

Edgecast

Real-Time Log Delivery

edgecast

Disclaimer

Care was taken in the creation of this guide. However, Edgecast cannot accept any responsibility for errors or omissions. There are no warranties, expressed or implied, including the warranty of merchantability or fitness for a particular purpose, accompanying this product.

Trademark Information

EDGECAST is a registered trademark of Edgecast Inc.

About This Guide

Real-Time Log Delivery

Version 3.40

5/16/2022

© 2022 Edgecast Inc. All rights reserved.

Table of Contents

Real-Time Log Delivery (RTLD)	1
Log Data	1
Quick Start.....	3
Log Delivery Profiles.....	3
Frequently Asked Questions	4
Setting up Web Server Log Delivery	6
Setting up AWS S3 Log Delivery	15
Setting up Azure Blob Storage Log Delivery.....	24
Setting up Google Cloud Storage Log Delivery	33
Setting up New Relic Log Delivery	41
Setting up Splunk Enterprise Log Delivery	47
Setting up Sumo Logic Log Delivery	57
Setting up Datadog Log Delivery.....	66
Verifying Log Data	73
Log Performance Statistics.....	73
Checking for Sequence Number Gaps	74
Log Fields (RTLD CDN)	76
Top-Level Name/Value Pairs.....	77
Logs Array.....	78
Sample Log Data	91
Log Fields (RTLD Rate Limiting)	95
Top-Level Name/Value Pairs.....	95
Logs Array.....	96
Sample Log Data	99
Log Fields (RTLD WAF)	102
Top-Level Name/Value Pairs.....	102

Logs Array.....	103
Sample Log Data	107
Appendix	111
Log File Naming Convention	111

Real-Time Log Delivery (RTLD)

Log Data

Real-Time Log Delivery (RTLD) delivers log data in near real-time to a variety of destinations. It consists of two modules, which are:

- **Real-Time Log Delivery CDN (RTLD CDN):** Delivers log data that describes requests submitted to our CDN service.

Note: This feature must be purchased separately. For more information, please contact your CDN account manager.

- **Real-Time Log Delivery Rate Limiting (RTLD Rate Limiting):** Delivers log data that describes requests for which Web Application Firewall (WAF) enforced a rate limit as defined through a rate rule.

Note: RTLD Rate Limiting requires WAF Premier, WAF Standard, or WAF Essentials. If you currently have WAF Insights and would like to use this capability, please contact your CDN account manager to upgrade to the full version.

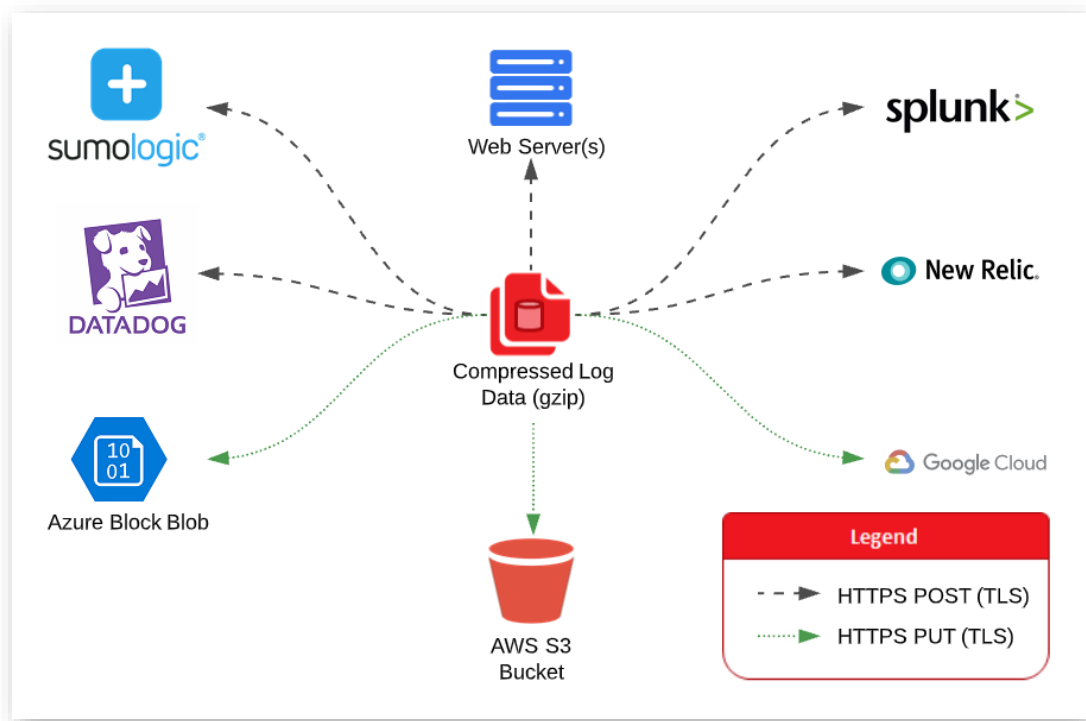
- **Real-Time Log Delivery WAF (RTLD WAF):** Delivers log data that describes requests identified as threats by Web Application Firewall (WAF).

Note: RTLD WAF requires WAF Premier, WAF Standard, or WAF Essentials. If you currently have WAF Insights and would like to use this capability, please contact your CDN account manager to upgrade to the full version.

Note: RTLD WAF delivers log data for threats identified by WAF. It excludes log data for rate limited requests as determined by rate rules. Use RTLD Rate Limiting to deliver log data for rate limited requests.

RTLD delivers compressed log data to one or more of the following destination(s):

- Your web server.
- An AWS S3 bucket.
- An Azure Block Blob.
- A Google Cloud Storage bucket.
- New Relic (RTLD CDN and RTLD Rate Limiting).
- Splunk Enterprise.
- Sumo Logic.
- Sumo Logic.
- Datadog.



Compressed Log Data Delivery

Log data consists a set of log entries. Each entry describes either:

- **RTLD CDN:** A HTTP/HTTPS request that was directed to our CDN service.
- **RTLD Rate Limiting:** A HTTP/HTTPS request that exceeded a rate limit enforced by a Security Application Manager configuration.
- **RTLD WAF:** A HTTP/HTTPS request that was identified as a threat by WAF and information on why it was deemed a threat.

Important: If our service is unable to deliver log data, then we will store it for up to 3 days and deliver it when communication resumes. If we cannot deliver log data within 3 days, then it will be permanently deleted.

Quick Start

Setting up log delivery consists of the following steps:

1. Decide on and prepare the service or web server(s) to which log data will be delivered.
2. If required, gather authentication information for the above destination.
3. Create a log delivery profile for the above destination.

Log Delivery Profiles

A log delivery profile identifies:


- Where log data will be delivered.
- The amount of data that will be delivered.
- Whether log data will be filtered prior to delivery.
- The set of data that will be delivered.

Multiple Profiles

You may create multiple profiles. This allows you to:

- Send log data to one or more destinations. This is useful for disaster recovery.
- Segregate log data by type within a single destination.
- Gather more detailed data as needed.

Key information:

- Perform profile administration from the Real-Time Log Delivery CDN or WAF landing page.
- Log fields vary by RTLD module.
- Log data will only be delivered when a profile's status is enabled.
- The procedure for creating and modifying profiles varies by the destination to which log files will be delivered.
- Delete a profile by clicking the corresponding  icon. When prompted, confirm the deletion.

Frequently Asked Questions

[Why can't I find Real-Time Log Delivery CDN?](#)

Load the **Real-Time Log Delivery CDN** page from the main menu by navigating to **More**, finding **Real-Time Log Delivery** under **Analytics**, and then selecting **CDN**.

If this menu item is not present, then check the following items:

- Verify that Real-Time Log Delivery CDN has been activated on your account. For more information, please contact your CDN account manager.
- Contact your CDN administrator to verify that you have sufficient permissions.

[Why can't I find Real-Time Log Delivery Rate Limiting?](#)

Load the **Real-Time Log Delivery Rate Limiting** page from the main menu by navigating to **More**, finding **Real-Time Log Delivery** under **Analytics**, and then selecting **RL**.

If this menu item is not present, then check the following items:

- Verify that Real-Time Log Delivery Rate Limiting has been activated on your account. This feature requires Web Application Firewall (WAF). For more information, please contact your CDN account manager.
- Contact your CDN administrator to verify that you have sufficient permissions.

[Why can't I find Real-Time Log Delivery WAF?](#)

Load the **Real-Time Log Delivery WAF** page from the main menu by navigating to **More**, finding **Real-Time Log Delivery** under **Analytics**, and then selecting **WAF**.

If this menu item is not present, then check the following items:

- Verify that Real-Time Log Delivery WAF has been activated on your account. This feature requires Web Application Firewall (WAF). For more information, please contact your CDN account manager.
- Contact your CDN administrator to verify that you have sufficient permissions.

[May I use Real-Time Log Delivery CDN to verify billing data?](#)

Yes. However, you cannot filter or downsample log data if you plan to use it for billing verification.

[May I deliver log data to an existing AWS S3 bucket?](#)

Yes. However, a specific bucket policy must be applied to it.

[May I deliver log data to an existing Azure Blob container?](#)

Yes. However, you must authorize log data uploads via either a SAS token or an access key.

[May I deliver log data to an existing Google Cloud Storage bucket?](#)

Yes. However, you must authorize our Google Cloud Storage user to upload log data.

May I securely deliver log data to my web server?

Yes. Authorize log data delivery via the Authorization request header by passing a token or user account credentials. Alternatively, log data may be delivered to your web server(s) without authorization.

May I limit the amount of log data delivered?

Yes. Log data delivery may be limited by:

- Filtering the set of log data that will be delivered.
- Downsampling logs to 0.1%, 1%, 25%, 50%, or 75% of the set of log entries that will be delivered.
- Selecting the type of data (i.e., fields) that will be delivered.

How should I configure my firewall to allow log delivery?

Firewall configuration is only required when delivering log data to either your web server(s) or an instance of Splunk Enterprise hosted within your network. Set up your firewall to allow POST requests from the following CIDR network addresses:

```
198.7.21.0/24
```

If you plan to deliver log data via a custom port, then you should also configure your firewall to open that port for the above IP blocks.

What happens if log data cannot be delivered?

If our service is unable to deliver log data, then we will store it for up to 3 days and deliver it when communication resumes. If we cannot deliver log data within 3 days, then it will be permanently deleted.

Can the same log data be sent multiple times because of multiple profiles?

Yes. Each profile is:

- Independent.
- Defines a set of log data.
- Determines where data will be delivered.

This means that more than one profile may be configured to deliver the same set of log data.

Can I mix and match log data from RTLD CDN, RTLD Rate Limiting, and RTLD WAF?

No. RTLD CDN, RTLD Rate Limiting, and RTLD WAF use separate logging mechanisms.

Does RTLD deliver compressed log data?

Yes. RTLD compresses all log data using gzip.

Key information:

- **Web Server Log Delivery:** You should decompress log data before transforming it. Your web framework may automatically handle compression on your behalf.
- **AWS S3, Azure Blob Storage, and Google Cloud Storage Log Delivery:** Each object contains compressed log data with a gz file extension.
- **All Other Destinations:** Your third-party data analytics platform manages compression on your behalf. No additional action is required.

Setting up Web Server Log Delivery

RTLD may automatically deliver compressed log data to a web server by submitting HTTPS POST requests to it. The body for each of these requests will be a JSON or CSV document that uniquely identifies a set of log data and describes one or more log entries. For more information, please refer to the **Log Fields** section.

Note: RTLD applies gzip compression to log data. Each HTTPS POST request includes a Content-Encoding header set to gzip.

To create a log delivery profile

1. Configure your web server(s) to:
 - Support the HTTPS protocol.

Important: Log delivery requires a certificate whose trust anchor is a publicly trusted certificate authority (CA). Additionally, the certificate must include a chain of trust for all intermediate certificate(s) and a leaf certificate.

 - Allow HTTPS POST requests.
 - Return a 2xx (e.g., 200 OK) response whenever data is successfully received.

Important: If your web server responds with any other status code, then our service will retransmit the same log data at regular intervals. This may result in the delivery of duplicate log data.

2. Configure your firewall to allow POST requests from the following IP blocks:
198.7.21.0/24

If you plan to deliver log data via a custom port, then you should also configure your firewall to open that port for the above IP blocks.

3. Set up a workflow for handling or processing the log data that will be posted to your web server(s).
Example:
Create a listener for HTTPS POST requests that mines specific data from log entries.
4. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting | WAF** page. From the main menu, navigate to **More** and then find **Real-Time Log Delivery** under **Analytics**. Select either **CDN, RL, or WAF**.
5. Click **Add Profile**.
6. From the **Log Delivery Method** option, select "HTTP Post."
7. Set the **Request URL** option to a URL that may leverage the workflow defined in step 3. This URL must use the HTTPS protocol.

Note: Specify a custom port to deliver log data over that port instead of 443.

Sample URL:

https://logs.mydomain.com/cdn/logs.aspx

8. From the **Authentication** option, select one of the following modes:
 - **Custom Authentication:** Select this mode when your web server(s) expects the Authorization request header to be set to a custom token value. Set the **Token** option to a value that will authorize requests to your web server(s).

Note: Log data will be posted to your web server(s) via HTTPS POST requests with an Authorization request header set to the specified value.

Authorization header syntax:

Authorization: *Token*

- **HTTP Basic:** Select this mode if your web server(s) allow content to be uploaded via standard HTTP basic authentication. Set the desired credentials via the **Username** and **Password** options. Base-64 encoding will be applied to the specified credentials. After which, the encoded value will be passed via the Authorization header.

Authorization header syntax:

Authorization: Basic *Base64-Encoded-Credentials*

- **None:** Select this mode if your web server(s) allow content to be posted without authorization.
9. From the **Log Format** option, select whether to format log data using our standard JSON format, as a JSON array, as JSON lines, or as a CSV (RTLD CDN only).

10. From the **Downsample the Logs** option, determine whether all or downsampled log data will be delivered.
 - **All Log Data:** Verify that the **Downsample the Logs** option is disabled.
 - **Downsampled Log Data:** Downsample logs to 0.1%, 1%, 25%, 50%, or 75% of total log data by enabling the **Downsample the Logs** option and then selecting the desired rate from the **Downsampling Rate** option.

Note: Use this capability to reduce the amount of data that needs to be processed or stored by your web server(s).

RTLD CDN Only: Downsampling log data also reduces usage charges for this service.

11. Log delivery setup varies according to whether you are delivering log data for CDN traffic, rate limited requests, or threats identified by WAF. Refer to the appropriate section below.
12. Set the **Log Delivery Enabled** option to the "on" position.
13. Click **Save**.

To set up RTLD CDN

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery CDN** page.
2. From the **Log Delivery** section, mark each delivery platform for which real-time log data may be delivered.
3. From the **Filter by Status Code** section, perform one of the following steps:
 - **Filter log data by status code:**
Mark each status code class (e.g., 2xx or 3xx) for which log data should be uploaded to your web server(s). Clear all other status code classes.
 - **Upload all log data regardless of status code:**
Clear all status code classes (e.g., 2xx and 3xx).
4. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
5. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
 6. From the **Log file contains the following fields** section, perform the following steps:
 - i. Add the request headers, response headers, and cookies that will be logged for each request from the **Custom Request Headers**, **Custom Response Headers**, and **Custom Cookies** options.

Tip: You may either select or type the name of the desired headers and/or cookies. Click on the list to add additional headers or cookies. Remove a header or cookie by clicking on its x.

Note: Although other settings take effect quickly, it may take up to 90 minutes before data for custom request/response headers and cookies is logged.

 - ii. Click "Expand All."
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
 7. Click **Save**.

To set up RTLD Rate Limiting

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery Rate Limiting** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.

3. From the **Filter by Country** section, perform one of the following steps:

- **Filter log data by one or more countries:**

- Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
- Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**

Verify that a country has not been defined within this section.

4. From the **Filter by User Agent** section, perform one of the following steps:

- **Filter log data by user agent:**

Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.

- **Upload all log data regardless of user agent:**

Set it to a blank value.

5. From the **Filter by Client IP** section, perform one of the following steps:

- **Filter log data by one or more IP addresses:**

- Determine whether log data will be filtered to include or exclude requests to the selected IP addresses by selecting either "Matches" or "Does Not Match," respectively.
- Type one or more IP addresses within the option directly to the right of the above option.

- **Upload all log data regardless of IP address:**

Set it to a blank value.

6. From the **Filter by Action Type** section, perform one of the following steps:
 - **Filter log data by one or more enforcement actions:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected enforcement actions by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type the name for one or more enforcement actions.
 - **Upload all log data regardless of enforcement action:**
Set it to a blank value.
7. From the **Filter by Request Method** section, perform one of the following steps:
 - **Filter log data by one or more request methods:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected request methods by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more request method(s).
 - **Upload all log data regardless of request method:**
Set it to a blank value.
8. From the **Filter By Scope Name** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**
Verify that a security application manager has not been defined within this section.
9. From the **Filter By Action Limit ID** option, perform one of the following steps:
 - **Filter log data by one or more rate rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected rate rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more rate rule(s).
 - **Upload all log data regardless of rate rule:**
Verify that a rate rule has not been defined within this section.

10. From the **Filter by URL Regex** section, perform one of the following steps:
 - **Filter log data by URL:**
Type a RE2-compatible regular expression pattern that identifies the set of URLs by which log data will be filtered.
 - **Upload all log data regardless of URL:**
Set it to a blank value.
11. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
12. Click **Save**.

To set up RTLD WAF

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery WAF** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

 - **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.

3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

 - **Upload all log data regardless of country of origin:**
Verify that a country has not been defined within this section.
4. From the **Filter By Managed Rule** option, perform one of the following steps:
 - **Filter log data by one or more managed rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected managed rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more managed rule(s).
 - **Upload all log data regardless of managed rule:**
Verify that a managed rule has not been defined within this section.
5. From the **Filter By Access Rule** option, perform one of the following steps:
 - **Filter log data by one or more access rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected access rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more access rule(s).
 - **Upload all log data regardless of access rule:**
Verify that an access rule has not been defined within this section.

6. From the **Filter By Custom Rule** option, perform one of the following steps:
 - **Filter log data by one or more custom rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected custom rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more custom rule(s).
 - **Upload all log data regardless of custom rule:**

Verify that a custom rule has not been defined within this section.
7. From the **Filter By Security Application Manager** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**

Verify that a security application manager(s) has not been defined within this section.
8. From the **Log file contains the following fields** section, perform the following steps:
 - Mark each field that will be reported for each request submitted to the CDN.
 - Clear each field for which log data should not be reported.
9. Click **Save**.

Setting up AWS S3 Log Delivery

RTLD may automatically deliver compressed log data to an AWS S3 bucket by submitting HTTPS PUT requests to it. Each request adds an object to the bucket. This object contains a compressed JSON or CSV document that uniquely identifies a set of log data and describes one or more log entries.

Key information:

- RTLD applies gzip compression to log data. AWS S3 stores compressed log data as an object with a gz file extension.
- AWS S3 may automatically decompress files downloaded via the S3 Management Console into JSON or CSV files. No additional decompression is required to process this data.
- Please refer to the **Appendix: Log File Naming Convention** section to learn the naming convention for log files.
- RTLD requires a bucket policy that authorizes our service to upload content to your bucket.
- If you have enabled server-side encryption on the desired AWS S3 bucket, then you must also enable default bucket encryption. Otherwise, RTLD will be unable to post log data to that bucket.

Note: RTLD does not include Amazon-specific encryption headers when posting log data to your bucket.

To create a log delivery profile

1. Create or identify an AWS S3 bucket to which log data will be posted.
[View AWS documentation on how to create a bucket.](#)
2. Apply the following bucket policy to the AWS S3 bucket identified in step 1. This bucket policy authorizes our service to upload content to your bucket.
[View AWS documentation on how to add a bucket policy.](#)

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "CDNRealTimeLogDelivery",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::638349102478:user/real-time-
log-delivery"
    },
    "Action": [
      "s3:PutObject",
      "s3:GetBucketLocation",
      "s3:PutObjectTagging",
      "s3:PutObjectACL"
    ],
    "Resource": [
      "arn:aws:s3:: Bucket-Name",
      "arn:aws:s3:: Bucket-Name/*"
    ]
  }
]
}

```

Note: Replace the term "Bucket-Name" with the name of the AWS S3 bucket to which this policy is being applied.

3. If you have enabled server-side encryption on the AWS S3 bucket identified in step 1, then you must also enable default bucket encryption.
4. Optional. Set up AWS to process the log data that will be posted to it.

Example:
Leverage AWS Lambda to mine specific data from log entries.
5. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting | WAF** page. From the main menu, navigate to **More** and then find **Real-Time Log Delivery** under **Analytics**. Select either **CDN**, **RL**, or **WAF**.
6. Click **Add Profile**.
7. From the **Log Delivery Method** option, select "AWS S3."
8. Set the **Bucket** option to the name of the AWS S3 bucket to which log data will be posted.

9. Optional. Set the **Prefix** option to the desired prefix that defines a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

- A prefix should not start with a forward slash.
- A forward slash within the specified prefix is interpreted as a delimiter for a virtual directory.
- A trailing forward slash means that the specified value only defines a virtual directory path within your AWS S3 bucket where logs will be stored. If the specified value ends in a character other than a forward slash, then the characters specified after the forward slash will be prepended to the file name for each log file uploaded to AWS S3.

Sample prefix:

logs/CDN/siteA_

The above prefix will store log files in the following virtual directory:

/logs/CDN

The file name for each log file uploaded to AWS S3 will start with "siteA_."

Sample log file name:

siteA_adn_0001_123_20190111_50550000F98AB95B_1.json

10. From the **AWS Region** option, select the region assigned to the AWS S3 bucket.
11. From the **Log Format** option, select whether to format log data using our standard JSON format, as a JSON array, as JSON lines, or as a CSV (RTLD CDN only).
12. From the **Downsample the Logs** option, determine whether all or downsampled log data will be delivered.

- **All Log Data:** Verify that the **Downsample the Logs** option is disabled.
- **Downsampled Log Data:** Downsample logs to 0.1%, 1%, 25%, 50%, or 75% of total log data by enabling the **Downsample the Logs** option and then selecting the desired rate from the **Downsampling Rate** option.

Note: Use this capability to reduce the amount of data that needs to be processed or stored by AWS S3.

RTLD CDN Only: Downsampling log data also reduces usage charges for this service.

12. Log delivery setup varies according to whether you are delivering log data for CDN traffic, rate limited requests, or threats identified by WAF. Refer to the appropriate section below.
13. Set the **Log Delivery Enabled** option to the "on" position.
14. Click **Save**.

To set up RTLD CDN

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery CDN** page.
2. From the **Log Delivery** section, mark each delivery platform for which real-time log data may be delivered.
3. From the **Filter by Status Code** section, perform one of the following steps:
 - **Filter log data by status code:**
Mark each status code class (e.g., 2xx or 3xx) for which log data should be delivered. Clear all other status code classes.
 - **Upload all log data regardless of status code:**
Clear all status code classes (e.g., 2xx and 3xx).
4. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

 - **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
5. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
6. From the **Log file contains the following fields** section, perform the following steps:
 - i. Add the request headers, response headers, and cookies that will be logged for each request from the **Custom Request Headers**, **Custom Response Headers**, and **Custom Cookies** options.

Tip: You may either select or type the name of the desired headers and/or cookies. Click on the list to add additional headers or cookies. Remove a header or cookie by clicking on its x.

Note: Although other settings take effect quickly, it may take up to 90 minutes before data for custom request/response headers and cookies is logged.

- ii. Click "Expand All."
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
7. Click **Save**.

To set up RTLD Rate Limiting

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery Rate Limiting** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**
Verify that a country has not been defined within this section.
4. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
 5. From the **Filter by Client IP** section, perform one of the following steps:
 - **Filter log data by one or more IP addresses:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected IP addresses by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more IP addresses within the option directly to the right of the above option.
 - **Upload all log data regardless of IP address:**
Set it to a blank value.
 6. From the **Filter by Action Type** section, perform one of the following steps:
 - **Filter log data by one or more enforcement actions:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected enforcement actions by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type the name for one or more enforcement actions.
 - **Upload all log data regardless of enforcement action:**
Set it to a blank value.
 7. From the **Filter by Request Method** section, perform one of the following steps:
 - **Filter log data by one or more request methods:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected request methods by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more request method(s).
 - **Upload all log data regardless of request method:**
Set it to a blank value.

8. From the **Filter By Scope Name** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**

Verify that a security application manager has not been defined within this section.
9. From the **Filter By Action Limit ID** option, perform one of the following steps:
 - **Filter log data by one or more rate rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected rate rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more rate rule(s).
 - **Upload all log data regardless of rate rule:**

Verify that a rate rule has not been defined within this section.
10. From the **Filter by URL Regex** section, perform one of the following steps:
 - **Filter log data by URL:**

Type a RE2-compatible regular expression pattern that identifies the set of URLs by which log data will be filtered.
 - **Upload all log data regardless of URL:**

Set it to a blank value.
11. From the **Log file contains the following fields** section, perform the following steps:
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
12. Click **Save**.

To set up RTLD WAF

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery WAF** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**

Verify that a country has not been defined within this section.
4. From the **Filter By Managed Rule** option, perform one of the following steps:
 - **Filter log data by one or more managed rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected managed rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more managed rule(s).

- **Upload all log data regardless of managed rule:**
Verify that a managed rule has not been defined within this section.
5. From the **Filter By Access Rule** option, perform one of the following steps:
- **Filter log data by one or more access rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected access rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more access rule(s).
 - **Upload all log data regardless of access rule:**
Verify that an access rule has not been defined within this section.
6. From the **Filter By Custom Rule** option, perform one of the following steps:
- **Filter log data by one or more custom rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected custom rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more custom rule(s).
 - **Upload all log data regardless of custom rule:**
Verify that a custom rule has not been defined within this section.
7. From the **Filter By Security Application Manager** option, perform one of the following steps:
- **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**
Verify that a security application manager(s) has not been defined within this section.
8. From the **Log file contains the following fields** section, perform the following steps:
- Mark each field that will be reported for each request submitted to the CDN.
 - Clear each field for which log data should not be reported.
9. Click **Save**.

Setting up Azure Blob Storage Log Delivery

RTLTD may automatically deliver compressed log data to an Azure Blob Storage container by submitting HTTPS PUT requests to it. Each request creates a block blob within the container. This block blob contains a compressed JSON or CSV document that uniquely identifies a set of log data and describes one or more log entries.

Note: RTLTD applies gzip compression to log data. Azure Blob Storage stores compressed log data as an object with a gz file extension.

Note: Please refer to the **Appendix: Log File Naming Convention** section to learn the naming convention for log files.

Setting up log delivery to Azure Blob Storage requires:

- An existing Azure Blob Storage account.
[Get started.](#)
- A container to which log data will be uploaded.
- A base URL that points to your container.
Blob Container URL:
`https://Storage Account.blob.core.windows.net/Container`
Sample Blob Container URL:
`https://myaccount.blob.core.windows.net/mycontainer`
- Either a SAS token or an access key through which our service will authorize requests to upload content to your Azure Blob Storage account.

Note: If you plan on providing a SAS token, make sure that the token has permission to write to the blob/container. Additionally, it should start with "sv=" and it should not include a "?."

Sample SAS token:

```
sv=2018-03-  
28&sr=c&si=myblobReadWritekey1_123456789012345678&sig=a1bCDefghijklMnOpqrs  
Tuv2wXYZABc3d34efGHIjkl%5M
```

In addition to the above requirements, you may specify an optional prefix that defines the location where log data will be uploaded within your container. Content will be uploaded to the location defined by this prefix as indicated by the following URL.

`https://Storage Account.blob.core.windows.net/Container/Prefix`

Key information:

- A prefix should not start with a forward slash.
- A forward slash within the specified prefix is interpreted as a delimiter for a virtual directory.
- A trailing forward slash means that the specified value only defines a virtual directory path within your container where logs will be stored. If the specified value ends in a character other than a forward slash, then the characters specified after the last forward slash will be prepended to the file name for each log file uploaded to Azure Blob Storage.

Sample Scenario

This scenario demonstrates how a prefix that does not end with a forward slash will affect the naming convention for log files.

Sample prefix:

logs/CDN/siteA_

The above prefix will store log files in the following virtual directory:

/logs/CDN

The file name for each log file uploaded to Azure Blob Storage will start with "siteA_."

Sample log file name:

siteA_adn_0001_123_20190111_50550000F98AB95B_1.json.gz

To create a log delivery profile

1. Create or identify an Azure storage account and a container to which log data will be posted.
[View Microsoft Azure documentation on how to create a storage account.](#)
2. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting | WAF** page. From the main menu, navigate to **More** and then find **Real-Time Log Delivery** under **Analytics**. Select either **CDN**, **RL**, or **WAF**.
3. Click **Add Profile**.
4. From the **Log Delivery Method** option, select "Azure Blob Storage."
5. Set the **Blob Container URL** option to a URL that points to the container to which log data will be posted.
6. Optional. Set the **Prefix** option to a value that defines a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
7. From the **Access Type** option, select whether log data uploads will be authorized via a SAS token or an access key and then paste it in the field below it.

Reminder: If you plan on providing a SAS token, make sure that the token has permission to write to the blob/container. Additionally, it should start with "sv=" and it should not include a "?."

8. From the **Log Format** option, select whether to format log data using our standard JSON format, as a JSON array, as JSON lines, or as a CSV (RTLD CDN only).
9. From the **Downsample the Logs** option, determine whether all or downsampled log data will be delivered.

- **All Log Data:** Verify that the **Downsample the Logs** option is disabled.
- **Downsampled Log Data:** Downsample logs to 0.1%, 1%, 25%, 50%, or 75% of total log data by enabling the **Downsample the Logs** option and then selecting the desired rate from the **Downsampling Rate** option.

Note: Use this capability to reduce the amount of data that needs to be processed or stored by Azure Blob Storage.

RTLD CDN Only: Downsampling log data also reduces usage charges for this service.

10. Log delivery setup varies according to whether you are delivering log data for CDN traffic, rate limited requests, or threats identified by WAF. Refer to the appropriate section below.
11. Set the **Log Delivery Enabled** option to the "on" position.
12. Click **Save**.

To set up RTLD CDN

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery CDN** page.
2. From the **Log Delivery** section, mark each delivery platform for which real-time log data may be delivered.
3. From the **Filter by Status Code** section, perform one of the following steps:
 - **Filter log data by status code:**
Mark each status code class (e.g., 2xx or 3xx) for which log data should be delivered. Clear all other status code classes.
 - **Upload all log data regardless of status code:**
Clear all status code classes (e.g., 2xx and 3xx).
4. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
5. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
 6. From the **Log file contains the following fields** section, perform the following steps:
 - i. Add the request headers, response headers, and cookies that will be logged for each request from the **Custom Request Headers**, **Custom Response Headers**, and **Custom Cookies** options.

Tip: You may either select or type the name of the desired headers and/or cookies. Click on the list to add additional headers or cookies. Remove a header or cookie by clicking on its x.

Note: Although other settings take effect quickly, it may take up to 90 minutes before data for custom request/response headers and cookies is logged.

 - ii. Click "Expand All."
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
 7. Click **Save**.

To set up RTLD Rate Limiting

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery Rate Limiting** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**

Verify that a country has not been defined within this section.
4. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**

Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**

Set it to a blank value.

5. From the **Filter by Client IP** section, perform one of the following steps:
 - **Filter log data by one or more IP addresses:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected IP addresses by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more IP addresses within the option directly to the right of the above option.
 - **Upload all log data regardless of IP address:**
Set it to a blank value.
6. From the **Filter by Action Type** section, perform one of the following steps:
 - **Filter log data by one or more enforcement actions:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected enforcement actions by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type the name for one or more enforcement actions.
 - **Upload all log data regardless of enforcement action:**
Set it to a blank value.
7. From the **Filter by Request Method** section, perform one of the following steps:
 - **Filter log data by one or more request methods:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected request methods by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more request method(s).
 - **Upload all log data regardless of request method:**
Set it to a blank value.
8. From the **Filter By Scope Name** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).

- **Upload all log data regardless of security application manager:**
Verify that a security application manager has not been defined within this section.
9. From the **Filter By Action Limit ID** option, perform one of the following steps:
 - **Filter log data by one or more rate rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected rate rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more rate rule(s).
 - **Upload all log data regardless of rate rule:**
Verify that a rate rule has not been defined within this section.
 10. From the **Filter by URL Regex** section, perform one of the following steps:
 - **Filter log data by URL:**
Type a RE2-compatible regular expression pattern that identifies the set of URLs by which log data will be filtered.
 - **Upload all log data regardless of URL:**
Set it to a blank value.
 11. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
 12. Click **Save**.

To set up RTLD WAF

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery WAF** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
- **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.
-
- Tip:** Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).
- **Upload all log data regardless of country of origin:**
Verify that a country has not been defined within this section.
4. From the **Filter By Managed Rule** option, perform one of the following steps:
- **Filter log data by one or more managed rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected managed rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more managed rule(s).
 - **Upload all log data regardless of managed rule:**
Verify that a managed rule has not been defined within this section.
5. From the **Filter By Access Rule** option, perform one of the following steps:
- **Filter log data by one or more access rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected access rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more access rule(s).
 - **Upload all log data regardless of access rule:**
Verify that an access rule has not been defined within this section.

6. From the **Filter By Custom Rule** option, perform one of the following steps:
 - **Filter log data by one or more custom rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected custom rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more custom rule(s).
 - **Upload all log data regardless of custom rule:**

Verify that a custom rule has not been defined within this section.
7. From the **Filter By Security Application Manager** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**

Verify that a security application manager(s) has not been defined within this section.
8. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
9. Click **Save**.

Setting up Google Cloud Storage Log Delivery

RTLD may automatically deliver compressed log data to a Google Cloud Storage bucket by submitting HTTPS PUT requests to it. Each request adds an object to a Cloud Storage bucket. This object contains a compressed JSON or CSV document that uniquely identifies a set of log data and describes one or more log entries.

Note: RTLD applies gzip compression to log data. Google Cloud Storage stores compressed log data as an object with a gz file extension.

Note: Please refer to the **Appendix: Log File Naming Convention** section to learn the naming convention for log files.

To create a log delivery profile

1. Create or identify a Google Cloud Storage bucket to which log data will be posted.

Key information:

- The recommended configuration is to set the **Access control** option to "Uniform."
- Set the **Encryption** option to "Google-managed encryption key."

[View Google Cloud Storage documentation on how to create a bucket.](#)

2. Add the following user to the bucket and assign it the Storage Object Creator role:
vdms-partner-gcs-transfer@maw-partner-gcs.iam.gserviceaccount.com

[View Google Cloud Storage documentation on how to set up an IAM policy for a bucket.](#)

3. Optional. Set up Google Cloud to process the log data that will be posted to it.

Example:

Load logs into BigQuery and then leverage BigQuery functionality through the BigQuery Browser Tool.

4. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting | WAF** page. From the main menu, navigate to **More** and then find **Real-Time Log Delivery** under **Analytics**. Select either **CDN**, **RL**, or **WAF**.
5. Click **Add Profile**.
6. From the **Log Delivery Method** option, select "Google Cloud Storage."
7. Set the **Bucket** option to the name of the Google Cloud Storage bucket to which log data will be posted.

8. Optional. Set the **Prefix** option to the desired prefix that defines a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

- A prefix should not start with a forward slash.
- A forward slash within the specified prefix is interpreted as a delimiter for a virtual directory.
- A trailing forward slash means that the specified value only defines a virtual directory path within your Google Cloud Storage bucket where logs will be stored. If the specified value ends in a character other than a forward slash, then the characters specified after the forward slash will be prepended to the file name for each log file uploaded to Google Cloud Storage.

Sample prefix:

logs/CDN/siteA_

The above prefix will store log files in the following virtual directory:

/logs/CDN

The file name for each log file uploaded to Google Cloud Storage will start with "siteA_."

Sample log file name:

siteA_adn_0001_123_20190111_50550000F98AB95B_1.json

9. From the **Log Format** option, select whether to format log data using our standard JSON format, as a JSON array, as JSON lines, or as a CSV (RTLD CDN only).

10. From the **Downsample the Logs** option, determine whether all or downsampled log data will be delivered.

- **All Log Data:** Verify that the **Downsample the Logs** option is disabled.
- **Downsampled Log Data:** Downsample logs to 0.1%, 1%, 25%, 50%, or 75% of total log data by enabling the **Downsample the Logs** option and then selecting the desired rate from the **Downsampling Rate** option.

Note: Use this capability to reduce the amount of data that needs to be processed or stored by Google Cloud Storage.

RTLD CDN Only: Downsampling log data also reduces usage charges for this service.

11. Log delivery setup varies according to whether you are delivering log data for CDN traffic, rate limited requests, or threats identified by WAF. Refer to the appropriate section below.

12. Set the **Log Delivery Enabled** option to the "on" position.

13. Click **Save**.

To set up RTLD CDN

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery CDN** page.
2. From the **Log Delivery** section, mark each delivery platform for which real-time log data may be delivered.
3. From the **Filter by Status Code** section, perform one of the following steps:
 - **Filter log data by status code:**
Mark each status code class (e.g., 2xx or 3xx) for which log data should be delivered. Clear all other status code classes.
 - **Upload all log data regardless of status code:**
Clear all status code classes (e.g., 2xx and 3xx).
4. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

 - **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
5. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.

6. From the **Log file contains the following fields** section, perform the following steps:
 - i. Add the request headers, response headers, and cookies that will be logged for each request from the **Custom Request Headers**, **Custom Response Headers**, and **Custom Cookies** options.

Tip: You may either select or type the name of the desired headers and/or cookies. Click on the list to add additional headers or cookies. Remove a header or cookie by clicking on its x.

Note: Although other settings take effect quickly, it may take up to 90 minutes before data for custom request/response headers and cookies is logged.

- ii. Click "Expand All."
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
7. Click **Save**.

To set up RTLD Rate Limiting

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery Rate Limiting** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.

3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**
Verify that a country has not been defined within this section.
4. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
 5. From the **Filter by Client IP** section, perform one of the following steps:
 - **Filter log data by one or more IP addresses:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected IP addresses by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more IP addresses within the option directly to the right of the above option.
 - **Upload all log data regardless of IP address:**
Set it to a blank value.
 6. From the **Filter by Action Type** section, perform one of the following steps:
 - **Filter log data by one or more enforcement actions:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected enforcement actions by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type the name for one or more enforcement actions.

- **Upload all log data regardless of enforcement action:**
Set it to a blank value.
7. From the **Filter by Request Method** section, perform one of the following steps:
- **Filter log data by one or more request methods:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected request methods by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more request method(s).
 - **Upload all log data regardless of request method:**
Set it to a blank value.
8. From the **Filter By Scope Name** option, perform one of the following steps:
- **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**
Verify that a security application manager has not been defined within this section.
9. From the **Filter By Action Limit ID** option, perform one of the following steps:
- **Filter log data by one or more rate rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected rate rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more rate rule(s).
 - **Upload all log data regardless of rate rule:**
Verify that a rate rule has not been defined within this section.
10. From the **Filter by URL Regex** section, perform one of the following steps:
- **Filter log data by URL:**
Type a RE2-compatible regular expression pattern that identifies the set of URLs by which log data will be filtered.
 - **Upload all log data regardless of URL:**
Set it to a blank value.

11. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
12. Click **Save**.

To set up RTLD WAF

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery WAF** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**

Verify that a country has not been defined within this section.

4. From the **Filter By Managed Rule** option, perform one of the following steps:
 - **Filter log data by one or more managed rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected managed rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more managed rule(s).
 - **Upload all log data regardless of managed rule:**

Verify that a managed rule has not been defined within this section.
5. From the **Filter By Access Rule** option, perform one of the following steps:
 - **Filter log data by one or more access rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected access rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more access rule(s).
 - **Upload all log data regardless of access rule:**

Verify that an access rule has not been defined within this section.
6. From the **Filter By Custom Rule** option, perform one of the following steps:
 - **Filter log data by one or more custom rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected custom rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more custom rule(s).
 - **Upload all log data regardless of custom rule:**

Verify that a custom rule has not been defined within this section.
7. From the **Filter By Security Application Manager** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).

- **Upload all log data regardless of security application manager:**
Verify that a security application manager(s) has not been defined within this section.
8. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
 9. Click **Save**.

Setting up New Relic Log Delivery

RTLTD may automatically deliver compressed log data to your New Relic account by submitting HTTPS POST requests to it. Each request adds a log file to your account. This log file contains a compressed JSON or CSV document that uniquely identifies a set of log data and describes one or more log entries.

Important: The format for log data delivered to New Relic is JSON Array. This log format does not provide information that uniquely identifies a set of log data. As a result, there is no way to check for gaps in sequence numbers when attempting to identify missing log data.

Note: RTLTD CDN and RTLTD Rate Limiting support delivery to the New Relic destination.

To create a log delivery profile

1. Optional. Register an Inserts insight API key that is dedicated for RTLTD log delivery.
[View New Relic documentation on how to register an Inserts insight API key.](#)
2. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting** page. From the main menu, navigate to **More** and then find **Real-Time Log Delivery** under **Analytics**. Select **CDN** or **RL**.
3. Click **Add Profile**.
4. From the **Log Delivery Method** option, select "New Relic."
5. Set the **Account ID** option to your New Relic account ID.
6. Set the **Event Type** option to a label that identifies log data delivered to New Relic as a result of this profile. Specify a label that solely consists of alphanumeric characters, underscores, and colons.

Tip: Query delivered log data by constructing a NRQL that selects data using this label (e.g., `SELECT * FROM {Event Type}`).

7. Set the **Insert Key** option to an Inserts insight API key.

8. From the **Downsample the Logs** option, determine whether all or downsampled log data will be delivered.
 - **All Log Data:** Verify that the **Downsample the Logs** option is disabled.
 - **Downsampled Log Data:** Downsample logs to 0.1%, 1%, 25%, 50%, or 75% of total log data by enabling the **Downsample the Logs** option and then selecting the desired rate from the **Downsampling Rate** option.

Note: Use this capability to reduce the amount of data that needs to be processed or stored by New Relic.

Note: Downsampling log data also reduces RTLD CDN usage charges.

9. Set up log delivery for CDN traffic. Refer to the section below.
10. Set the **Log Delivery Enabled** option to the "on" position.
11. Click **Save**.

To set up RTLD CDN log delivery

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery CDN** page.
2. From the **Log Delivery** section, mark each delivery platform for which real-time log data may be delivered.
3. From the **Filter by Status Code** section, perform one of the following steps:
 - **Filter log data by status code:**
Mark each status code class (e.g., 2xx or 3xx) for which log data should be delivered. Clear all other status code classes.
 - **Upload all log data regardless of status code:**
Clear all status code classes (e.g., 2xx and 3xx).
4. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
5. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
 6. From the **Log file contains the following fields** section, perform the following steps:
 - i. Add the request headers, response headers, and cookies that will be logged for each request from the **Custom Request Headers, Custom Response Headers, and Custom Cookies** options.

Tip: You may either select or type the name of the desired headers and/or cookies. Click on the list to add additional headers or cookies. Remove a header or cookie by clicking on its x.

Note: Although other settings take effect quickly, it may take up to 90 minutes before data for custom request/response headers and cookies is logged.

 - ii. Click "Expand All."
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
 7. Click **Save**.

To set up RTLD Rate Limiting

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery Rate Limiting** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.

3. From the **Filter by Country** section, perform one of the following steps:

- **Filter log data by one or more countries:**

- Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
- Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**

Verify that a country has not been defined within this section.

4. From the **Filter by User Agent** section, perform one of the following steps:

- **Filter log data by user agent:**

Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.

- **Upload all log data regardless of user agent:**

Set it to a blank value.

5. From the **Filter by Client IP** section, perform one of the following steps:

- **Filter log data by one or more IP addresses:**

- Determine whether log data will be filtered to include or exclude requests to the selected IP addresses by selecting either "Matches" or "Does Not Match," respectively.
- Type one or more IP addresses within the option directly to the right of the above option.

- **Upload all log data regardless of IP address:**

Set it to a blank value.

6. From the **Filter by Action Type** section, perform one of the following steps:
 - **Filter log data by one or more enforcement actions:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected enforcement actions by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type the name for one or more enforcement actions.
 - **Upload all log data regardless of enforcement action:**
Set it to a blank value.
7. From the **Filter by Request Method** section, perform one of the following steps:
 - **Filter log data by one or more request methods:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected request methods by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more request method(s).
 - **Upload all log data regardless of request method:**
Set it to a blank value.
8. From the **Filter By Scope Name** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**
Verify that a security application manager has not been defined within this section.
9. From the **Filter By Action Limit ID** option, perform one of the following steps:
 - **Filter log data by one or more rate rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected rate rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more rate rule(s).
 - **Upload all log data regardless of rate rule:**
Verify that a rate rule has not been defined within this section.

10. From the **Filter by URL Regex** section, perform one of the following steps:
 - **Filter log data by URL:**
Type a RE2-compatible regular expression pattern that identifies the set of URLs by which log data will be filtered.
 - **Upload all log data regardless of URL:**
Set it to a blank value.
11. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
12. Click **Save**.

Setting up Splunk Enterprise Log Delivery

RTLD may automatically deliver compressed log data to Splunk Enterprise by submitting HTTPS requests to it. The Splunk HTTP Event Collector (HEC) will collect and log each request. Each request contains a compressed JSON document that describes one or more log entries.

Important: The format for log data delivered to Splunk Enterprise is JSON Lines. This log format does not provide information that uniquely identifies a set of log data. As a result, there is no way to check for gaps in sequence numbers when attempting to identify missing log data.

To create a log delivery profile

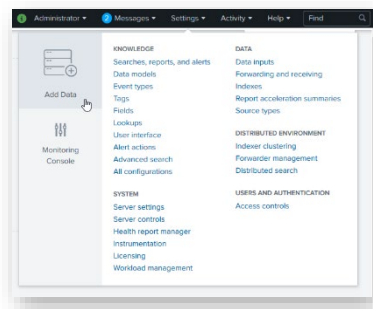
1. Set up Splunk Enterprise's HTTP Event Collector to accept CDN log data in JSON format.

i. Verify your Splunk Enterprise 7.x setup.

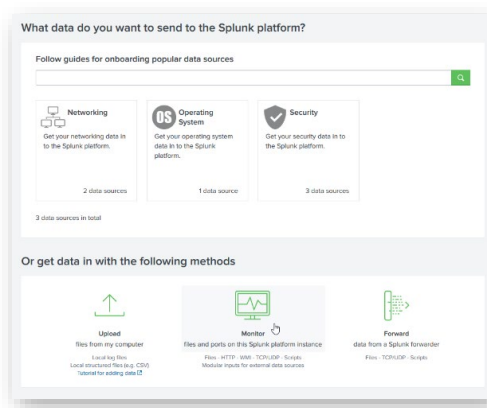
- Your instance of Splunk Enterprise 7.x must be secured with SSL.
- SSL must be enabled on the HTTP Event Collector.

For information on how to set up Splunk Enterprise, please refer to [their documentation](#).

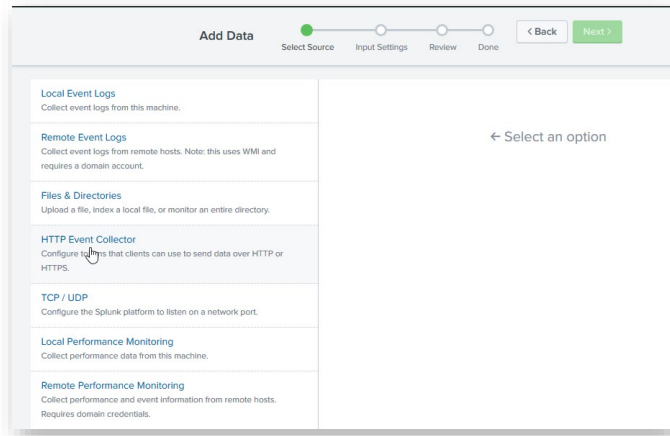
ii. From within Splunk Enterprise, click **Settings** and then **Add Data**.



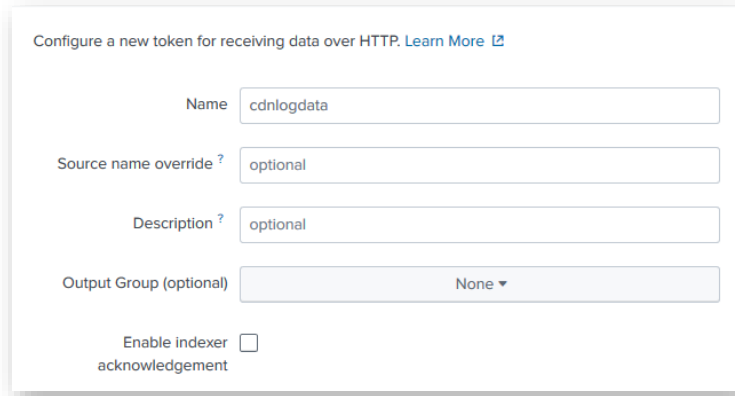
iii. Click **Monitor**.



iv. Click **HTTP Event Collector**.

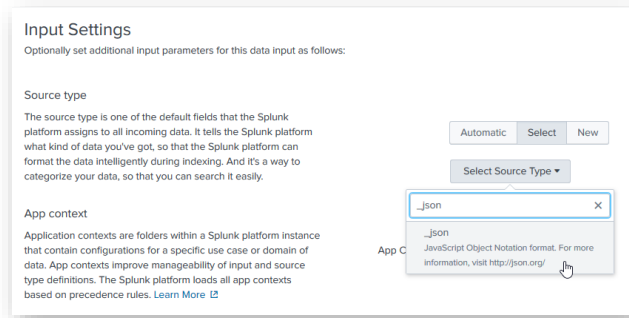


v. In the **Name** option, define a name for the CDN log data that will be collected.



vi. Click **Next >**.

vii. Click **Select** to display the **Select Source Type** option. Click that option, type "_json" to filter source types, and then select it.



viii. Click **Review**.

- ix. Click **Submit** > to finish setting up the HTTP Event Collector. An HEC token will be generated. Use this token to authorize requests posted to the HEC.
2. Perform the following steps if you have hosted Splunk Enterprise within your network:
 - i. Configure your firewall to allow POST requests from the following IP blocks:
198.7.21.0/24
 - ii. If you plan to deliver log data via a custom port, then you should also configure your firewall to open that port for the above IP blocks.
 - iii. Set up support for the HTTPS protocol.

Important: Log delivery requires a certificate whose trust anchor is a publicly trusted certificate authority (CA). Additionally, the certificate must include a chain of trust for all intermediate certificate(s) and a leaf certificate.

3. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting | WAF** page. From the main menu, navigate to **More** and then find **Real-Time Log Delivery** under **Analytics**. Select either **CDN**, **RL**, or **WAF**.
4. Click **Add Profile**.
5. From the **Log Delivery Method** option, select "Splunk Enterprise."
6. Set the **Splunk URL** option to a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.

Default URL syntax:
`https://Splunk-Enterprise-Hostname:port/services/collector/raw`

 - Replace *Splunk-Enterprise-Hostname* with the hostname where your instance of Splunk Enterprise is hosted.
 - Replace *port* with the port number (e.g., 8088) that the HTTP Event Collector is listening for data. This port number may be configured when defining your HEC's global settings.
7. Set the **HEC Token** option to the token generated for the HTTP Event Collector configuration created in step 1.

8. From the **Downsample the Logs** option, determine whether all or downsampled log data will be delivered.
 - **All Log Data:** Verify that the **Downsample the Logs** option is disabled.
 - **Downsampled Log Data:** Downsample logs to 0.1%, 1%, 25%, 50%, or 75% of total log data by enabling the **Downsample the Logs** option and then selecting the desired rate from the **Downsampling Rate** option.

Note: Use this capability to reduce the amount of data that needs to be processed or stored by Splunk Enterprise.

RTLD CDN Only: Downsampling log data also reduces usage charges for this service.

9. Log delivery setup varies according to whether you are delivering log data for CDN traffic, rate limited requests, or threats identified by WAF. Refer to the appropriate section below.
10. Set the **Log Delivery Enabled** option to the "on" position.
11. Click **Save**.

To set up RTLD CDN

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery CDN** page.
2. From the **Log Delivery** section, mark each delivery platform for which real-time log data may be delivered.
3. From the **Filter by Status Code** section, perform one of the following steps:
 - **Filter log data by status code:**
Mark each status code class (e.g., 2xx or 3xx) for which log data should be delivered. Clear all other status code classes.
 - **Upload all log data regardless of status code:**
Clear all status code classes (e.g., 2xx and 3xx).
4. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
5. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
 6. From the **Log file contains the following fields** section, perform the following steps:
 - i. Add the request headers, response headers, and cookies that will be logged for each request from the **Custom Request Headers**, **Custom Response Headers**, and **Custom Cookies** options.

Tip: You may either select or type the name of the desired headers and/or cookies. Click on the list to add additional headers or cookies. Remove a header or cookie by clicking on its x.

Note: Although other settings take effect quickly, it may take up to 90 minutes before data for custom request/response headers and cookies is logged.

 - ii. Click "Expand All."
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
 7. Click **Save**.

To set up RTLD Rate Limiting

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery Rate Limiting** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.

3. From the **Filter by Country** section, perform one of the following steps:

- **Filter log data by one or more countries:**

- Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
- Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**

Verify that a country has not been defined within this section.

4. From the **Filter by User Agent** section, perform one of the following steps:

- **Filter log data by user agent:**

Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.

- **Upload all log data regardless of user agent:**

Set it to a blank value.

5. From the **Filter by Client IP** section, perform one of the following steps:

- **Filter log data by one or more IP addresses:**

- Determine whether log data will be filtered to include or exclude requests to the selected IP addresses by selecting either "Matches" or "Does Not Match," respectively.
- Type one or more IP addresses within the option directly to the right of the above option.

- **Upload all log data regardless of IP address:**

Set it to a blank value.

6. From the **Filter by Action Type** section, perform one of the following steps:
 - **Filter log data by one or more enforcement actions:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected enforcement actions by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type the name for one or more enforcement actions.
 - **Upload all log data regardless of enforcement action:**
Set it to a blank value.
7. From the **Filter by Request Method** section, perform one of the following steps:
 - **Filter log data by one or more request methods:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected request methods by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more request method(s).
 - **Upload all log data regardless of request method:**
Set it to a blank value.
8. From the **Filter By Scope Name** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**
Verify that a security application manager has not been defined within this section.
9. From the **Filter By Action Limit ID** option, perform one of the following steps:
 - **Filter log data by one or more rate rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected rate rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more rate rule(s).
 - **Upload all log data regardless of rate rule:**
Verify that a rate rule has not been defined within this section.

10. From the **Filter by URL Regex** section, perform one of the following steps:
 - **Filter log data by URL:**
Type a RE2-compatible regular expression pattern that identifies the set of URLs by which log data will be filtered.
 - **Upload all log data regardless of URL:**
Set it to a blank value.
11. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
12. Click **Save**.

To set up RTLD WAF

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery WAF** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

 - **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**
Verify that a country has not been defined within this section.
4. From the **Filter By Managed Rule** option, perform one of the following steps:
- **Filter log data by one or more managed rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected managed rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more managed rule(s).
 - **Upload all log data regardless of managed rule:**
Verify that a managed rule has not been defined within this section.
5. From the **Filter By Access Rule** option, perform one of the following steps:
- **Filter log data by one or more access rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected access rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more access rule(s).
 - **Upload all log data regardless of access rule:**
Verify that an access rule has not been defined within this section.
6. From the **Filter By Custom Rule** option, perform one of the following steps:
- **Filter log data by one or more custom rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected custom rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more custom rule(s).
 - **Upload all log data regardless of custom rule:**
Verify that a custom rule has not been defined within this section.

7. From the **Filter By Security Application Manager** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**

Verify that a security application manager(s) has not been defined within this section.
8. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
9. Click **Save**.

To test connectivity

1. From the Splunk Enterprise's home page, click **Search & Reporting**.
2. Observe the **What to Search** section. Log data pushed from the CDN to Splunk Enterprise will be reported as events in this section.

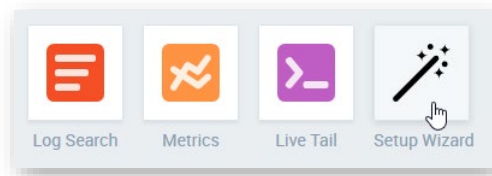
Setting up Sumo Logic Log Delivery

RTLD may automatically deliver compressed log data to Sumo Logic by submitting HTTPS requests to it. Sumo Logic will collect these requests as they are pushed from the CDN. Each request contains a compressed JSON document that describes one or more log entries.

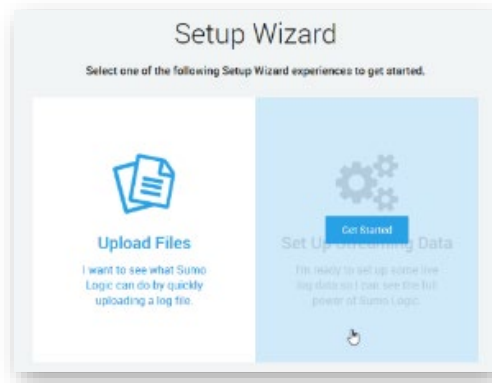
Important: The format for log data delivered to Sumo Logic is JSON Lines. This log format does not provide information that uniquely identifies a set of log data. As a result, there is no way to check for gaps in sequence numbers when attempting to identify missing log data.

To create a log delivery profile

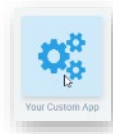
1. Set up Sumo Logic to listen for CDN log data in JSON format.
 - i. Log in to Sumo Logic.
 - ii. Click **Setup Wizard**.



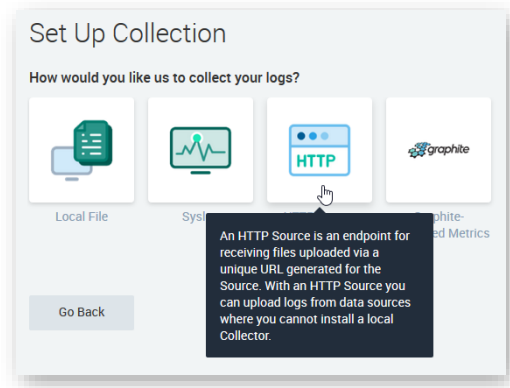
- iii. Click **Set Up Streaming Data**.



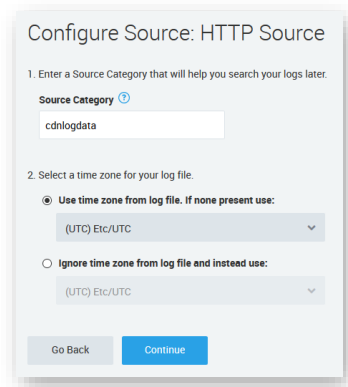
- iv. Click **Your Custom App**.



- v. Click **HTTP Source**.



- vi. In the **Source Category** option, type the name of the tag that will be applied to CDN log data. This tag may be used to search for CDN log data within Sumo Logic.



- vii. Click **Continue**. An HTTP Source for CDN log data will be created.
- viii. Copy the URL associated with this HTTP Source.
2. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting | WAF** page. From the main menu, navigate to **More** and then find **Real-Time Log Delivery** under **Analytics**. Select either **CDN, RL, or WAF**.
3. Click **Add Profile**.
4. From the **Log Delivery Method** option, select "Sumo Logic."
5. In the **Sumo Logic URL** option, paste the URL associated with the HTTP Source created in step 1.

6. From the **Downsample the Logs** option, determine whether all or downsampled log data will be delivered.
 - **All Log Data:** Verify that the **Downsample the Logs** option is disabled.
 - **Downsampled Log Data:** Downsample logs to 0.1%, 1%, 25%, 50%, or 75% of total log data by enabling the **Downsample the Logs** option and then selecting the desired rate from the **Downsampling Rate** option.

Note: Use this capability to reduce the amount of data that needs to be processed or stored by Sumo Logic.

RTLD CDN Only: Downsampling log data also reduces usage charges for this service.

7. Log delivery setup varies according to whether you are delivering log data for CDN traffic, rate limited requests, or threats identified by WAF. Refer to the appropriate section below.
8. Set the **Log Delivery Enabled** option to the "on" position.
9. Click **Save**.

To set up RTLD CDN

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery CDN** page.
2. From the **Log Delivery** section, mark each delivery platform for which real-time log data may be delivered.
3. From the **Filter by Status Code** section, perform one of the following steps:
 - **Filter log data by status code:**
Mark each status code class (e.g., 2xx or 3xx) for which log data should be delivered. Clear all other status code classes.
 - **Upload all log data regardless of status code:**
Clear all status code classes (e.g., 2xx and 3xx).
4. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
5. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
 6. From the **Log file contains the following fields** section, perform the following steps:
 - i. Add the request headers, response headers, and cookies that will be logged for each request from the **Custom Request Headers**, **Custom Response Headers**, and **Custom Cookies** options.

Tip: You may either select or type the name of the desired headers and/or cookies. Click on the list to add additional headers or cookies. Remove a header or cookie by clicking on its x.

Note: Although other settings take effect quickly, it may take up to 90 minutes before data for custom request/response headers and cookies is logged.

 - ii. Click "Expand All."
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
 7. Click **Save**.

To set up RTLD Rate Limiting

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery Rate Limiting** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**

Verify that a country has not been defined within this section.
4. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**

Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**

Set it to a blank value.

5. From the **Filter by Client IP** section, perform one of the following steps:
 - **Filter log data by one or more IP addresses:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected IP addresses by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more IP addresses within the option directly to the right of the above option.
 - **Upload all log data regardless of IP address:**
Set it to a blank value.
6. From the **Filter by Action Type** section, perform one of the following steps:
 - **Filter log data by one or more enforcement actions:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected enforcement actions by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type the name for one or more enforcement actions.
 - **Upload all log data regardless of enforcement action:**
Set it to a blank value.
7. From the **Filter by Request Method** section, perform one of the following steps:
 - **Filter log data by one or more request methods:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected request methods by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more request method(s).
 - **Upload all log data regardless of request method:**
Set it to a blank value.
8. From the **Filter By Scope Name** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).

- **Upload all log data regardless of security application manager:**
Verify that a security application manager has not been defined within this section.
9. From the **Filter By Action Limit ID** option, perform one of the following steps:
- **Filter log data by one or more rate rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected rate rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more rate rule(s).
 - **Upload all log data regardless of rate rule:**
Verify that a rate rule has not been defined within this section.
10. From the **Filter by URL Regex** section, perform one of the following steps:
- **Filter log data by URL:**
Type a RE2-compatible regular expression pattern that identifies the set of URLs by which log data will be filtered.
 - **Upload all log data regardless of URL:**
Set it to a blank value.
11. From the **Log file contains the following fields** section, perform the following steps:
- i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
12. Click **Save**.

To set up RTLD WAF

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery WAF** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
- **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.
-
- Tip:** Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).
-
- **Upload all log data regardless of country of origin:**
Verify that a country has not been defined within this section.
4. From the **Filter By Managed Rule** option, perform one of the following steps:
- **Filter log data by one or more managed rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected managed rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more managed rule(s).
 - **Upload all log data regardless of managed rule:**
Verify that a managed rule has not been defined within this section.
5. From the **Filter By Access Rule** option, perform one of the following steps:
- **Filter log data by one or more access rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected access rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more access rule(s).
 - **Upload all log data regardless of access rule:**
Verify that an access rule has not been defined within this section.

6. From the **Filter By Custom Rule** option, perform one of the following steps:
 - **Filter log data by one or more custom rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected custom rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more custom rule(s).
 - **Upload all log data regardless of custom rule:**

Verify that a custom rule has not been defined within this section.
7. From the **Filter By Security Application Manager** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**

Verify that a security application manager(s) has not been defined within this section.
8. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
9. Click **Save**.

Setting up Datadog Log Delivery

RTLD may automatically deliver compressed log data to Datadog by submitting HTTPS requests to it. Datadog will collect these requests as they are pushed from the CDN. Each request contains a compressed JSON document that describes one or more log entries.

Important: The format for log data delivered to Datadog is a JSON Array. This log format does not provide information that uniquely identifies a set of log data. As a result, there is no way to check for gaps in sequence numbers when attempting to identify missing log data.

To create a log delivery profile

1. From within the Datadog portal, copy your API key.
2. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting | WAF** page. From the main menu, navigate to **More** and then find **Real-Time Log Delivery** under **Analytics**. Select either **CDN, RL, or WAF**.
3. Click **Add Profile**.
4. From the **Log Delivery Method** option, select "Datadog."
5. From the **Datadog Site** option, select the Datadog location to which log data will be delivered.
6. From the **Datadog API Key** option, paste your Datadog API key. This API key authorizes our service to upload log data to Datadog.
7. From the **Datadog Service Attribute Value** option, type a value that uniquely identifies the data delivered as a result of this profile.
8. From the **Downsample the Logs** option, determine whether all or downsampled log data will be delivered.
 - **All Log Data:** Verify that the **Downsample the Logs** option is disabled.
 - **Downsampled Log Data:** Downsample logs to 0.1%, 1%, 25%, 50%, or 75% of total log data by enabling the **Downsample the Logs** option and then selecting the desired rate from the **Downsampling Rate** option.

Note: Use this capability to reduce the amount of data that needs to be processed or stored by Datadog.

RTLD CDN Only: Downsampling log data also reduces usage charges for this service.

9. Log delivery setup varies according to whether you are delivering log data for CDN traffic, rate limited requests, or threats identified by WAF. Refer to the appropriate section below.
10. Set the **Log Delivery Enabled** option to the "on" position.

11. Click **Save**.

To set up RTLD CDN

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery CDN** page.
2. From the **Log Delivery** section, mark each delivery platform for which real-time log data may be delivered.
3. From the **Filter by Status Code** section, perform one of the following steps:
 - **Filter log data by status code:**
Mark each status code class (e.g., 2xx or 3xx) for which log data should be delivered. Clear all other status code classes.
 - **Upload all log data regardless of status code:**
Clear all status code classes (e.g., 2xx and 3xx).
4. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

 - **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.
5. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.

6. From the **Log file contains the following fields** section, perform the following steps:
 - i. Add the request headers, response headers, and cookies that will be logged for each request from the **Custom Request Headers**, **Custom Response Headers**, and **Custom Cookies** options.

Tip: You may either select or type the name of the desired headers and/or cookies. Click on the list to add additional headers or cookies. Remove a header or cookie by clicking on its x.

Note: Although other settings take effect quickly, it may take up to 90 minutes before data for custom request/response headers and cookies is logged.

- ii. Click "Expand All."
 - iii. Mark each field that will be reported for each request submitted to the CDN.
 - iv. Clear each field for which log data should not be reported.
7. Click **Save**.

To set up RTLD Rate Limiting

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery Rate Limiting** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**
Verify that an edge CNAME has not been defined within this section.

3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**
Verify that a country has not been defined within this section.
4. From the **Filter by User Agent** section, perform one of the following steps:
 - **Filter log data by user agent:**
Type a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
 - **Upload all log data regardless of user agent:**
Set it to a blank value.
 5. From the **Filter by Client IP** section, perform one of the following steps:
 - **Filter log data by one or more IP addresses:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected IP addresses by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more IP addresses within the option directly to the right of the above option.
 - **Upload all log data regardless of IP address:**
Set it to a blank value.
 6. From the **Filter by Action Type** section, perform one of the following steps:
 - **Filter log data by one or more enforcement actions:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected enforcement actions by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type the name for one or more enforcement actions.

- **Upload all log data regardless of enforcement action:**
Set it to a blank value.
7. From the **Filter by Request Method** section, perform one of the following steps:
- **Filter log data by one or more request methods:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected request methods by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Type one or more request method(s).
 - **Upload all log data regardless of request method:**
Set it to a blank value.
8. From the **Filter By Scope Name** option, perform one of the following steps:
- **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).
 - **Upload all log data regardless of security application manager:**
Verify that a security application manager has not been defined within this section.
9. From the **Filter By Action Limit ID** option, perform one of the following steps:
- **Filter log data by one or more rate rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected rate rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more rate rule(s).
 - **Upload all log data regardless of rate rule:**
Verify that a rate rule has not been defined within this section.
10. From the **Filter by URL Regex** section, perform one of the following steps:
- **Filter log data by URL:**
Type a RE2-compatible regular expression pattern that identifies the set of URLs by which log data will be filtered.
 - **Upload all log data regardless of URL:**
Set it to a blank value.

11. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
12. Click **Save**.

To set up RTLD WAF

1. If you are not currently creating or modifying the desired log delivery profile, select it from the **Real-Time Log Delivery WAF** page.
2. From the **Filter by Edge CNAME** section, perform one of the following steps:
 - **Filter log data by one or more edge CNAME(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected edge CNAME(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more edge CNAMEs from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial hostname. For example, typing "co" will filter the list to include all hostnames that contain "co" (e.g., cdn.example.com and corp.example.org).

- **Upload all log data regardless of edge CNAME:**

Verify that an edge CNAME has not been defined within this section.
3. From the **Filter by Country** section, perform one of the following steps:
 - **Filter log data by one or more countries:**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected countries by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select one or more countries from the option directly to the right of the above option.

Tip: Filter the list by typing the entire or partial country name. For example, typing "un" will filter the list to include all countries that contain "un" (e.g., United States and United Kingdom).

- **Upload all log data regardless of country of origin:**

Verify that a country has not been defined within this section.

4. From the **Filter By Managed Rule** option, perform one of the following steps:
 - **Filter log data by one or more managed rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected managed rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more managed rule(s).
 - **Upload all log data regardless of managed rule:**

Verify that a managed rule has not been defined within this section.
5. From the **Filter By Access Rule** option, perform one of the following steps:
 - **Filter log data by one or more access rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected access rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more access rule(s).
 - **Upload all log data regardless of access rule:**

Verify that an access rule has not been defined within this section.
6. From the **Filter By Custom Rule** option, perform one of the following steps:
 - **Filter log data by one or more custom rule(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected custom rule(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more custom rule(s).
 - **Upload all log data regardless of custom rule:**

Verify that a custom rule has not been defined within this section.
7. From the **Filter By Security Application Manager** option, perform one of the following steps:
 - **Filter log data by one or more security application manager(s):**
 - i. Determine whether log data will be filtered to include or exclude requests to the selected security application manager(s) by selecting either "Matches" or "Does Not Match," respectively.
 - ii. Select or type the name for one or more security application manager(s).

- **Upload all log data regardless of security application manager:**
Verify that a security application manager(s) has not been defined within this section.
8. From the **Log file contains the following fields** section, perform the following steps:
 - i. Mark each field that will be reported for each request submitted to the CDN.
 - ii. Clear each field for which log data should not be reported.
 9. Click **Save**.

Verifying Log Data

Check for missing log data by either:

- Reviewing recent log performance statistics.
- Looking for gaps in the sequential number reported by each Real-Time Log Delivery software agent.

Log Performance Statistics

The **Log Performance** page provides a summary view and a breakdown of log delivery failures for up to the last 30 days.

Note: Find out which log files are missing by manually checking for gaps in the sequence number reported by each Real-Time Log Delivery software agent.

Key information:

- Navigate to the **Log Performance** page by performing the following steps:
 1. Navigate to the **Real-Time Log Delivery CDN | Rate Limiting | WAF** page. From the main menu, navigate to either **CDN**, **RL**, or **WAF** under **Analytics | Real-Time Log Delivery**.
 2. Select the desired profile.
 3. Click the **Analytics** tab from the upper-right hand corner of the page.
- Choose the time period for which log performance statistics will be reported from the upper-right hand corner of the page.

- Log delivery failures are graphed according to the following categories:

Category	Description
Bad Certificate	<p>Indicates that the SSL certificate corresponding to the domain where log data is being sent is invalid. Please verify your SSL certificate and then update as needed.</p> <hr/> <p>Tip: There are online tools (e.g., SSL Checker) that analyze your SSL certificate for issues.</p> <p>Reminder: Log delivery requires a certificate whose trust anchor is a publicly trusted certificate authority (CA). Additionally, the certificate must include a chain of trust for all intermediate certificate(s) and a leaf certificate.</p> <hr/>
Connection Time Out	Indicates that the destination server failed to respond in a timely fashion.
Failed Authentication	Indicates that log delivery failed due to an unauthorized request (i.e., 401 Unauthorized or 403 Forbidden).
Failed Connection	Indicates that the destination server was unavailable.
Failed to Deliver	Indicates that log delivery failed for none of the above reasons.

Checking for Sequence Number Gaps

Use the following information when assessing whether there is a gap in the sequential number reported by each Real-Time Log Delivery software agent.

- A software agent's unique ID is reported within the:
 - Log file name (AgentID) – AWS S3, Azure Blob Storage, and Google Cloud Storage only
 - JSON payload (agent-id).
- A software agent's sequence number is reported within the:
 - Log file name (SequenceNumber) – AWS S3, Azure Blob Storage, and Google Cloud Storage only
 - JSON payload (seq-num).
- The sequential number reported for each software agent starts at 0.

- This sequential number resets to 0 at the start of a new day (UTC). The date on which log data was generated is reported within the:
 - Log file name (DateStamp) – AWS S3, Azure Blob Storage, and Google Cloud Storage only
 - JSON payload (date-stamp).
- If the software agent stops running, then it will be assigned a new unique ID.

Important: If log data uses either the CSV (RTLD CDN only), JSON Array, or JSON Lines log format, then you will be unable to use the JSON payload to check for sequence number gaps. This means that you will be unable to check for sequence gaps when delivering log data to your web server(s), Splunk Enterprise, Sumo Logic, New Relic, or Datadog.

Reminder: Please refer to the **Appendix: Log File Naming Convention** section to learn the naming convention for log files.

Log File Example

RTLD CDN: On 12/8/2019, the log file naming convention was updated to include the profile ID for your Real-Time Log Delivery configuration.

Let's assume that your AWS S3 bucket, Azure Blob container, or Google Cloud Storage bucket contains the following log files:

```
wac_0001_123_20190114_0000000000000123_0.json
wac_0001_123_20190114_0000000000000123_1.json
wac_0001_123_20190114_0000000000000123_3.json
```

In this situation, we can tell that there is missing log data. Specifically, the log entries associated with the following log file are missing:

```
wac_0001_123_20190114_0000000000000123_2.json
```

Log Fields (RTLD CDN)

Log data is reported as a JSON or CSV document. Log format determines whether log data identification information will be included and how the data is formatted. Each type of log format is described below.

- **JSON:** This format includes:
 - Top-level name/value pairs that uniquely identify the set of log entries reported in the JSON document.
 - An object for each log entry associated with the current JSON document.
- **JSON Array:** This format generates a JSON document that contains an array of objects. Each object is a log entry associated with the current JSON document.
- **JSON Lines:** This format generates an invalid JSON document that contains an object on each line. Each object is a log entry associated with the current JSON document. This object is an exact match for an object contained by the Logs array.
- **CSV:** This format generates a comma-separated value (CSV) document with the following format:
 - **First Line:** Identifies the set of log fields that will be reported for each log entry and the order in which data for these fields will be reported. View log field definitions within the **Logs Array** section.
 - **Subsequent Lines:** Each subsequent line contains a log entry. Each log entry contains comma-separated values for the log fields identified in the first line.

Important: Adding or removing log fields may alter the order in which they are reported within a CSV document. It is important to rely on the CSV's first line to identify the set of log fields that are reported for each log entry and the order in which data for those fields will be provided.

Important: If log data uses either the CSV (RTLD CDN only), JSON Array, or JSON Lines log format, then it will not contain information that uniquely identifies a set of log data. If log data is delivered to a destination other than AWS S3, Azure Blob Storage, or Google Cloud Storage, then there is no way to check for gaps in sequence numbers when attempting to identify missing log data.

Note: A log entry describes a HTTP/HTTPS request that was submitted to our CDN service.

Top-Level Name/Value Pairs

Reminder: Top-level name/value pairs are unavailable for the CSV (RTLD CDN only), JSON Array, and JSON Lines log formats. If you require this information, please choose the standard JSON log format.

Top-level name/value pairs are described below.

Name	Friendly Name	Description
account_number	Customer Account Number	A string that indicates your CDN account number (e.g., 0001). This account number may be viewed from the upper-right hand corner of the MCC.
agent_id	Agent ID	A string that indicates the unique ID that identifies the Real-Time Log Delivery software agent that generated the log data.
datestamp	Date Stamp	A string that indicates the date on which the log data was generated. Syntax: YYYYMMDD Example: 20220516
logs	Log Data	An array of objects that describe the log entries associated with the current JSON document. Each object contains a set of fields that describe the request/response for a single log entry. The members of this object are described in the Logs Array section.
platform	Platform	A string that indicates the delivery platform for which CDN activity was logged. Valid values are: <ul style="list-style-type: none">• wpc: HTTP Large platform• wac: HTTP Small platform• adn: Application Delivery Network platform
profile_id	Profile ID	An integer that identifies a RTLD profile by its system-defined ID.
seq_num	Sequence Number	An integer that indicates the sequential number that identifies the order in which the log data was generated by the software agent identified by the agent_id field.

Logs Array

The logs array contains an object for each log entry associated with the current JSON document. Each object contains the members described below.

Name	Friendly Name	Description
auth_user	User (Basic Authentication)	Request A string that indicates the user name passed in the request URL for the purpose of HTTP basic authentication. Sample request: http:// joe :mypassword@cdn.mydomain.com/index.html The following value will be reported for this field: joe
background_fill_wait_time	Background Fill Wait Time	Network An integer that indicates the amount of time, in seconds, that it took for a sub-request to receive the first byte of the response.
bytes_in	Bytes In	Network An integer that indicates the sum of the number of bytes read from both of the following sources: <ul style="list-style-type: none">• Requesting Client• Origin Server
bytes_out	Bytes Out	Network An integer that indicates the number of bytes sent in the response from the edge server to the client.
cache_status	Cache Status Code	Response A string that indicates the cache status code that was generated by the request. This code indicates how the request was handled by the CDN service with regards to caching. For more information, please refer to the Cache Status Codes article in the CDN Help Center . Sample value: TCP_HIT

Name	Friendly Name	Description
client_as_org	Client AS Org	<p>Client Network</p> <p>A string that indicates the organization corresponding to the client's ASN.</p>
client_asn	Client ASN	<p>Client Network</p> <p>An integer that indicates the Autonomous System Number (ASN) associated with the client's IP address.</p>
client_city	Client City	<p>Client Geography</p> <p>A string that indicates the city from which the request originated.</p>
client_continent_code	Client Continent Code	<p>Client Geography</p> <p>A string that indicates the continent from which the request originated using one of the following codes:</p> <ul style="list-style-type: none"> • AF: Africa • AS: Asia • EU: Europe • NA: North America • OC: Oceania • SA: South and Central America • Empty String: Unknown continent
client_country_code	Client Country Code	<p>Client Geography</p> <p>An integer that indicates the two-character ISO 3166-1 code for the country from which the request originated.</p> <p>View a listing of country codes.</p>
client_geo_latitude	Client Latitude	<p>Client Geography</p> <p>A number (decimal) that indicates the approximate latitude of the postal code, city, subdivision, or country associated with the client's IP address.</p> <hr/> <p>Note: A null value is reported when the client's latitude cannot be determined.</p> <hr/>

Name	Friendly Name	Description
client_geo_longitude	Client Longitude	<p>Client Geography</p> <p>A number (decimal) that indicates the approximate longitude of the postal code, city, subdivision, or country associated with the client's IP address.</p> <hr/> <p>Note: A null value is reported when the client's longitude cannot be determined.</p> <hr/>
client_ip	Client IP Address	<p>Client Network</p> <p>A string that indicates the IP address for the computer that submitted the request to our CDN service.</p>
client_ip_version	Client IP Protocol Version	<p>Client Network</p> <p>A string that indicates the version for the client's IP protocol.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • INET: IPv4 • INET6: IPv6
client_isp	Client ISP	<p>Client Network</p> <p>A string that indicates the Internet Service Provider (ISP) associated with the client's IP address.</p>
client_port	Client Port	<p>Client Network</p> <p>An integer that indicates the port number on the client's computer to which the HTTP response was directed.</p>
client_protocol	Client Protocol	<p>Request</p> <p>A string that indicates the HTTP protocol and version defined within the client's request. Valid values are:</p> <p>HTTP_1_0 HTTP_1_1 HTTP_2_0</p>
client_region	Client Region	<p>Client Geography</p> <p>A string that indicates the geographical region (e.g., state or province) from which the request originated.</p>
client_tls_cipher	SSL Cipher Name	<p>Request</p> <p>A string that indicates the cipher suite used in the handshake between the client that submitted the request and one of our servers.</p>

Name	Friendly Name	Description
client_tls_version	TLS Version	<p>Request</p> <p>A string that indicates the TLS protocol version used for the communication between the client and our network.</p> <p>Example:</p> <p>TLSv1.2</p>
cookie_Cookie	Cookie	<p>A string that indicates the value of the cookie defined within the field name. A key-value pair will be included for each cookie defined within the Custom Cookies option.</p> <p>Example:</p> <p>The following key-value pair indicates that the sessionId cookie was set to "abc123def":</p> <p>"cookie_sessionId": "abc123def",</p>
custom_field	Custom Field	<p>General</p> <p>Indicates the data defined by the Custom Log Field 1 feature (Rules Engine).</p> <hr/> <p>Note: This field is omitted when you have not configured custom data logging via the Custom Log Field 1 feature.</p> <hr/>
file_size	File Size	<p>Response</p> <p>An integer that indicates the size, in bytes, of the requested asset (i.e., response body).</p>
first_byte_served	First Byte Served	<p>Network</p> <p>An integer that indicates whether the first byte of the requested content was served to the client. Valid values are:</p> <ul style="list-style-type: none"> • 1: True • 0: False

Name	Friendly Name	Description
host	Host Header	<p>Request Header</p> <p>A string that indicates the Host header value sent in the client's request to the CDN service.</p> <p>Example 1:</p> <p>We will examine log data for the following request: http://wpc.0001.edgecastcdn.net/800001/myorigin/index.html</p> <p>The following value will be reported for this field: wpc.0001.edgecastcdn.net</p> <p>Example 2:</p> <p>We will examine log data for the following request: http://cdn.mydomain.com/index.html</p> <p>The following value will be reported for this field: cdn.mydomain.com</p>
last_byte_served	Last Byte Served	<p>Network</p> <p>An integer that indicates whether the last byte of the requested content was served to the client. Valid values are:</p> <ul style="list-style-type: none"> • 1: True • 0: False
method	HTTP Method	<p>Request</p> <p>A string that indicates the request's HTTP method (e.g., GET, HEAD, and POST).</p>
origin_name	Origin Name	<p>Request Header</p> <p>A string that indicates the URL segment that appears directly after your account number in the CDN URL. This URL segment is identified as <i>Directory</i> below.</p> <p><i>{Scheme}://{Hostname}/{Origin Identifier}{Account Number}/{Directory}/{Content Path}</i></p> <hr/> <p>Note: Our CDN converts edge CNAME URLs to CDN URLs.</p> <hr/>

Name	Friendly Name	Description
path	URL Path	<p>Request</p> <p>A string that indicates the URL path for the CDN content that was requested, posted, or deleted. This URL, which excludes the query string, is reported as a relative path that starts directly after the hostname.</p> <hr/> <p>Note: What is the difference between path and rewritten_path? The path field always reports the requested URL's relative path, while rewritten_path reports the relative path after the URL has been rewritten (e.g., URL rewrites due to edge CNAME URLs or the Rules Engine's URL Rewrite feature).</p> <hr/> <p>Example 1:</p> <p>We will examine log data for the following request: http://wpc.0001.edgecastcdn.net/800001/myorigin/index.html</p> <p>The following value will be reported for this field: /800001/myorigin/index.html</p> <p>Example 2:</p> <p>We will examine log data for the following request: http://cdn.mydomain/index.html?parameter=value</p> <p>The following value will be reported for this field: /index.html</p>
platform	Platform	<p>Network</p> <p>A string that identifies the delivery platform that handled the request. Valid values are:</p> <ul style="list-style-type: none"> • wpc: HTTP Large platform • wac: HTTP Small platform • adn: Application Delivery Network platform
pop	POP	<p>Network</p> <p>A string that identifies the POP that handled the client's request by its three-letter abbreviation.</p>

Name	Friendly Name	Description
prewrite_time	Prewrite Time	<p>Performance</p> <p>A number (decimal) that indicates the length of time, in seconds, that it took to initiate the response to the client. This metric measures the duration between when an edge server receives a request and when it starts sending the response to the client.</p> <p>Syntax:</p> <p><i>Seconds.Microseconds</i></p>
proxy_ip	Proxy IP	<p>Network</p> <p>A string that indicates the IP address to which an edge server forwarded a request. This IP address may identify an Origin Shield server, an ADN Gateway server, or an external web server associated with a customer origin configuration.</p>
proxy_port	Proxy Port	<p>Network</p> <p>An integer that indicates the port number on an Origin Shield server, an ADN Gateway server, or an external web server to which an edge server forwarded a request. Valid values are:</p> <ul style="list-style-type: none"> • 80: HTTP request • 443: HTTPS request

Name	Friendly Name	Description
proxy_type	Proxy Type	<p data-bbox="800 254 911 279">Network</p> <p data-bbox="800 304 1422 401">An integer that indicates the type of server to which an edge server forwarded a request. Valid values are:</p> <ul data-bbox="849 428 1430 684" style="list-style-type: none"> <li data-bbox="849 428 1430 562">• NONE: Indicates that the request was served directly from the edge of our network and therefore it was not proxied to another server. <li data-bbox="849 590 1430 684">• MIDGRESS: Indicates that an edge server proxied the request to a different CDN server. <p data-bbox="898 695 1019 720">Examples:</p> <ul data-bbox="946 747 1430 898" style="list-style-type: none"> <li data-bbox="946 747 1430 810">▪ The request was proxied to an Origin Shield or an ADN Gateway server. <li data-bbox="946 837 1430 898">▪ The request was proxied to a peer edge server due to hotfiling. <ul data-bbox="849 926 1430 1161" style="list-style-type: none"> <li data-bbox="849 926 1430 989">• ORIGIN: Indicates that the request was proxied to either of the following servers: <ul data-bbox="946 1016 1430 1161" style="list-style-type: none"> <li data-bbox="946 1016 1430 1100">▪ An external web server associated with a customer origin configuration. <li data-bbox="946 1127 1430 1161">▪ A CDN storage server.
query	Query String	<p data-bbox="800 1188 902 1213">Request</p> <p data-bbox="800 1239 1430 1299">A string that indicates the query string defined in the request URL.</p> <hr data-bbox="800 1318 1430 1323"/> <p data-bbox="800 1331 1382 1392">Note: This field excludes the question mark that delimits the query string from the request URL.</p> <hr data-bbox="800 1396 1430 1400"/>

Name	Friendly Name	Description
read_time	Read Time	<p>Performance</p> <p>A number (decimal) that indicates the length of time, in seconds, that it took an edge server to read the response. This measurement varies according to the number of layers (e.g., peer edge server, Origin Shield server, or origin server) through which the request is proxied.</p> <hr/> <p>Note: Our servers forward data as it is read. This means that the read_time and write_time reported for an asset spans over an overlapping time period.</p> <hr/> <p>Syntax:</p> <p><i>Seconds.Microseconds</i></p>
referrer	Referrer	<p>Request Header</p> <p>A string that indicates the Referrer header value sent in the client's request to the CDN service. This header reports the URL of the site from which the request originated.</p> <hr/> <p>Note: This field will typically be set to a blank value for the HTTP Small and the ADN platforms.</p>
req_hdr_RequestHeader	Request Header	<p>A string that indicates the value of the request header defined within the field name. A key-value pair will be included for each request header defined within the Custom Request Headers option.</p> <hr/> <p>Note: The name of this field identifies a request header using lowercase letters. Additionally, hyphens in the request header's name are converted to underscores.</p> <hr/> <p>Example:</p> <p>The following key-value pair indicates that the Accept-Encoding request header was set to "gzip, deflate":</p> <pre>"req_hdr_accept_encoding": "gzip, deflate",</pre>

Name	Friendly Name	Description
resp_hdr_ResponseHeader	Response Header	<p>A string that indicates the value of the response header defined within the field name. A key-value pair will be included for each response header defined within the Custom Response Headers option.</p> <hr/> <p>Note: The name of this field identifies a response header using lowercase letters. Additionally, hyphens in the response header's name are converted to underscores.</p> <hr/> <p>Example:</p> <p>The following key-value pair indicates that the Content-Length request header was set to "445":</p> <pre>"resp_hdr_content_length": "445",</pre>
rewritten_path	Rewritten URL Path	<p>Request</p> <p>A string that indicates the rewritten URL path for the CDN content that was requested, posted, or deleted. This URL, which excludes the query string, is reported as a relative path that starts directly after the hostname.</p> <p>This URL path will be rewritten under the following circumstances:</p> <ul style="list-style-type: none"> • Edge CNAME URLs: The request URL will be rewritten to point to the source (i.e., customer origin or CDN storage) associated with the edge CNAME. See example 2 below. • URL Rewrite: Rules Engine allows requests to be rewritten via the URL Rewrite feature. <p>If either of the above conditions apply, this field will report the URL path associated with the rewritten request.</p> <hr/> <p>Important: This field reports the URL path after all URL rewrites have been applied to the URL. For example, if the URL Rewrite feature is applied to an edge CNAME URL, then this field will report the URL path as determined by the URL Rewrite feature.</p> <p>Reminder: What is the difference between path and rewritten_path? The path field always reports the requested URL's relative path, while rewritten_path reports the relative path after the URL has been rewritten (e.g., URL rewrites due to edge CNAME</p>

Name	Friendly Name	Description
		<p>URLs or the Rules Engine's URL Rewrite feature).</p> <hr/> <p>Example 1:</p> <p>We will examine log data for the following request: http://wpc.0001.edgecastcdn.net/800001/myorigin/index.html</p> <p>The following value will be reported for this field: /800001/myorigin/index.html</p> <p>Example 2:</p> <p>We will examine log data for the following request: http://cdn.mydomain.com/index.html?parameter=value</p> <hr/> <p>Note: This second example assumes that an edge CNAME called "cdn.mydomain.com" maps to a HTTP Large customer origin called "myorigin."</p> <hr/> <p>The following value will be reported for this field: /800001/myorigin/index.html</p> <hr/> <p>Note: The same value is reported for both requests, since they both point to the same asset.</p> <hr/>
scheme	Scheme	<p>Request</p> <p>A string that indicates the request's scheme. Valid values are: http https</p>
server_ip	Edge Server IP Address	<p>Network</p> <p>A string that indicates the IP address for the edge server that processed the request.</p>
server_port	Edge Server Port	<p>Network</p> <p>An integer that indicates the port number on an edge server to which the client directed a request.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • 80: HTTP request • 443: HTTPS request

Name	Friendly Name	Description
status	Status Message	<p>Response</p> <p>An integer that indicates the HTTP status message for the response generated by an origin server, origin shield server, ADN gateway server, or an edge server.</p> <p>Sample value:</p> <p>OK</p>
status_code	Status Code	<p>Response</p> <p>A string that indicates the HTTP status code for the response generated by an origin server, origin shield server, ADN gateway server, or an edge server.</p> <p>Sample value:</p> <p>200</p>
timestamp	Timestamp	<p>Response</p> <p>A number (decimal) that indicates the Unix time, in seconds, at which an edge server delivered the requested content to the client.</p> <p>Syntax:</p> <p><i>Seconds.Microseconds</i></p>
total_time	Total Time	<p>Performance</p> <p>A number (decimal) that indicates the length of time, in seconds, that it took to send a response to the client. This metric measures the duration between when an edge server receives a request and when it finishes sending the response to the client.</p> <hr/> <p>Note: This field does not take into account network time.</p> <hr/> <p>Syntax:</p> <p><i>Seconds.Microseconds</i></p>
user_agent	User Agent	<p>Request Header</p> <p>A string that indicates the user agent that submitted the HTTP request to our CDN service. A web browser is an example of a user agent.</p>

Name	Friendly Name	Description
uuid	UUID	<p>Request</p> <p>A string that identifies the request using a universally unique identifier (UUID).</p> <hr/> <p>Note: This field is our implementation of a unique identifier and it bears no relationship to a traditional universally unique identifier (UUID).</p> <hr/>
write_time	Write Time	<p>Performance</p> <p>A number (decimal) that indicates the length of time, in seconds, that it took an edge server to write the response. This metric measures the duration between when an edge server starts writing the response and when it finishes sending the response to the client.</p> <hr/> <p>Note: Our servers forward data as it is read. This means that the read_time and write_time reported for an asset spans over an overlapping time period.</p> <p>Note: This field does not take into account network time.</p> <hr/> <p>Syntax:</p> <p><i>Seconds.Microseconds</i></p>

Sample Log Data

Sample log data that contains two log entries is provided below for all log formats.

Example (JSON):

```
{
  "agent_id": "123450008619D55A",
  "seq_num": 0,
  "platform": "adn",
  "account_number": "0001",
  "datestamp": "20180416",
  "logs": [{
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0)
    Gecko/20100101 Firefox/59.0",
    "rewritten_path":
    "/800001/marketing/Resources/Scripts/script.js",
    "timestamp": 1523916295.768957,
    "client_ip": "121.11.22.3",
    "client_ip_version": "INET",
    "client_port": 25773,
    "status": "OK",
    "cache_status": "TCP_HIT",
    "bytes_out": 65895,
    "write_time": 0.000707,
    "file_size": 65535,
    "server_ip": "155.155.123.210",
    "server_port": 80,
    "method": "GET",
    "host": "cdn.mydomain.com",
    "query": "",
    "auth_user": "",
    "read_time": 0.000000,
    "bytes_in": 812,
    "referer": "http://cdn.mydomain.com/default.htm",
    "path": "/Resources/Scripts/script.js",
    "status_code": 200
  }, {
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0)
    Gecko/20100101 Firefox/59.0",
    "rewritten_path": "/800001/marketing/skins/Images/print-black-24-
```

```
px.png",
    "timestamp": 1523916295.841614,
    "client_ip": "123.10.10.2",
    "client_ip_version": "INET",
    "client_port": 25773,
    "status": "OK",
    "cache_status": "TCP_HIT",
    "bytes_out": 563,
    "write_time": 0.000213,
    "file_size": 262,
    "server_ip": "156.15.122.134",
    "server_port": 80,
    "method": "GET",
    "host": "cdn.mydomain.com",
    "query": "",
    "auth_user": "",
    "read_time": 0.000000,
    "bytes_in": 866,
    "referer": "http://cdn.mydomain.com/skins/styles/styles.css",
    "path": "/skins/Images/print-black-24-px.png",
    "status_code": 200
  }
]
}
```


Example (JSON array):

```
[{
  "user_agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0)
  Gecko/20100101 Firefox/59.0",
  "rewritten_path": "/800001/marketing/Resources/Scripts/script.js",
  "timestamp": 1523916295.768957,
  "client_ip": "121.11.22.3",
  "client_ip_version": "INET",
  "client_port": 25773,
  "status": "OK",
  "cache_status": "TCP_HIT",
  "bytes_out": 65895,
  "write_time": 0.000707,
  "file_size": 65535,
  "server_ip": "155.155.123.210",
  "server_port": 80,
  "method": "GET",
  "host": "cdn.mydomain.com",
  "query": "",
  "auth_user": "",
  "read_time": 0.000000,
  "bytes_in": 812,
  "referer": "http://cdn.mydomain.com/default.htm",
  "path": "/Resources/Scripts/script.js",
  "status_code": 200
}, {
  "user_agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0)
  Gecko/20100101 Firefox/59.0",
  "rewritten_path": "/800001/marketing/skins/Images/print-black-24-px.png",
  "timestamp": 1523916295.841614,
  "client_ip": "123.10.10.2",
  "client_ip_version": "INET",
  "client_port": 25773,
```

```

        "status": "OK",
        "cache_status": "TCP_HIT",
        "bytes_out": 563,
        "write_time": 0.000213,
        "file_size": 262,
        "server_ip": "156.15.122.134",
        "server_port": 80,
        "method": "GET",
        "host": "cdn.mydomain.com",
        "query": "",
        "auth_user": "",
        "read_time": 0.000000,
        "bytes_in": 866,
        "referer": "http://cdn.mydomain.com/skins/styles/styles.css",
        "path": "/skins/Images/print-black-24-px.png",
        "status_code": 200
    }
]

```

Example (JSON lines):

```

{"user_agent": "Mozilla/5.0 (Windows NT ...)"}
{"user_agent": "Mozilla/5.0 (Windows NT ...)"}

```

Example (CSV):

```

user_agent,rewritten_path,timestamp,...,status_code
"Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0) Gecko/20100101
Firefox/59.0","/800001/marketing/Resources/Scripts/script.js",1523916295.768957,...,200
"Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0) Gecko/20100101
Firefox/59.0","/800001/marketing/skins/Images/print-black-24-
px.png",1523916295.841614,...,200

```

Log Fields (RTLD Rate Limiting)

Log data is reported as a JSON document. Log format determines whether log data identification information will be included and how the data is formatted. Each type of log format is described below.

- **JSON:** This format includes:
 - Top-level name/value pairs that uniquely identify the set of log entries reported in the JSON document.
 - An object for each log entry associated with the current JSON document.
- **JSON Array:** This format generates a JSON document that contains an array of objects. Each object is a log entry associated with the current JSON document.
- **JSON Lines:** This format generates an invalid JSON document that contains an object on each line. Each object is a log entry associated with the current JSON document. This object is an exact match for an object contained by the Logs array.

Important: If log data uses either the JSON Array or JSON Lines log format, then it will not contain information that uniquely identifies a set of log data. If log data is delivered to a destination other than AWS S3, Azure Blob Storage, or Google Cloud Storage, then there is no way to check for gaps in sequence numbers when attempting to identify missing log data.

Note: A log entry describes a HTTP/HTTPS request that was submitted to our CDN service.

Top-Level Name/Value Pairs

Reminder: Top-level name/value pairs are unavailable for the JSON Array and JSON Lines log formats. If you require this information, please choose the standard JSON log format.

Top-level name/value pairs are described below.

Name	Friendly Name	Description
account_number	Customer Account Number	A string that indicates your CDN account number (e.g., 0001). This account number may be viewed from the upper-right hand corner of the MCC.
agent_id	Agent ID	A string that indicates the unique ID that identifies the Real-Time Log Delivery software agent that generated the log data.
datestamp	Date Stamp	A string that indicates the date on which the log data was generated. Syntax: YYYYMMDD Example: 20220516

Name	Friendly Name	Description
logs	Log Data	An array of objects that describe the log entries associated with the current JSON document. Each object contains a set of fields that describe the request/response for a single log entry. The members of this object are described in the Logs Array section.
profile_id	Profile ID	An integer that identifies a RTLD profile by its system-defined ID.
seq_num	Sequence Number	An integer that indicates the sequential number that identifies the order in which the log data was generated by the software agent identified by the agent_id field.
service	Service	This field always reports "rl."

Logs Array

The logs array contains an object for each log entry associated with the current JSON document. Each object contains the members described below.

Name	Friendly Name	Description
account_number	Customer AN	General A string that indicates your CDN account number (e.g., 0001). This account number may be viewed from the upper-right hand corner of the MCC.
client_city	City Name	Client Geography A string that indicates the city from which the request originated.
client_country_code	Country Code	Client Geography A string that indicates the two-character ISO 3166-1 code for the country from which the request originated.
client_country	Country Name	Client Geography A string that indicates the country from which the request originated.
client_ip	Client IP	Client Network A string that indicates the IP address for the computer that submitted the request to our CDN.

Name	Friendly Name	Description
host	Host	Request Header A string that indicates the Host header value sent in the client's request to the CDN.
limit_action_duration	Rate Limiting Action Duration	Security Configuration A string that indicates the minimum length of time, in seconds, that eligible requests were rate limited when the event took place.
limit_action_percentage	Rate Limiting Action Percentage	Security Configuration A string that indicates the percentage of eligible requests that were rate limited when the event took place.
limit_action_type	Rate Limiting Action Type	Security Configuration A string that indicates how the rate limit was enforced on the request. <ul style="list-style-type: none"> • BLOCK_REQUEST: Block Request • ALERT: Alert Only • REDIRECT_302: Redirect (HTTP 302) • CUSTOM_RESPONSE: Custom Response • DROP_REQUEST: Drop Request (503 Service Unavailable response with a retry-after of 10 seconds)
limit_id	Rate Limiting Action Limit ID	Security Configuration A string that indicates the system-defined ID of the rate rule whose rate limit was exceeded by the request.
limit_start_timestamp	Rate Limiting Action Start Epoch	Security Configuration A string that indicates the timestamp, in Unix time (milliseconds), at which the enforcement of the rate limit started.
method	Request Method	Security Configuration A string that indicates the request's HTTP method.

Name	Friendly Name	Description
referer	Referer	<p>Request Header</p> <p>A string that indicates the Referer header value sent in the client's request to the CDN. This header reports the URL of the site from which the request originated.</p> <hr/> <p>Note: This field will typically be set to a blank value for the HTTP Small and the ADN platforms.</p> <hr/>
scope_id	Scope ID	<p>Security Configuration</p> <p>A string that indicates the system-defined ID of the Security Application Manager configuration that enforced the rate limit.</p>
scope_name	Scope Name	<p>Security Configuration</p> <p>A string that indicates the name of the Security Application Manager configuration that enforced the rate limit.</p>
timestamp	Epoch Time	<p>Response</p> <p>A decimal that indicates the Unix time, in seconds, at which an edge server delivered the requested content to the client.</p> <p>Syntax:</p> <p><i>Seconds.Microseconds</i></p>
url	URL	<p>Request</p> <p>A string that indicates the URL that was requested.</p>
user_agent	User Agent	<p>Request Header</p> <p>A string that indicates the user agent that submitted the HTTP request to our CDN.</p>

Sample Log Data

Sample log data that contains two log entries is provided below for all log formats.

JSON log format:

```
{
  "agent_id": "123450008619D55A",
  "seq_num": 4,
  "service": "rl",
  "account_number": "0001",
  "profile_id": 1,
  "datestamp": "20210812",
  "logs": [{
    "timestamp": 1628804857.1012251,
    "account_number": "0001",
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0",
    "url": "https://cdn.example.com/images/bunny.png",
    "client_ip": "93.113.59.253",
    "referer": "https://models.example.com/",
    "host": "cdn.example.com",
    "client_country_code": "RO",
    "client_country": "Romania",
    "client_city": "Bucharest",
    "limit_action_duration": 0,
    "limit_id": "SJu03wey",
    "limit_action_percentage": 100,
    "limit_start_timestamp": 1628804857.167,
    "limit_action_type": "ALERT",
    "method": "GET",
    "scope_id": "dJR9RX4S",
    "scope_name": "SAM"
  }, {
    "timestamp": 1628804858.1012254,
    "account_number": "0001",
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0",
    "url": "https://cdn.example.com/photos/sky.png",
    "client_ip": "107.190.102.233",
```

```

        "referer": "https://example2.com/",
        "host": "cdn.example.com",
        "client_country_code": "CA",
        "client_country": "Canada",
        "client_city": "Windsor",
        "limit_action_duration": 0,
        "limit_id": "SJuO3wey",
        "limit_action_percentage": 100,
        "limit_start_timestamp": 1628804832.024,
        "limit_action_type": "ALERT",
        "method": "GET",
        "scope_id": "dJR9RX4S",
        "scope_name": "SAM"
    }
]
}

```

JSON Array log format:

```

[
  {
    "timestamp": 1628804857.1012251,
    "account_number": "0001",
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0",
    "url": "https://cdn.example.com/images/bunny.png",
    "client_ip": "93.113.59.253",
    "referer": "https://models.example.com/",
    "host": "cdn.example.com",
    "client_country_code": "RO",
    "client_country": "Romania",
    "client_city": "Bucharest",
    "limit_action_duration": 0,
    "limit_id": "SJuO3wey",
    "limit_action_percentage": 100,
    "limit_start_timestamp": 1628804857.167,
    "limit_action_type": "ALERT",
  }
]

```



```

        "method": "GET",
        "scope_id": "dJR9RX4S",
        "scope_name": "SAM"
    }, {
        "timestamp": 1628804858.1012254,
        "account_number": "0001",
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0)
        Gecko/20100101 Firefox/59.0",
        "url": "https://cdn.example.com/photos/sky.png",
        "client_ip": "107.190.102.233",
        "referrer": "https://example2.com/",
        "host": "cdn.example.com",
        "client_country_code": "CA",
        "client_country": "Canada",
        "client_city": "Windsor",
        "limit_action_duration": 0,
        "limit_id": "SJuO3wey",
        "limit_action_percentage": 100,
        "limit_start_timestamp": 1628804832.024,
        "limit_action_type": "ALERT",
        "method": "GET",
        "scope_id": "dJR9RX4S",
        "scope_name": "SAM"
    }
]

```

JSON Lines log format:

```

{"user_agent": "Mozilla/5.0 (Windows NT ...}
{"user_agent": "Mozilla/5.0 (Windows NT ...}

```

Log Fields (RTLD WAF)

Log data is reported as a JSON document. Log format determines whether log data identification information will be included and how the data is formatted. Each type of log format is described below.

- **JSON:** This format includes:
 - Top-level name/value pairs that uniquely identify the set of log entries reported in the JSON document.
 - An object for each log entry associated with the current JSON document.
- **JSON Array:** This format generates a JSON document that contains an array of objects. Each object is a log entry associated with the current JSON document.
- **JSON Lines:** This format generates an invalid JSON document that contains an object on each line. Each object is a log entry associated with the current JSON document. This object is an exact match for an object contained by the Logs array.

Important: If log data uses either the JSON Array or JSON Lines log format, then it will not contain information that uniquely identifies a set of log data. If log data is delivered to a destination other than AWS S3, Azure Blob Storage, or Google Cloud Storage, then there is no way to check for gaps in sequence numbers when attempting to identify missing log data.

Note: A log entry describes a HTTP/HTTPS request that was submitted to our CDN service.

Top-Level Name/Value Pairs

Reminder: Top-level name/value pairs are unavailable for the JSON Array and JSON Lines log formats. If you require this information, please choose the standard JSON log format.

Top-level name/value pairs are described below.

Name	Friendly Name	Description
account_number	Customer Account Number	A string that indicates your CDN account number (e.g., 0001). This account number may be viewed from the upper-right hand corner of the MCC.
agent_id	Agent ID	A string that indicates the unique ID that identifies the Real-Time Log Delivery software agent that generated the log data.
timestamp	Date Stamp	A string that indicates the date on which the log data was generated. Syntax: YYYYMMDD Example: 20220516

Name	Friendly Name	Description
logs	Log Data	An array of objects that describe the log entries associated with the current JSON document. Each object contains a set of fields that describe the request/response for a single log entry. The members of this object are described in the Logs Array section.
profile_id	Profile ID	An integer that identifies a RTLD profile by its system-defined ID.
seq_num	Sequence Number	An integer that indicates the sequential number that identifies the order in which the log data was generated by the software agent identified by the agent_id field.
service	Service	This field always reports "waf."

Logs Array

The logs array contains an object for each log entry associated with the current JSON document. Each object contains the members described below.

Name	Friendly Name	Description
account_number	Customer AN	<p>General</p> <p>A string that indicates your CDN account number (e.g., 0001). This account number may be viewed from the upper-right hand corner of the MCC.</p>
action_type	Action Type	<p>Event</p> <p>A string that indicates the action that was triggered as a result of the violation. Valid values are:</p> <ul style="list-style-type: none"> • BLOCK_REQUEST: Indicates that the request that violated a rule was blocked. • NOP: Indicates that an alert was generated in response to the rule violation. • REDIRECT_302: Indicates that the request that violated a rule was redirected to the URL associated with the instance defined by the Instance Name field. • CUSTOM_RESPONSE: Indicates that a custom response was returned to the client that submitted a request that violated a rule.

Name	Friendly Name	Description
client_city	City Name	<p>Client Geography</p> <p>A string that indicates the city from which the request originated.</p>
client_country_code	Country Code	<p>Client Geography</p> <p>A string that indicates the two-character ISO 3166-1 code for the country from which the request originated.</p>
client_country	Country Name	<p>Client Geography</p> <p>A string that indicates the country from which the request originated.</p>
client_ip	IP Address	<p>Client Network</p> <p>A string that indicates the IP address for the computer that submitted the request to our CDN.</p>
host	Host	<p>Request Header</p> <p>A string that indicates the Host header value sent in the client's request to the CDN.</p>
referrer	Referer	<p>Request Header</p> <p>A string that indicates the Referer header value sent in the client's request to the CDN. This header reports the URL of the site from which the request originated.</p> <hr/> <p>Note: This field will typically be set to a blank value for the HTTP Small and the ADN platforms.</p> <hr/>
rule_message	Rule Message	<p>Event</p> <p>A string that provides a description of the rule that the request violated.</p>
rule_tags	Rule Tags	<p>Event</p> <p>An array that contains a string value for each tag associated with the rule that the request violated. These tags may be used to determine whether a rule, access control, or global setting was violated.</p>

Name	Friendly Name	Description
server_port	Server Port	<p>Network</p> <p>An integer that indicates the port number on an edge server to which the client directed a request. Valid values are:</p> <ul style="list-style-type: none"> • 80: HTTP request • 443: HTTPS request
sub_events_count	Sub Events Count	<p>Sub Event</p> <p>An integer that indicates the total number of sub events.</p>
sub_events	Sub Events	<p>Sub Event</p> <p>An array that contains a list of fields that describe each sub event associated with the current event. A sub event is reported for each rule violation incurred by a request.</p>
timestamp	Epoch Time	<p>Response</p> <p>A decimal that indicates the Unix time, in seconds, at which an edge server delivered the requested content to the client.</p> <p>Syntax:</p> <p><i>Seconds.Microseconds</i></p>
url	URL	<p>Request</p> <p>A string that indicates the URL that was requested.</p>
user_agent	User Agent	<p>Request Header</p> <p>A string that indicates the user agent that submitted the HTTP request to our CDN.</p>
uuid	Event ID	<p>Request</p> <p>A string that indicates the unique ID assigned to the event.</p> <hr/> <p>Tip: Pass this ID to the Get Event Log Entry endpoint to retrieve this event log entry.</p> <hr/>
waf_instance_name	Instance Name	<p>Security Configuration</p> <p>A string that indicates the name of the instance that activated the profile containing the rule that the requested violated.</p>

Name	Friendly Name	Description
waf_profile_name	Profile Name	Security Configuration A string that indicates the name of the profile that triggered the violation.
waf_profile_type	Profile Type	Security Configuration A string that indicates whether the request was screened as a result of an instance's production or audit profile. Valid values are: PRODUCTION AUDIT

sub_events Array

The sub_events array contains a list of fields that describe each sub event associated with the current event. A sub event is reported for each rule violation incurred by a request.

Name	Friendly Name	Description
matched_on	Matched On	A string that indicates the variable that identifies where the violation was found.
matched_value	Matched Value	A string that indicates the value of the variable defined in the matched_on field.
rule_id	Rule ID	An integer that indicates the ID for the rule that the request violated.
rule_message	Rule Message	A string that provides a description of the rule that the request violated.
total_anomaly_score	Total Anomaly Score	An integer that indicates the total anomaly score for the current rule violation. This score is calculated by summing the anomaly score of the current rule violation with all rule violations reported above this sub event.

Sample Log Data

Sample log data that contains two log entries is provided below for all log formats.

JSON log format:

```
{
  "agent_id": "123450008619D55A",
  "seq_num": 0,
  "service": "waf",
  "account_number": "0001",
  "profile_id": 0,
  "datestamp": "20201008",
  "logs": [{
    "timestamp": 1602200337.177535713,
    "user_agent": "curl/7.64.1",
    "url": "https://cdn.example.com/",
    "client_ip": "190.220.230.2",
    "referer": "",
    "host": "cdn.example.com",
    "uuid": "38046679731278771327748811544613832704",
    "client_country_code": "US",
    "waf_profile_name": "Site 1",
    "waf_profile_type": "PRODUCTION",
    "waf_instance_name": "Site 1 Instance",
    "sub_events_count": 1,
    "sub_events": [{
      "total_anomaly_score": 0,
      "matched_on": "REQUEST_METHOD",
      "matched_value": "POST",
      "rule_id": 80009,
      "rule_message": "Method is not allowed by policy"
    }
  ],
  "rule_tags": [],
  "rule_message": "Method is not allowed by policy",
  "action_type": "BLOCK_REQUEST",
  "server_port": 443,
  "client_country": "United States",
```

```

        "client_city": "Los Angeles"
    }, {
        "timestamp": 1602200338.598465258,
        "user_agent": "curl/7.64.1",
        "url": "https://cdn.example.com/",
        "client_ip": "230.180.240.23",
        "referrer": "",
        "host": "cdn.example.com",
        "uuid": "38046679731278771327748811544613832998",
        "client_country_code": "US",
        "waf_profile_name": "Site 1",
        "waf_profile_type": "PRODUCTION",
        "waf_instance_name": "Site 1 Instance",
        "sub_events_count": 1,
        "sub_events": [{
            "total_anomaly_score": 0,
            "matched_on": "REQUEST_METHOD",
            "matched_value": "POST",
            "rule_id": 80009,
            "rule_message": "Method is not allowed by policy"
        }
    ],
        "rule_tags": [],
        "rule_message": "Method is not allowed by policy",
        "action_type": "BLOCK_REQUEST",
        "server_port": 443,
        "client_country": "United States",
        "client_city": "Los Angeles"
    }
]
}

```


JSON Array log format:

```
{
  "timestamp": 1602200337.177535713,
  "user_agent": "curl/7.64.1",
  "url": "https://cdn.example.com/",
  "client_ip": "190.220.230.2",
  "referer": "",
  "host": "cdn.example.com",
  "uuid": "38046679731278771327748811544613832704",
  "client_country_code": "US",
  "waf_profile_name": "Site 1",
  "waf_profile_type": "PRODUCTION",
  "waf_instance_name": "Site 1 Instance",
  "sub_events_count": 1,
  "sub_events": [{
    "total_anomaly_score": 0,
    "matched_on": "REQUEST_METHOD",
    "matched_value": "POST",
    "rule_id": 80009,
    "rule_message": "Method is not allowed by policy"
  }
],
  "rule_tags": [],
  "rule_message": "Method is not allowed by policy",
  "action_type": "BLOCK_REQUEST",
  "server_port": 443,
  "client_country": "United States",
  "client_city": "Los Angeles"
}, {
  "timestamp": 1602200338.598465258,
  "user_agent": "curl/7.64.1",
  "url": "https://cdn.example.com/",
```

```
"client_ip": "230.180.240.23",
"referer": "",
"host": "cdn.example.com",
"uuid": "38046679731278771327748811544613832998",
"client_country_code": "US",
"waf_profile_name": "Site 1",
"waf_profile_type": "PRODUCTION",
"waf_instance_name": "Site 1 Instance",
"sub_events_count": 1,
"sub_events": [{
    "total_anomaly_score": 0,
    "matched_on": "REQUEST_METHOD",
    "matched_value": "POST",
    "rule_id": 80009,
    "rule_message": "Method is not allowed by policy"
  }
],
"rule_tags": [],
"rule_message": "Method is not allowed by policy",
"action_type": "BLOCK_REQUEST",
"server_port": 443,
"client_country": "United States",
"client_city": "Los Angeles"
}
]
```

JSON Lines log format:

```
{"user_agent": "Mozilla/5.0 (Windows NT ...}
{"user_agent": "Mozilla/5.0 (Windows NT ...}
```

Appendix

Log File Naming Convention

RTLD CDN: On 12/8/2019, the log file naming convention was updated to include the profile ID for your Real-Time Log Delivery configuration.

Note: This section only applies to AWS S3, Azure Blob Storage, and Google Cloud Storage log file delivery.

The log data stored within an object is compressed using gzip. Each object follows this naming convention:

```
LogType_AN_ProfileID_DateStamp_AgentID_SequenceNumber.FileExtension.gz
```

The JSON document contained within an object follow this naming convention:

```
LogType_AN_ProfileID_DateStamp_AgentID_SequenceNumber.FileExtension
```

Sample file name (JSON log format):

```
adn_0001_123_20190111_50550000F98AB95B_1.json
```

The above file naming variables are described below.

Variable	Description
Log Type	Represents the type of log data. <ul style="list-style-type: none">• RTLD CDN: Identifies the delivery platform for which CDN activity was logged. Valid values are:<ul style="list-style-type: none">▪ wpc: HTTP Large platform▪ wac: HTTP Small platform▪ adn: Application Delivery Network platform• RTLD Rate Limiting: This variable is always set to "rl."• RTLD WAF: This variable is always set to "waf."
AN	Represents your CDN account number (e.g., 0001). This account number may be viewed from the upper-right hand corner of the MCC.

Variable	Description
ProfileID	<p>Represents the system-defined ID for your Real-Time Log Delivery configuration.</p> <hr/> <p>Note: You cannot currently view the system-defined ID assigned to your Real-Time Log Delivery configuration from within the MCC.</p> <hr/>
DateStamp	<p>Represents the date on which the log file was generated.</p> <p>Syntax: YYYYMMDD</p> <p>Example: 20220516</p>
AgentID	<p>Represents a unique ID that identifies the Real-Time Log Delivery software agent that generated the log file.</p>
SequenceNumber	<p>Represents a sequential number that identifies the order in which the log file was generated by the software agent identified above.</p> <hr/> <p>Important: Each software agent assigns a sequential number to the log files that it generates. A gap between log files generated on the same day by the same software agent indicates missing log data. For more information, please refer to the Verifying Log Data section.</p> <hr/> <p>Key information:</p> <ul style="list-style-type: none"> • This number starts at 0. • This number resets to 0 at the start of a new day (UTC).
FileExtension	<p>Represents the file extension for the log file. This file extension varies by log format.</p> <ul style="list-style-type: none"> • JSON Log Format: json • JSON Array Log Format: json_array • JSON Lines Log Format: json_lines