Create a remote log source (AWS CloudTrail)

⚠ To obtain Log Relay and to configure your account for remote log collection, you must have the following AMP permissions added to your account:

- Write Virtual Machine
- Delete Log Management
- Read Log Endpoints
- Read Log Relays
- Write Log Relays
- Delete Log Relays

⚠ In your AWS account, you must have read privileges for AWS S3 buckets and AWS CloudTrail.

You can use this document to add a remote log collector to a AWS CloudTrail remote device (log source).

Pre-Deployment Considerations

AWS Account Information

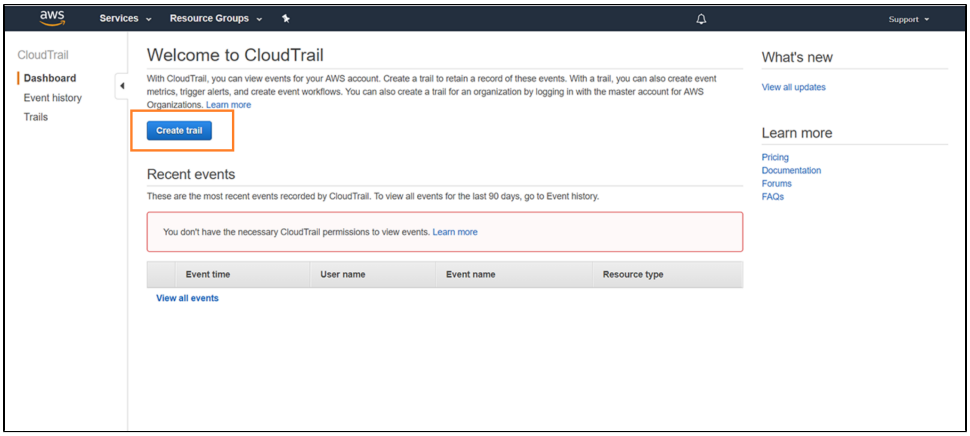
1. Access your AWS console.
2. In the top, right corner, locate and copy your account number and corresponding region. You will need this information later.

Create a remote log source

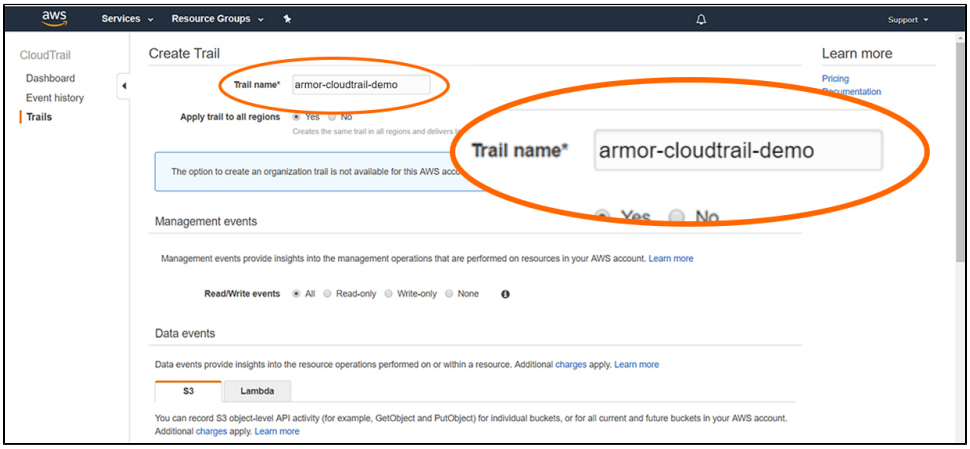
1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **External Sources**.
4. Click the plus (+) sign.
    - If you do not have any log sources already created, then click **Add a New Log Source**.
5. Complete the missing fields:
    - In **Endpoint**, select the available Armor Endpoint.
    - In **Log Source Type**, select **Amazon AWS CloudTrail**.
    - In **Log Source Identifier**, confirm that the listed system hostname matches the system for log collection.
        - This field will populate after you complete the **Account Number** field.
    - In **Protocol**, confirm that **Amazon AWS S3 REST API** is selected.
    - In **Account Number**, paste the AWS account number that you copied early. You must remove any dashes or hyphens (-).
    - In **Region to Monitor**, select the region that corresponds to the account number.
6. Click **Save Log Source**.
7. In the pop-up window, copy and paste the URL text. You will need this information in the AWS console.
8. Click **Return to the Log Source List**. You will be redirected to the **External Sources** screen.
9. In the **External Sources** screen, refresh the screen until the log source reaches an **Online** status.

Create a new trail and sync your AWS S3 bucket

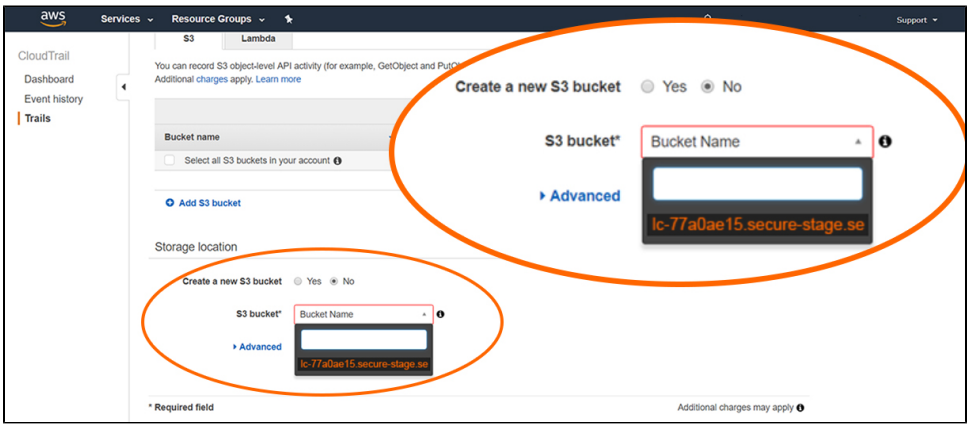
1. In the AWS console, navigate to the AWS CloudTrail section.
2. Update your account's region settings to match the region previously selected in AMP.
3. Click **Create trail**. (You may first need to click **View trails**, and then click **Create trail**.)



4. In **Trail name**, enter a descriptive name.



5. For **Apply trail to all regions**, mark **No**.
6. For **Create a new S3 bucket**, mark **No**.



7. In **S3 bucket**, paste the bolded URL text that you copied earlier from AMP.
8. Click **Create**.

Verify Connection in AMP

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**, and then select **External Sources**.
3. Locate the newly created remote log source.
4. Under **Last Event**, verify that a recent activity took place.
    - This status will indicate that the configurations were successful.
    - After you update your AWS account, it may take 30 minutes for AMP to display the updates.

Additionally, you can view the actual logs to confirm that the configuration was successful.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**, and then select **Search**.
3. In the search field, enter your AWS account number surrounded by asterisks wildcards.
    - For example, you can enter ***123456789123***
    - This action will display collected AWS CloudTrail logs.

Troubleshooting

If you are having issues adding a remote log collector to an AWS CloudTrail remote device, consider that:

- You need to update your permissions in AWS.
    - You must have read privileges for S3 buckets and write privileges for AWS CloudTrail.
        - Your account must be assigned to the **AWSCloudTrailFullAccess** policy. To learn more the permissions (policies) for AWS CloudTrail, please see the documentation in AWS.
- Ensure that the region you entered in AMP matches your AWS account's region.
- If you are having difficult searching for your logs, consider entering you AWS account number surrounded by asterisks wildcards, such as ***123456789123*.**

Was this helpful?

Your Rating: Results: 3 rates