

Logging web ACL traffic information

[PDF \(waf-dg.pdf#logging\)](#)

[Kindle \(https://web.archive.org/web/20201111183928mp_/https://www.amazon.com/dp/B07641Q364\)](https://web.archive.org/web/20201111183928mp_/https://www.amazon.com/dp/B07641Q364)

[RSS \(aws-waf-doc-history.rss\)](#)

You can enable logging to get detailed information about traffic that is analyzed by your web ACL. Information that is contained in the logs includes the time that AWS WAF received the request from your AWS resource, detailed information about the request, and the action for the rule that each request matched.

You send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, AWS WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose.

For information about how to create an Amazon Kinesis Data Firehose and review your stored logs, see [What Is Amazon Kinesis Data Firehose?](#)

[\(https://web.archive.org/web/20201111183928/https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html\)](https://web.archive.org/web/20201111183928/https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html) To understand the permissions required for your Kinesis Data Firehose configuration, see [Controlling Access with Amazon Kinesis Data Firehose](#)

[\(https://web.archive.org/web/20201111183928/https://docs.aws.amazon.com/firehose/latest/dev/controlling-access.html\)](https://web.archive.org/web/20201111183928/https://docs.aws.amazon.com/firehose/latest/dev/controlling-access.html) .

You must have the following permissions to successfully enable logging:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

For more information about service-linked roles and the `iam:CreateServiceLinkedRole` permission, see [Using service-linked roles for AWS WAF](#)

[\(https://web.archive.org/web/20201111183928mp_/https://docs.aws.amazon.com/docs.aws.amazon.com/waf/latest/developerguide/service-linked-roles.html\)](https://web.archive.org/web/20201111183928mp_/https://docs.aws.amazon.com/docs.aws.amazon.com/waf/latest/developerguide/service-linked-roles.html) .

Managing logging for a web ACL

You can enable and disable logging for a web ACL at any time.

To enable logging for a web ACL

1. Create an Amazon Kinesis Data Firehose using a name starting with the prefix `aws-waf-logs-`. For example, `aws-waf-logs-us-east-2-analytics`. Create the data firehose with a PUT source and in the region that you are operating. If you are capturing logs for Amazon CloudFront, create the firehose in US East (N. Virginia). For more information, see [Creating an Amazon Kinesis Data Firehose Delivery Stream](#)
 [\(https://web.archive.org/web/20201111183928/https://docs.aws.amazon.com/firehose/latest/dev/basic-create.html\)](https://web.archive.org/web/20201111183928/https://docs.aws.amazon.com/firehose/latest/dev/basic-create.html) .

Important

Do not choose Kinesis stream as your source.

One AWS WAF log is equivalent to one Kinesis Data Firehose record. If you typically receive 10,000 requests per second and you enable full logs, you should have a 10,000 records per second setting in Kinesis Data Firehose. If you don't configure Kinesis Data Firehose correctly, AWS WAF won't record all logs. For more information, see

Amazon Kinesis Data Firehose Quotas

(<https://web.archive.org/web/20201111183928/https://docs.aws.amazon.com/firehose/latest/dev/limits.html>) .

2. Sign in to the AWS Management Console and open the AWS WAF console at <https://console.aws.amazon.com/wafv2/> (<https://web.archive.org/web/20201111183928/https://console.aws.amazon.com/wafv2/>) .
3. In the navigation pane, choose **Web ACLs**.
4. Choose the web ACL that you want to enable logging for.
5. On the **Logging** tab, choose **Enable logging**.
6. Choose the Kinesis Data Firehose that you created in the first step. You must choose a firehose that begins with `aws-waf-logs-`.
7. (Optional) If you don't want certain fields and their values included in the logs, redact those fields. Choose the field to redact, and then choose **Add**. Repeat as necessary to redact additional fields. The redacted fields appear as XXX in the logs. For example, if you redact the **URI** field, the **URI** field in the logs will be XXX.
8. Choose **Enable logging**.

Note

When you successfully enable logging, AWS WAF will create a service linked role with the necessary permissions to write logs to the Amazon Kinesis Data Firehose. For more information, see [Using service-linked roles for AWS WAF](#)

(https://web.archive.org/web/20201111183928mp_/https://docs.aws.amazon.com/docs.aws.amazon.com/waf/latest/developing/service-linked-roles.html) .

To disable logging for a web ACL

1. In the navigation pane, choose **Web ACLs**.
2. Choose the web ACL that you want to disable logging for.
3. On the **Logging** tab, choose **Disable logging**.
4. In the dialog box, choose **Disable logging**.

Log Fields

The following list describes the possible log fields.

timestamp

The timestamp in milliseconds.

formatVersion

The format version for the log.

webaclId

The GUID of the web ACL.

terminatingRuleId

The ID of the rule that terminated the request. If nothing terminates the request, the value is `Default_Action`.

terminatingRuleType

The type of rule that terminated the request. Possible values: `RATE_BASED`, `REGULAR`, `GROUP`, and `MANAGED_RULE_GROUP`.

action

The action. Possible values for a terminating rule: `ALLOW` and `BLOCK`. `COUNT` is not a valid value for a terminating rule.

terminatingRuleMatchDetails

Detailed information about the terminating rule that matched the request. A terminating rule has an action that ends the inspection process against a web request. Possible actions for a terminating rule are `ALLOW` and `BLOCK`. This is only populated for SQL injection and cross-site scripting (XSS) match rule statements. As with all rule statements that inspect for more than one thing, AWS WAF applies the action on the first match and stops inspecting the web request. A web request with a terminating action could contain other threats, in addition to the one reported in the log.

httpSourceName

The source of the request. Possible values: `CF` for Amazon CloudFront, `APIGW` for Amazon API Gateway, `ALB` for Application Load Balancer, and `APPSYNC` for AWS AppSync.

httpSourceId

The source ID. This field shows the ID of the associated resource.

ruleGroupList

The list of rule groups that acted on this request. In the preceding code example, there is only one.

ruleGroupId

The ID of the rule group. If the rule blocked the request, the ID for `ruleGroupId` is the same as the ID for `terminatingRuleId`.

terminatingRule

The rule within the rule group that terminated the request. If this is a non-null value, it also contains a **ruleId** and **action**. In this case, the action is always `BLOCK`.

nonTerminatingMatchingRules

The list of non-terminating rules in the rule group that match the request. These are always `COUNT` rules (non-terminating rules that match).

action (nonTerminatingMatchingRules group)

This is always `COUNT` (non-terminating rules that match).

ruleId (nonTerminatingMatchingRules group)

The ID of the rule within the rule group that matches the request and was non-terminating. That is, `COUNT` rules.

ruleMatchDetails (nonTerminatingMatchingRules group)

Detailed information about the rule that matched the request. This field is only populated for SQL injection and cross-site scripting (XSS) match rule statements.

excludedRules

The list of rules in the rule group that you have excluded. The action for these rules is set to `COUNT`.

exclusionType (excludedRules group)

A type that indicates that the excluded rule has the action COUNT.

ruleId (excludedRules group)

The ID of the rule within the rule group that is excluded.

rateBasedRuleList

The list of rate-based rules that acted on the request.

rateBasedRuleId

The ID of the rate-based rule that acted on the request. If this has terminated the request, the ID for `rateBasedRuleId` is the same as the ID for `terminatingRuleId`.

limitKey

The field that AWS WAF uses to determine if requests are likely arriving from a single source and thus subject to rate monitoring. Possible value: IP.

maxRateAllowed

The maximum number of requests, which have an identical value in the field that is specified by `limitKey`, allowed in a five-minute period. If the number of requests exceeds the `maxRateAllowed` and the other predicates specified in the rule are also met, AWS WAF triggers the action that is specified for this rule.

httpRequest

The metadata about the request.

clientIp

The IP address of the client sending the request.

country

The source country of the request. If AWS WAF is unable to determine the country of origin, it sets this field to `-`.

headers

The list of headers.

uri

The URI of the request. The preceding code example demonstrates what the value would be if this field had been redacted.

args

The query string.

httpVersion

The HTTP version.

httpMethod

The HTTP method in the request.

requestId

The ID of the request, which is generated by the underlying host service. For Application Load Balancer, this is the trace ID. For all others, this is the request ID.

limitKey

Indicates the IP address source that AWS WAF should use to aggregate requests for rate limiting by a rate-based rule. Possible values are IP, for web request origin, and `FORWARDED_IP`, for an IP forwarded in a header

in the request.

limitValue

The IP address used by a rate-based rule to aggregate requests for rate limiting. If a request contains an IP address that isn't valid, the limitvalue is INVALID.

Log Examples

Example log output for a rule that triggered on SQLi detection (terminating)

```
{
  "timestamp": 1576280412771,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:ap-southeast-2:EXAMPLE12345:regional/webacl/STMTTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
  "terminatingRuleId": "STMTest_SQLi_XSS",
  "terminatingRuleType": "REGULAR",
  "action": "BLOCK",
  "terminatingRuleMatchDetails": [
    {
      "conditionType": "SQL_INJECTION",
      "location": "HEADER",
      "matchedData": [
        "10",
        "AND",
        "1"
      ]
    }
  ],
  "httpSourceName": "-",
  "httpSourceId": "-",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "httpRequest": {
    "clientIp": "1.1.1.1",
    "country": "AU",
    "headers": [
      {
        "name": "Host",
        "value": "localhost:1989"
      },
      {
        "name": "User-Agent",
        "value": "curl/7.61.1"
      },
      {
        "name": "Accept",
        "value": "*/*"
      }
    ]
  }
}
```

```

        {
            "name": "x-stm-test",
            "value": "10 AND 1=1"
        }
    ],
    "uri": "/foo",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "rid"
}
}

```

Example log output for a rule that triggered on SQLi detection (non-terminating)

```

{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-world/5933d6d9-9dde-
js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
        [{
            "conditionType":"SQL_INJECTION"
            ,"location":"HEADER"
            ,"matchedData":[
                "10"
                ,"and"
                ,"1"]
            }]
        }]
    },
    "httpRequest":{
        "clientId":"3.3.3.3"
        ,"country":"US"
        ,"headers":[
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/.*"}
        ]
    }
}

```

```

    ,{"name":"foo","value":"10 AND 1=1"}
  ]
  , "uri":"/foo","args":""
  , "httpVersion":"HTTP/1.1"
  , "httpMethod":"GET"
  , "requestId":"rid"
}
}

```

Example log output for multiple rules that triggered inside a rule group (RuleA-XSS is terminating and Rule-B is non-terminating)

```

{
  "timestamp":1592361810888,
  "formatVersion":1,
  "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-world/5933d6d9-9dde-
js82-v8aw-9ck28nv9"
  , "terminatingRuleId":"RG-Reference"
  , "terminatingRuleType":"GROUP"
  , "action":"BLOCK",
  "terminatingRuleMatchDetails":
  [{
    "conditionType":"XSS"
    , "location":"HEADER"
    , "matchedData":["<","frameset"]
  }]
  , "httpSourceName":"-"
  , "httpSourceId":"-"
  , "ruleGroupList":
  [{
    "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c051b698-1f11-4m41-aef4-99a506d53f4b"
    , "terminatingRule":{
      "ruleId":"RuleA-XSS"
      , "action":"BLOCK"
      , "ruleMatchDetails":null
    }
    , "nonTerminatingMatchingRules":
    [{
      "ruleId":"RuleB-SQLi"
      , "action":"COUNT"
      , "ruleMatchDetails":
      [{
        "conditionType":"SQL_INJECTION"
        , "location":"HEADER"
        , "matchedData":[
          "10"
          , "and"
          , "1"]
      ]
    }
  ]
}

```

```

        }}
    ]}
    , "excludedRules": null
}]
, "rateBasedRuleList": []
, "nonTerminatingMatchingRules": []
, "httpRequest": {
    "clientId": "3.3.3.3"
    , "country": "US"
    , "headers":
    [
        {"name": "Host", "value": "localhost:1989"}
        , {"name": "User-Agent", "value": "curl/7.61.1"}
        , {"name": "Accept", "value": "*/*"}
        , {"name": "xssfoo", "value": "<frameset onload=alert(1)>"}
        , {"name": "bar", "value": "10 AND 1=1"}
    ]
    , "uri": "/foo"
    , "args": ""
    , "httpVersion": "HTTP/1.1"
    , "httpMethod": "GET"
    , "requestId": "rid"
}
}

```

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.