

Cloudflare Integration

Introduction

Cloudflare integration uses Cloudflare's API to retrieve audit logs and traffic logs from Cloudflare, for a particular zone, and ingest them into Elasticsearch. This allows you to search, observe and visualize the Cloudflare log events through Elasticsearch.

Users of Cloudflare use Cloudflare services to increase the security and performance of their web sites and services.

To enable the Cloudflare Logpush, please refer to Section 5. Currently, the procedures described is for the setup of Amazon S3.

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Requirements

Configure Cloudflare audit logs data stream

Enter values "Auth Email", "Auth Key" and "Account ID".

1. Auth Email is the email address associated with your account.
2. Auth Key is the API key generated on the "My Account" page.
3. Account ID can be found on the Cloudflare dashboard. Follow the navigation documentation from [here](#).

Configure Cloudflare logs

These logs contain data related to the connecting client, the request path through the Cloudflare network, and the response from the origin web server. For more information see [here](#).

The integration can retrieve Cloudflare logs using -

1. Auth Email and Auth Key
2. API Token More information is available [here](#).

CONFIGURE USING AUTH EMAIL AND AUTH KEY

Enter values "Auth Email", "Auth Key" and "Zone ID".

1. Auth Email is the email address associated with your account.
2. Auth Key is the API key generated on the "My Account" page.
3. Zone ID can be found [here](#).

CONFIGURE USING API TOKEN

Enter values "API Token" and "Zone ID".

For the Cloudflare integration to be able to successfully get logs the following permissions must be granted to the API token -

- Account.Access: Audit Logs: Read
1. API Tokens allow for more granular permission settings.
 2. Zone ID can be found [here](#).

Logs

Audit

Audit logs summarize the history of changes made within your Cloudflare account. Audit logs include account-level actions like login and logout, as well as setting changes to DNS, Crypto, Firewall, Speed, Caching, Page Rules, Network, and Traffic features, etc.

Logpull

These logs contain data related to the connecting client, the request path through the Cloudflare network, and the response from the origin web server.

Cloudflare Integration Procedures

Please provide the following information to CyTech:

See the Screenshot Below

Cloudflare

My Profile

Preferences

Authentication

API Tokens

Sessions

API Tokens

Managing access and permissions for your accounts, sites, and products

Token name	Permissions	Resources	Status
No API tokens			

Create Token

API Keys

Keys used to access Cloudflare APIs

Global API Key	Please provide the : Global API key :	Change	View
Origin CA Key	Origin CA Key :	Change	View

Contact

What we do

Resources

Support

About us

Cloudflare

Select Account

Communication

Authentication

API Tokens

Sessions

Back to view all tokens

Create a new API token from this template

1Token name: Edit zone DNS

Permissions

2Select edit or read permissions to apply to your accounts or websites for this token

ZoneDNSEdit

Add more

Zone Resources

3Select zones to include or exclude.

IncludeSpecific zoneSelect...

Add more

IP Address Filtering

Select IP addresses or ranges of IP addresses to filter. By default, this token will apply to all addresses.

OperatorValue

Select...e.g. 192.168.1.88


Add more

TTL

Define how long this token will stay active.

Start DateEnd Date

CancelContinue to summary

Select Account ▾

CommunicationAuthenticationAPI TokensSessions

[← Edit token](#)

Edit zone DNS API token summary

This API token will affect the below accounts and zones, along with their respective permissions

└─ Burrito Bot

└─ theburritobot.com - DNS:Edit

CancelCreate Token

API Tokens

Edit zone DNS API token was successfully created


Copy this token to access the Cloudflare API. For security this will not be shown again. [learn more](#)

XXXXXXXXXXXXXXXXXXXXCopy

Test this token

To confirm your token is working correctly, copy and paste the below CURL command in a terminal shell to test.

```
curl -X GET "https://api.cloudflare.com/client/v4/user/tokens/verify" \  
-H "Authorization: Bearer y8sZdu8QR-nz-1a6_LSSxjgnhcJLX-4pTT26Cnwn" \  
-H "Content-Type:application/json"
```

Email Auth

dev@lina.co... ▾

Websites

Domain Registration ▾

Analytics & Logs ▾


Security Center ▾

Home

Search websites in Tech.dev@selina.com's Account...

lina.com

win

lina.com ▾

Overview

Analytics & Logs ▾

DNS ▾

Email ▾

Spectrum ▾

SSL/TLS ▾

Security ▾

Access ▾

Speed ▾


Caching ▾

Workers Routes ▾

Rules ▾

Data Cached

52 GB



[View more analytics](#)

[Download data](#)

[API](#)

[Page Rules](#)

[Billing](#)

Enterprise plan

[Support Resources](#)

Non-critical Production Issues:

[Contact Support](#)

[Documentation](#)

API

Zone ID

Click to copy

Account ID

Click to copy

Audit Logs

1. Auth Email -
2. Auth Key
3. Account ID

Cloudflare Logs

1. Auth Token
2. Zone ID

Enable Logpush to Amazon S3

To enable the Cloudflare Logpush service:

1. Log in to the Cloudflare dashboard.
2. Select the Enterprise account or domain you want to use with Logpush.
3. Go to Analytics & Logs > Logs.
4. Select Add Logpush job. A modal window opens where you will need to complete several steps.
5. Select the dataset you want to push to a storage service.
6. Select the data fields to include in your logs. Add or remove fields later by modifying your settings in Logs > Logpush.
7. Select Amazon S3.
8. Enter or select the following destination information:
 - Bucket path
 - Daily subfolders
 - Bucket region
 - Encryption constraint in bucket policy
 - For Grant Cloudflare access to upload files to your bucket, make sure your bucket has a policy (if you did not add it already):
 - Copy the JSON policy, then go to your bucket in the Amazon S3 console and paste the policy in Permissions > Bucket Policy and click Save.

9. Click Validate access.
10. Enter the Ownership token (included in a file or log Cloudflare sends to your provider) and click Prove ownership. To find the ownership token, click the Open button in the Overview tab of the ownership challenge file.
11. Click Save and Start Pushing to finish enabling Logpush.

Once connected, Cloudflare lists Amazon S3 as a connected service under Logs > Logpush. Edit or remove connected services from here.

Revision #2

Created 23 April 2024 11:29:02

Updated 19 June 2024 06:54:01