

RSA NetWitness Platform

Event Source Log Configuration Guide



AWS CloudTrail

Last Modified: Monday, September 13, 2021

Event Source Product Information:

Vendor: [Amazon Web Services](#)

Event Source: AWS CloudTrail

Versions: all

RSA Product Information:

Supported On: Security Analytics 10.5 and later

Event Source Log Parser: cef

Collection Method: cloudtrail

Event Source Class.Subclass: Host.Cloud

Note: This plugin will be deprecated soon. Customers using NetWitness Platform version 11.5 or later can use either the [Amazon cloudwatch](#) plugin or [S3 Universal Connector](#) to capture cloudtrail logs.

To configure AWS CloudTrail, complete these tasks

- I. Configure the AWS CloudTrail event source
- II. Configure the Log Collector for CloudTrail Collection

Configure the AWS CloudTrail Event Source

AWS CloudTrail is a web service that records AWS API calls. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. RSA NetWitness Platform can collect all of this information.

Note: The AWS plugin is meant only for collecting from AWS CloudTrail logs, and not for collecting from arbitrary logs in S3 buckets (under arbitrary directories). The AWS CloudTrail logs are sent in JSON format, as detailed in the AWS documentation here: <http://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-event-reference.html>.

Perform the following tasks:

- I. Set Up CloudTrail in AWS
- II. Provide Read Permissions to an IAM user for an S3 Bucket

Set Up CloudTrail in AWS

You need to work with three AWS services:

- IAM: this is where you create your user or users.
- S3: this is where you create a bucket that holds the logs.
- CloudTrail: you need to enable this service.

To set up CloudTrail in AWS:

1. Create an Amazon AWS account at <https://aws.amazon.com>.
2. Create a user for the IAM (Identity and Access Management) service.
Your user is given an access key and a secret access key. Make sure to record the secret access key, as you cannot see this except at sign up.
3. In the S3 service, create a bucket. You need to remember the values you enter here, as you need them later when you configure the event source in RSA NetWitness Platform.
 - a. Enter a name.
 - b. Select a region.
 - c. **Optional.** Enter a prefix.
4. Enable the CloudTrail service.
5. Attach a policy that allows users access to the bucket that you created in step 3.

Provide Read Permissions to an IAM user for an S3 Bucket

In the IAM service area, you can either create a new user, or edit an existing IAM user. General documentation for managing IAM users can be found here:

<https://aws.amazon.com/iam/details/manage-users/>.

You need to give this user read permissions for the S3 bucket used in your CloudTrail configuration, and also give read access to the subfolders that CloudTrail uses for logging.

- AWS provides a policy generator here: <https://awspolicygen.s3.amazonaws.com/policygen.html>.
- To see examples, visit <https://docs.aws.amazon.com/AmazonS3/latest/dev/example-policies-s3.html>.

A policy for a given bucket called **poc.logcollector.rsa.emc.com** might look like this:

```
{ "Version": "2012-10-17", "Statement": [ { "Action": [ "s3:Get*", "s3:List*" ], "Effect": "Allow", "Resource": [ "arn:aws:s3:::poc.logcollector.rsa.emc.com", "arn:aws:s3:::poc.logcollector.rsa.emc.com/*" ] } ] }
```

Note: In the policy code above, replace *poc.logcollector.rsa.emc.com* with the bucket name that you created. For us-gov regions, `arn` path in "Resource" should be **arn:aws-us-gov:s3**.

Bucket names are restricted as follows:

- Bucket names can only contain lowercase letters, numbers, and hyphens
- Bucket names should be between 3 and 63 characters long
- Bucket names should not end with a hyphens

Set Up the CloudTrail Event Source in NetWitness Platform

In RSA NetWitness Platform, perform the following tasks:

- Deploy the CEF parser and AWS CloudTrail transform file from Live.
- Configure the event source.

Other information provided:

- Descriptions of AWS CloudTrail parameters
- Troubleshooting information

Deploy the AWS Files from Live

AWS CloudTrail uses the `cef` parser.

To deploy the `cef` parser from Live:

1. In the RSA NetWitness Platform menu, select **Live**.
2. Browse Live for the `cef` parser, using **RSA Log Device** as the **Resource Type**.
 - The `cef` parser, using **RSA Log Device** as the **Resource Type**.
 - The `awscloudtrail` transform file, using **RSA Log Collector** as the **Resource Type**
3. Select the `cef` parser.
4. Click Deploy to deploy the `cef` parser to the appropriate Log Decoders, using the Deployment Wizard.
5. Repeat steps 2–4 for the `awscloudtrail` transform file, using **RSA Log Collector** as the **Resource Type**.

For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic, or the [Live Services Management Guide](#).

Configure the AWS Cloudtrail Event Source

To configure the AWS CloudTrail Event Source:

1. In the RSA NetWitness Platform menu, select **Administration > Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View > Config**.

3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

The Event Categories panel displays the File event sources that are configured, if any.

4. In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.

5. Select **cloudtrail** from the list, and click **OK**.

The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.

The screenshot shows the 'Add Source' dialog box with the following fields and values:

- Name * (empty)
- Enabled
- Account ID * (empty)
- S3 Bucket Name * (empty)
- Access Key * (empty)
- Secret Key * (masked with asterisks)
- Region * (us-east-1)
- Region Endpoint (empty)
- Start Date * (0)
- Log File Prefix (empty)

A note below the Log File Prefix field reads: "If the CloudTrail account is configured with a Log File Prefix, this field is required." The dialog also features a 'Test Connection' button and 'Cancel' and 'OK' buttons at the bottom.

7. Define parameter values, as described below, in [CloudTrail Parameters](#).

8. Click **Test Connection**.

The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and RSA NetWitness Platform displays an error message.

9. If the test is successful, click **OK**.

The new event source is displayed in the Sources panel.

CloudTrail User Parameters

The following table describes the parameters that you need to enter when you configure CloudTrail event source. Items marked with an asterisk (*) are required; all other parameters are optional.

Basic parameters

Parameter	Description
Name *	Name of the event source.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Account ID*	Account Identification code of the S3 Bucket.

Parameter	Description
S3 Bucket Name*	<p>Name of the AWS (CloudTrail) S3 bucket.</p> <p>Amazon S3 bucket names are globally unique, regardless of the AWS (CloudTrail) region in which you create the bucket. You specify the name at the time you create the bucket.</p> <p>Bucket names should comply with DNS naming conventions. The rules for DNS-compliant bucket names are:</p> <ul style="list-style-type: none"> • Bucket names must be at least three and no more than 63 characters long. • Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period “.”. Bucket names can contain lowercase letters, numbers, and hyphens. Each label must start and end with a lowercase letter or a number. • Bucket names must not be formatted as an IP address (for example, 192.168.5.4). <p>The following examples are valid bucket names:</p> <ul style="list-style-type: none"> • myawsbucket • my.aws.bucket • myawsbucket.1 <p>The following examples are invalid bucket names:</p> <ul style="list-style-type: none"> • .myawsbucket - Do not start a Bucket Name with a period “.”. • myawsbucket. - Do not end a Bucket Name with a period “.”. • my..examplebucket - Only use one period between labels.
Access Key*	<p>Key used to access the S3 bucket. Access Keys are used to make secure REST or Query protocol requests to any AWS service API. Please refer to Manage User Credentials on the Amazon Web Services support site for more information on Access Keys</p>
Secret Key *	<p>Secret key used to access the S3 bucket</p>

Parameter	Description
Region*	Region of the S3 bucket: us-east-1 is the default value.
Region Endpoint*	Specifies the AWS cloudtrail hostname. For example, for an AWS public cloud for us-east region, the Region Endpoint would be s3.amazonaws.com . More information can be found at http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region . This parameter is required: it is needed to collect CloudTrail logs from AWS Government or Private clouds.
Start Date*	Starts AWS (CloudTrail) collection from the specified number of days in the past, measured from the current timestamp. The default value is 0, which starts from today. The range is 0–89 days.
Log File Prefix	Prefix of the files to be processed. Note: If you set a prefix when you set up your CloudTrail service, make sure to enter the same prefix in this parameter.
Source Address*	Arbitrary IP address to be sent to the cloudtrail plugin instance. This IP is used only to label all the logs collected via this instance using <code>device.ip</code> meta.

Advanced Parameters

Parameter	Description
Debug	<p>Warning: Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector.</p> <p>Enables/disables debug logging for the event source.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • Off = (default) disabled • On = enabled

Parameter	Description
	<ul style="list-style-type: none"> • Verbose = enabled in verbose mode - adds thread information and source context information to the messages. <p>This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact.</p> <p>If you change this value, the change takes effect immediately (no restart required).</p>
Organization ID	<p>Input the Organization ID if it is available. If multiple organization's accounts are collecting logs into the same CloudTrail bucket, then this value is required.</p>
Command Args	<p>Arguments added to the script.</p>
Polling Interval	<p>Interval (amount of time in seconds) between each poll. The default value is 60.</p> <p>For example, if you specify 60, the collector schedules a polling of the event source every 60 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 60 seconds for the polling to start because the threads are busy.</p>
SSL Enabled	<p>Select the check box to communicate using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates.</p> <p>The check box is selected by default.</p>
Test Connection	<p>Validates the configuration parameters specified in this dialog are correct. For example, this test validates that:</p> <ul style="list-style-type: none"> • RSA NetWitness Platform can connect with the S3 Bucket in AWS using the credentials specified in this dialog. • RSA NetWitness Platform can download a log file from the bucket (test connection would fail if there were no log files for the entire bucket, but this would be extremely unlikely).

Troubleshooting the AWS Cloudtrail Event Source

You may already have various AWS policies configured for your organization. This can lead to permission problems arising from a policy document that does not provide the proper permissions to the S3 bucket and the corresponding subfolders.

A symptom of this problem is that users receive "403 authentication failed" or similar errors while attempting to connect to CloudTrail. In this case, users should first make sure that their credentials are correct. If that does not fix the problem, check the policies for both the IAM user involved and for the S3 bucket, since you can also give permissions to a user or group from the S3 bucket policy document.

© 2021 RSA Security LLC or its affiliates. All Rights Reserved.

November 2020

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.