "curling_finals_B" are the flow names you specified in each flow:

   ```
   arn:aws:mediaconnect:us-west-
   1:111122223333:flow:1bgf67:curling_finals_A
   arn:aws:mediaconnect:us-west-
   1:111122223333:flow:9pmlk76:curling_finals_B
   ```

7. Make a note of these ARNs. You need them to set up the Elemental Live output(s).

STEP D: CREATE THE ELEMENTAL LIVE OUTPUT GROUP

You must create one output group of type "Reliable TS". Inside that group, you must create one or two outputs: create two outputs if you created two MediaConnect flows, create one output if you created only one flow.

1. In the Elemental Live event, go to Output Groups > Reliable TS.
2. Click Add Output to create an output in this Reliable TS output group.
3. Complete the fields in each output as follows:
   - Delivery Protocol: Choose AWS Elemental MediaConnect.
   - Destination/Amazon Resource Name: Enter the ARN for the flow. Following from the example above, enter the following in the first output:
     ```
     arn:aws:mediaconnect:us-west-
     1:111122223333:flow:1bgf67:curling_finals_A
     ```
   - Interface: Optional; see the tooltip.
   - Lock icon: Click this icon. Two more fields appear:
     - Username/Access Key ID: The Access key ID for the user you created in AWS IAM. For example, AKIAIOSFODNNYEXAMPLE
     - Password/Secret Access Key: The Secret access key for this user. For example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
4. Note that there is no encryption field. See "How It Works at Runtime", below, to understand how encryption is handled.
5. Repeat these steps to create a second output in this output group, if applicable. Use the same Access key ID and Secret access key.

HOW IT WORKS AT RUNTIME

Here is the data that Elemental Live has: The flow ARN. The Access key ID and Secret access key. Here is the data that MediaConnect has: The flow ARN. The destination IPs and protocol details. The encryption type and algorithm. The role ARN (for obtaining the

© 2019 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.

secret - the encryption key). The secret ARN. When the event starts, Elemental Live authenticates with AWS using the AWS access key ID and AWS secret access key. It then sends the flow ARN to MediaConnect. MediaConnect accepts the request because Elemental Live has permission to make requests to MediaConnect. MediaConnect looks up the flow and determines if the flow is set up for encryption.

- If the flow is set up for encryption, MediaConnect sends the encryption type and algorithm information, and the secret ARN to Elemental Live. Elemental Live uses the secret ARN to get the secret (the encryption key) from Secrets Manager. Secrets Manager accepts the request from Elemental Live because Elemental Live has permission to get this secret.
  Elemental Live uses the encryption key to encrypt the video and sends the encrypted video to MediaConnect.
  MediaConnect in its turn uses the secret ARN to get the secret (the encryption key) from the Secrets Manager. Secrets Manager accepts the request from MediaConnect because MediaConnect has permission to get this secret; it has permission because it has been set up as a trusted entity with Secrets Manager. MediaConnect uses the encryption key to decrypt the video.
- If the flow is not set up for encryption, MediaConnect instructs Elemental Live to deliver the video unencrypted. Secrets Manager is not involved.

© 2019 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.