ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

Log Management

Document Version: 20201021

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Log service

1.1. Overview

WAF integrates Log Service to provide the Log Service of WAF feature.

The feature collects and stores website access logs and attack protection logs in real time.It leverages the capabilities of Log Service, allows you to query and analyze log data, generate reports, and configure alerts, and delivers log data to downstream services for consumption. This way, Log Service for WAF provides an easy approach to log query and search and allows you to focus more on log analysis.

Limits

The following table describes support for Log Service for WAF and limits on log storage durations.

WAF edition	Support for Log Service for WAF	Log storage duration	Support for modification of log storage duration
Pro edition (subscription)	×	None.	×
Business edition (subscription)	√	180 days or 360 days. The duration is determined based on the configurations you specify when you enable Log Service for WAF.	√
Enterprise edition (subscription)	√	180 days or 360 days. The duration is determined based on the configurations you specify when you enable Log Service for WAF.	√

Benefits

Log Service for WAF offers the following benefits:

- Compliance audits: This feature allows you to store website access logs for more than six months to meet classified protection requirements.
- Flexible configuration: Website access logs and attack protection logs can be collected in real time with simple configuration. You can customize the log storage duration and capacity and select a website for log collection as required. You can also modify an existing report template or customize a report template to meet your business or security requirements.
- Real-time log analysis: WAF provides the real-time log analysis feature and an out-of-the-box (OOTB) report center, and supports data interaction and mining. This allows you to identify and analyze various attacks on your website and access details in seconds.

- Real-time alerting: You can customize real-time monitoring and alert rules based on specific metrics to respond to exceptions that occur in critical services in a timely manner.
- Collaboration: This feature collaborates with other data solutions such as real-time computing, cloud storage, and visualization to further explore the value of data.

Intended users

- Large-scale enterprises and organizations, such as financial entities and government agencies that need to comply with log storage requirements. The logs include host, network, and security logs for various assets in the cloud.
- Organizations, such as large-scale real-estate, e-commerce, financial entities, and government agencies that have security operations centers (SOCs) and require centralized collection and management of security and alert logs.
- Enterprises with advanced technologies, such as companies in the IT, gaming, or financial industry, which require in-depth analysis on logs collected from various assets in the cloud and automated alert handling.
- All users who need to trace business security events and generate weekly, monthly, and yearly reports, or users who need to meet classified protection requirements (level 3 or higher).

Features

After you enable Log Service for WAF, which is based on powerful features of Alibaba Cloud Log Service, you can analyze website access logs and attack protection logs. You can also display data on visual dashboards and use preset thresholds to configure monitoring and alert rules.

Feature	Description
Query and analysis	You can enter a query and analysis statement to query and analyze collected log data in real time. The query and analysis statement consists of a search clause and an analytics clause, which are separated with a vertical bar (`|`). For example, you can use the following statement to query the number of visits to a domain: `* | select time_series(__time__,'15m','%H:%i','0') as time,COUNT_if(block_action='waf') as "wafmodule",COUNT_if(block_action='acl') as "aclmodule",COUNT_if(block_action='tmd') as "httpfloodmodule" GROUP by time order by time` For more information about query and analysis statements, see Common query statements.
Analysis charts	A query and analysis statement contains the syntax for analytics. After the statement is executed, analysis results are displayed in tables by default. You can also choose a line chart, column chart, or pie chart to display the results.

Feature	Description
Dashboards	Log Service for WAF provides dashboards for real-time data analysis. You can save analysis charts to the dashboards. You can also subscribe to dashboards and sends dashboard data to specific recipients by using emails or DingTalk messages.
Monitoring and alerting	You can configure alert rules based on the charts in a dashboard to monitor the service status in real time.

Usage notes

All log data of WAF is stored in a dedicated Logstore. Take note of the following points on the Logstore:

- You cannot write data into the dedicated Logstore by using API operations or SDKs.

  Note The dedicated Logstore has no limits on queries, statistics, alerts, and streaming consumption.

- The dedicated Logstore is not billed. However, it runs normally on the condition that Log Service does not have overdue payments.
- The built-in charts of the dedicated Logstore may be updated.

Scenarios

- Trace web attack logs and locate the source of security threats.
- Monitor web requests in real time and view traffic trends.
- Obtain information about the efficiency of security operations and respond to issues in a timely manner.
- Generate and deliver security network logs to user-created data and computing centers.

Common query statements

- Query request blocking types.

```
* | select count(*) as times,host,block_action group by host,block_action order by times desc
```

- Query the number of queries per second.

```
* | select time_series(__time__,'15m','%H:%i','0') as time,count(*)/900 as QPS group by time order by time
```

- Query attacked domains.

```
* and acl_blocks:1 | select count(*) as times,host group by host order by times desc
```

- Query attacked URLs.

```
* and acl_blocks:1 | select count(*)as times,host,request_path group by host,request_path order by times
```

- Query request details.

```
* | select date_format(date_trunc('second',__time__),'%H:%i:%s') as time,host,request_path,request_method,status,upstream_status,querystring limit 10
```

- Query web attack types.

```
* | SELECT web_attack_type,times,concat(try_cast(round((times*100.0/sum(times) over()),2)as varchar),'%') as pre from (SELECT COUNT(*) as times,web_attack_type
 from log GROUP by host) ORDER by times desc limit 10
```

1.2. Billing methods

This topic describes the billing methods of Log Service for WAF. Log Service for WAF is billed based on the storage capacity and storage duration.

Overview

Log Service for WAF is available for subscription WAF instances of the Pro or higher edition.

On the WAF buy page, you can set **Access Log Service** to YES. Then, specify **Log Storage Period** and **Log Storage Size**. The price is automatically calculated based on the specifications you choose. For more information about how to enable Log Service for WAF, see Enable Log Service for WAF for a subscription WAF instance. For the prices of Log Service for WAF at different specifications, see Log storage specifications.

Log storage specifications

The following table lists the prices of Log Service for WAF at different log storage specifications.

Log storage duration	Storage capacity	Recommended scenario	Instance outside mainland China		Instance in mainland China	
			Monthly subscription (USD)	Yearly subscription (USD)	Monthly subscription (USD)	Yearly subscription (USD)
	3TB	Average daily QPS is up to 80.	USD 450	USD 5,400	USD 225	USD 2,700
	5TB	Average daily QPS is up to 120.	USD 750	USD 9,000	USD 375	USD 4,500
	10TB	Average daily QPS is up to 260.	USD 1,500	USD 18,000	USD 750	USD 9,000
	20TB	Average daily QPS is up to 500.	USD 3,000	USD 36,000	USD 1,500	USD 18,000

180 days Log storage duration	Storage capacity	Recommended scenario	Instance outside mainland China		Instance in mainland China	
			Monthly subscription (USD)	Yearly subscription (USD)	Monthly subscription (USD)	Yearly subscription (USD)
	50TB	Average daily QPS is up to 1,200.	USD 7,500	USD 90,000	USD 3,000	USD 36,000
	100TB	Average daily QPS is up to 2,600.	USD 15,000	USD 180,000	USD 7,500	USD 90,000
360 days	5TB	Average daily QPS is up to 60.	USD 750	USD 9,000	USD 375	USD 4,500
	10TB	Average daily QPS is up to 120.	USD 1,500	USD 18,000	USD 750	USD 9,000
	20TB	Average daily QPS is up to 260.	USD 3,000	USD 36,000	USD 1,500	USD 18,000
	50TB	Average daily QPS is up to 600.	USD 7,500	USD 90,000	USD 3,000	USD 36,000
	100TB	Average daily QPS is up to 1,200.	USD 15,000	USD 180,000	USD 7,500	USD 90,000

Upgrade of storage capacity

If the log storage capacity that you purchase is exhausted, the system automatically sends you a notification. You can increase the capacity at any time by upgrading the log storage capacity specifications.

> **Notice** If you do not upgrade the log storage capacity, WAF stops writing new log data to the Logstore in Log Service. Existing log data in the Logstore is retained and is not automatically deleted until the storage period is exceeded. If Log Service for WAF expires and is not renewed within seven days, all log data in the Logstore is automatically deleted.

Subscription duration

The subscription duration of Log Service for WAF depends on that of the WAF instance.

- **New purchase**: If you purchase a subscription WAF instance, the price of Log Service for WAF is calculated based on the subscription duration of the WAF instance.
- **Upgrade**: If you enable Log Service for WAF by upgrading the existing subscription WAF instance, the price of Log Service for WAF is calculated based on the remaining validity of the existing WAF instance. The remaining validity is accurate to minutes.

Service expiration

If your WAF instance expires, Log Service for WAF also expires.

- After Log Service for WAF expires, WAF stops writing log data to the Logstore.
- Log data is retained for seven days after Log Service for WAF expires. If you renew Log Service for WAF within seven days, you can continue to use this feature. Otherwise, all log data is deleted.

1.3. Enable Log Service for WAF

WAF integrates Log Service to provide the Log Service for WAF feature. This feature collects logs of websites protected by WAF in a near-real-time manner, allows you to query and analyze the collected log data, and displays results on dashboards. This feature meets the classified protection requirements and your website protection and operations requirements. This topic describes how to enable the Log Service for WAF feature.

Prerequisites

- A WAF instance is purchased. If it is a subscription WAF instance, its edition must be **Business** or higher. For more information, see Purchase a WAF instance.
- Log Service is activated.

  The first time you log on to the Log Service console, activate Log Service as prompted.

Enable Log Service for WAF for a subscription WAF instance

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Log Service** .
4. On the **Log Service** page, click **Upgrade**.

   > **Note** If the Log Service for WAF feature is enabled, the **Upgrade** button is not displayed.

5. On the Upgrade/Downgrade page, set **Access Log Service** to YES. Then, specify **Log Storage Period** and **Log Storage Size** based on your business requirements.
6. Click **Buy Now** and complete the payment.
7. (Optional)Authorize WAF to access Log Service.If this is the first time you enable Log Service for WAF, you must authorize WAF to access Log Service. If you have already completed the authorization, skip this step.

   To authorize WAF to access Log Service, perform the following operations:

   i. On the **Log Service** page, click **Authorize Now**.

   > **Note** If you have already completed the authorization, **Authorize Now** is not displayed.

   ii. On the **Cloud Resource Access Authorization** page, click **Confirm Authorization Policy**.

   

What to do next

After you enable the Log Service for WAF feature, you must enable log collection for domains that are protected by WAF. For more information, see Enable log collection.

1.4. Enable log collection

This topic describes how to enable the log collection feature of Web Application Firewall (WAF) for a specified domain in the WAF console. After this feature is enabled, all log data in this domain is automatically stored in the dedicated Logstore of WAF. In this way, you can analyze and query log data in real time.

Prerequisites

- WAF is activated and domains are added to WAF for protection.
- Log Service is activated.

Context

Log Service is used to collect website access logs and attack protection logs on Alibaba Cloud WAF in real time. It retrieves and analyzes log data in real time and displays the results in dashboards. You can use the collected log data to analyze the number of visits to and attacks on your websites in real time. You can also use the log data to assist security engineers to develop protection policies.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Log Service** .
4. (Optional)If you configure the log collection feature for the first time, click **Authorize** and follow the instructions on the Log Service page to authorize WAF to write all log data to your dedicated Logstore.
5. Select the target domain and turn on **Status** next to the domain.

   The log collection feature is enabled for the domain. A dedicated project and a dedicated Logstore are automatically created by Log Service under your Alibaba Cloud account. WAF automatically imports logs from the domains with the log collection feature enabled to this Logstore.

Dedicated project and Logstore

The following table describes default configurations of a dedicated project and a dedicated Logstore.

Item	Description

Item	Description
Project	A project is created by default. The project name is determined based on the region of your WAF instance. • If your WAF instance is deployed in a region in mainland China, the project name is in the following format: `waf-project-`*`Alibaba Cloud account ID`*`-cn-hangzhou`. • If your WAF instance is deployed in a region outside mainland China, the project name is in the following format: `waf-project-`*`Alibaba Cloud account ID`*`-ap-southeast-1`.
Logstore	The Logstore named `waf-logstore` is created by default. All log data collected by the WAF log collection feature is stored in this Logstore.
Region	• If your WAF instance is deployed in a region in mainland China, the project is saved in the China (Hangzhou) region by default. • If your WAF instance is deployed in a region outside mainland China, the project is saved in the Singapore region by default.
Shard	Two shards are created by default, with the automatic sharding feature enabled. For more information, see Manage shards.
Dashboard	Three dashboards are created by default: • Access Center • Operation Center • Security Center For more information, see Enable log analysis.

Limits and instructions

- Only log data of WAF can be written into this Logstore.

  Log data of WAF is stored in this Logstore. Other data cannot be written into this Logstore, whether by calling API operations or using SDKs.

  > Note The Logstore has no limits on features such as queries, statistics, alerts, and streaming consumption.

- The Logstore is not billed.

  To use the Logstore, you must activate Log Service for your Alibaba Cloud account.

  > Note When your Log Service is overdue, the log collection feature of WAF is suspended until you pay the overdue bills.

- Do not delete or modify configurations of the default project, Logstore, index, and dashboards created in Log Service. Log Service automatically updates data from the log query and

analysis function of WAF, the index of the Logstore, and the default reports.

- A RAM user can use the log query and analysis service of WAF only after the Log Service permissions are granted to the RAM user. For more information, see Grant log query and analysis permissions to a RAM user.

1.5. Enable log query

This topic describes how to enable log query. The log query and log analysis features provided by Log Service are integrated in Web Application Firewall (WAF). You can query and analyze logs on the Log Service page of the WAF console. After you enable the WAF log collection feature for a specified domain, you can query and analyze collected log entries in real time, view or edit dashboard data, and set monitoring and alert rules on the Log Service page in the WAF console.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Log Service** .
4. On the Log Service page that appears, select a domain and ensure that **Status** next to the domain is turned on.
5. Click the **Log Query** tab. This tab is integrated with the log query and analysis page in the Log Service console. A query statement is automatically entered. For example, `matched_host: "<yourDomainName>"` is automatically entered. This statement is used to query all log entries about the domain that you select.

   

6. Enter a query and analysis statement, select a time range, and click **Search & Analyze**.

More operations on the Log Query tab

On the Log Query tab, you can perform the following operations on log entries:

- Customize query and analysis

  Log Service supports a wide range of query and analysis statements that can be used in complex scenarios. For more information, see Query and analyze log entries by using statements.

- View the distribution of log entries within a specified time range

  The column chart below the search bar shows the distribution of log entries that are filtered by a time range and query statements. The horizontal axis indicates the time range, and the vertical axis indicates the number of log entries. The total number of the log entries is displayed below the chart.

  > **Note** You can drag a column in the column chart to narrow down the time range. The time picker automatically changes the time range, and the corresponding query results are updated.

- View raw logs

On the **Raw Logs** tab, the details of each log entry are displayed in a separate section. The details include the time when the log was collected, the content, and other fields. Click **Display Content Column** to set the display mode to **Full Line** or **New Line** for long strings in the Content column. Click **Column Settings** to select the columns you want to view. Click the download icon to download the query results.

- View analysis charts

  Log analysis results are displayed in charts. You can select various types of charts on the **Graph** tab. For more information, see Overview.

  

- Perform quick analysis

  On the **Raw Logs** tab, view the distribution of a log field within a specified time range with one click. This helps reduce the time needed to query key data. For more information, see Quick analysis.

  

Query and analyze log entries by using statements

A query and analysis statement consists of a search clause and an analytics clause that are separated with a vertical bar (`|`).

```
$Search | $Analytics
```

Clause	Description
Search	Specifies the keyword, fuzzy string, numeric value, range, or a combination of these items as the query condition. If the statement is empty or only contains an asterisk (`*`) wildcard, all log entries are queried.
Analytics	Calculates and analyzes the query results or all log entries.

> **Note** Both the search and analytics clauses are optional.
>
> - If the search clause is empty, all log entries within a specified time range are queried and analyzed.
> - If the analytics clause is empty, the query results are returned without analysis.

Query syntax

The query syntax of Log Service supports full text query and field-based query. Statements in the search bar can be displayed in multiple lines and highlighted.

- Full text query

  When you enter keywords, you do not have to specify fields for log entry queries. If you want to query the log entries that contain the entire keyword, you can enter a keyword in a pair of double quotation marks ("). If you enter more than one keyword, separate them with spaces or `and` .

Examples

- Query log entries based on multiple keywords

  You can execute one of the following statements to query all the log entries that contain `www.aliyun.com` and `error`:

  `www.aliyun.com error` and `www.aliyun.com and error`

- Query log entries based on query conditions

  You can execute the following statement to query the log entries that contain `www.aliyun.com` and `error` or `404`:

  ```
  www.aliyun.com and (error or 404)
  ```

- Query log entries based on a prefix

  You can execute the following statement to query the log entries that contain `www.aliyun.com` and start with `failed_`:

  ```
  www.aliyun.com and failed_*
  ```

  > **Note** The asterisk (`*`) wildcard can only be added as a suffix and cannot be added as a prefix. For example, the statement cannot be `*_error`.

- Field-based query

  You can query log entries based on fields.

  You can specify a numeric field and value in the format of `Field name: Value` or `Field name >= Value`. You can also use the `and` and `or` operators to specify a combination of fields or use field-based query together with full text query.

  > **Note** The log entries that record access, operations, and attacks on a specific domain in Log Service for WAF can also be queried by field. For information about the definition, type, and format of each field, see Log fields.

  Examples

- Query log entries based on multiple fields

  You can execute the following statement to query the log entries that record HTTP flood attacks blocked by WAF on the `www.aliyun.com` domain:

  ```
  matched_host: www.aliyun.com and cc_blocks: 1
  ```

  You can execute the following statement to query all the log entries that record access, with a 404 error reported, from a specified client whose IP address is `1.2.3.4` to the `www.aliyun.com` domain:

  ```
  real_client_ip: 1.2.3.4 and matched_host: www.aliyun.com and status: 404
  ```

  > **Note** In this example, the `matched_host`, `cc_blocks`, `real_client_ip`, and `status` fields are the fields defined in a WAF log.

- Query log entries based on numeric fields

  You can execute the following statement to query the log entries that record slow requests whose response time exceeds 5 seconds:

  ```
  request_time_msec > 5000
  ```

  You can also query log entries based on a time range. For example, you can execute the following statement to query the log entries that record the requests whose response time exceeds 5 seconds but does not exceed 10 seconds:

  ```
  request_time_msec in (5000 10000]
  ```

  > **Note** You can execute the following statement to obtain the same query results: `request_time_msec > 5000 and request_time_msec <= 10000`.

- Check the field availability status

  You can determine whether a field is available in log entries by executing the following statements:

  - Query the log entries that contain the `ua_browser` field.

    ```
    ua_browser: *
    ```

  - Query the log entries that do not contain the `ua_browser` field.

    ```
    not ua_browser: *
    ```

For more information about the query statements supported by Log Service, see Overview.

Analytics syntax

You can use SQL-92 statements to analyze log entries.

For more information about the statement syntax and functions supported by Log Service, see Real-time analysis.

> Note
>
> - You can omit the `from Table name` part (that is, `from log`) in standard SQL statements.
> - By default, the first 100 log entries are returned. You can modify the number by using the LIMIT syntax.

Query and analysis examples

Time-based log query and analysis

Each log entry has a `time` field, which indicates the time the log entry was generated. The time is in the format of `yyyy-MM-ddTHH:mm:ss+Time zone`. For example, in `2018-05-31T20:11:58+08:00`, the time zone is `UTC+8`.

Each log entry has a built-in field `__time__`. This field also indicates the time the log entry was generated. The time is in the format of a UNIX timestamp. The value is used in the time-based calculation. The value of this field indicates the number of seconds that have elapsed since the UTC time 00:00:00, January 1, 1970. If you want to obtain a recognizable calculation result, you must convert the format first.

- **Select and display the time**

  You can use the `time` field to display time information in logs. For example, search for the last 10 log entries that record the HTTP flood attacks on the `www.aliyun.com` domain. The attacks are blocked by WAF in a specific time period. The data about the time, real_client_ip, and http_user_agent fields is displayed.

```
matched_host: www.aliyun.com and cc_blocks: 1
| select time, real_client_ip, http_user_agent
   order by time desc
   limit 10
```

- **Calculate the time**

  You can use the `__time__` field to calculate the time. For example, calculate the number of days that have elapsed since the domain suffered an HTTP flood attack.

```
matched_host: www.aliyun.com  and cc_blocks: 1
| select time, round((to_unixtime(now()) - __time__)/86400, 1) as "days_passed", real_client_ip, http_
user_agent
    order by time desc
    limit 10
```

In this example, `round((to_unixtime(now()) - __time__)/86400, 1)` is used to calculate the number of days that have elapsed since the domain suffered an HTTP flood attack. First, use `now()` to obtain the current time and convert the current time into a Unix timestamp by using `to_unixtime`. Then, subtract the value of the built-in field `__time__` from the converted time to obtain the number of seconds that have elapsed. Finally, divide this number of seconds by `86400` (the total number of seconds in a day) and apply the `round(data, 1)` function to keep one decimal place. The result is the number of days that have elapsed since each attack log entry was generated.

- **Perform statistical analysis in groups based on the time**

  You can query the log entries about the trend of HTTP flood attacks on a specific domain within a specified time period.

```
matched_host: www.aliyun.com and cc_blocks: 1
| select date_trunc('day', __time__) as dt, count(1) as PV
    group by dt
    order by dt
```

  In this example, the built-in field `__time__` is used by the `date_trunc('day', ..)` function to align the time of the entries by day. Each log entry is grouped based on the day when the log entry was generated. The total number of log entries in each group is counted by using count(1). Then, these entries are ordered by the group. You can use other values for the first parameter of the `date_trunc` function to group the log entries based on other time units, such as `second`, `minute`, `hour`, `week`, `month`, and `year`. For more information about this function, see Date and time functions.

  We recommend that you display the results in a line chart.

- **Group log entries by a custom time period**

  If you want to use more flexible groupings to analyze log entries based on time, complex calculations are required. For example, you can query the log entries about the trend of HTTP flood attacks on a specified domain within every five minutes.

```
matched_host: www.aliyun.com and cc_blocks: 1
| select from_unixtime(__time__ - __time__% 300) as dt,
      count(1) as PV
    group by dt
    order by dt
    limit 1000
```

  In this example, the built-in field is used to align the time by using the formula `__time__ - __time__% 300`, and the `from_unixtime` function is used to convert the format of the result. Then, each log entry is assigned to a group that indicates a time period of five minutes (300 seconds), and the total number of log entries in each group is counted by using count(1). Finally, the query results are ordered by time range and the first 1,000 result entries are returned, which include the log entries that were generated within the first 83 hours of the specified time period.

We recommend that you display the results in a line chart.

The `date_parse` and `date_format` functions convert the time format. For more information about the functions that can be used to parse the time, see Date and time functions.

Client IP address-based log query and analysis

A WAF log contains the field `real_client_ip`, which reflects the real client IP address. In scenarios where your website is accessed by using a proxy server or the IP address in a request header is incorrect, you cannot obtain the real IP address of the user. However, the `remote_addr` field forms a direct connection to the client, which can be used to obtain the real IP address.

- **Classify attackers by country**

  You can query the log entries about the distribution of HTTP flood attacks by country.

  ```
  matched_host: www.aliyun.com and cc_blocks: 1
  | SELECT ip_to_country(if(real_client_ip='-', remote_addr, real_client_ip)) as country,
        count(1) as "number of attacks"
        group by country
  ```

  In this example, the function `if(condition, option1, option2)` returns the real client IP address. If `real_client_ip` is `-`, the function returns the value of `remote_addr`. Otherwise, the function returns the value of `real_client_ip`. Then, the `ip_to_country` function is used to obtain the country information from the client IP address.

  We recommend that you display the results on a world map.

- **Classify visitors by province**

  To further obtain the distribution of visitors by province, you can use the `ip_to_province` function to obtain the province information from IP addresses.

  ```
  matched_host: www.aliyun.com and cc_blocks: 1
  | SELECT ip_to_province(if(real_client_ip='-', remote_addr, real_client_ip)) as province,
        count(1) as "number of attacks"
        group by province
  ```

  In this example, the `ip_to_province` function is used to obtain the country information from the real IP address of a client. If the IP address is in a region outside mainland China, the function can be used to attempt to obtain the specific state information. If you choose to display the results with a map of China, IP addresses that are in regions outside mainland China are not displayed.

  We recommend that you display the results with a map of China.

- **Classify attackers on a heat map**

  You can use the `ip_to_geo` function to obtain the geographic information (the latitude and the longitude) from the real IP addresses of clients. This information can be used to generate a heat map to indicate the density of attacks.

```
matched_host: www.aliyun.com  and cc_blocks: 1
| SELECT ip_to_geo(if(real_client_ip='-', remote_addr, real_client_ip)) as geo,
      count(1) as "number of attacks"
      group by geo
      limit 10000
```

In this example, the `ip_to_geo` function is used to obtain the latitude and the longitude from the real IP addresses of clients. The first 10,000 result entries are returned.

Select AMAP and click **Show Heat Map**.

For more information about IP-based functions, see IP functions. For example, you can use the `ip_to_provider` function to obtain the provider information of an IP address. You can use the `ip_to_domain` function to determine whether an IP address is public or private.

1.6. Enable log analysis

This topic describes how to enable log analysis in the WAF console. The Log Analysis tab on the Log Service page in the WAF console displays the data of default dashboards in the Log Service console. If you want to query website and security data, you can modify the time range or add query conditions.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Log Service** .
4. On the Log Service page that appears, select a domain and ensure that **Status** next to the domain is turned on.
5. Click the **Log Analysis** tab. The dashboard page in the Log Service console is integrated into this tab. The system automatically specifies **Filter**, such as `matched_host:<yourDomainName>` , to display all the log data that is recorded from your domain.

   After you enable the log collection feature of WAF, the following default dashboards are automatically created on the Log Service page: Operation Center, Access Center, and Security Center.

Dashboard	Description
Operation Center	Displays operation details such as the valid request rate and the statistics of attacks and peaks of inbound and outbound traffic. It also displays the number of received requests, operations trends, and attack overview.
Access Center	Displays basic access details such as the number of page views (PVs) and the number of unique visitors (UVs), the access trend, and the distribution of visitors by source.

Dashboard	Description
Security Center	Displays basic metric information of attacks, attack types, attack trend, and attacker distribution.

For more information, see Description of default dashboards.

Dashboards display various reports by using the predefined layout. The following table describes the supported chart types.

Chart type	Description
Individual value plot	Displays important metrics, such as the valid request rate and the peak of attacks.
Line chart or area chart	Displays the trends of important metrics within a specified period of time, such as the trend of inbound bandwidth and attack blocking.
Map	Displays the geographical distribution of visitors and attackers, such as the distribution of attacks by country and access heat map.
Pie chart	Displays data proportions, such as the distribution proportions of attacked websites and client types.
Table	Displays detailed information, such as the information of attackers.

For more information about the chart types provided by Log Service, see Overview.

Time picker

All charts are based on statistics results for different time periods. If you want all charts on the current page to display data for the same time range, you must configure the time picker.

1. On the **Log Analysis** tab, click **Please Select**.
2. In the **Time** pane, specify the time range.

You can select relative time or a time frame, or customize a time range. After you modify the time range, it takes effect in all charts.

> **Note** The time picker only provides a temporary view of charts on the current page, and the system does not save the setting. The next time you view the charts, the system displays the default time range.

To change the time range for a specific chart, move the pointer over the

icon in the upper-right corner of the chart and click **Select Time Range**.

Chart data drilldown

Data drilldown is configured for some charts. This allows you to quickly view underlying data details. Move the pointer over the

icon in the upper-right corner of a specific chart. If the

icon is displayed, data drilldown is configured for this chart.

You can click an underscored number in this chart to view underlying data details. For example, you can quickly identify the domains that are attacked and the number of attacks by clicking the number in the **Attacked Hosts** chart of the **Security Center** tab.

> **Note** Alternatively, you can switch to the **Raw Logs** tab to view the original log data.

Description of default dashboards

- **Operation Center**: displays operation details such as the valid request rate and the statistics of attacks and peaks of inbound and outbound traffic. It also displays the number of received requests, operations trends, and attack overview.

Chart name	Chart type	Default time range	Description	Example value
Valid Request Ratio	Individual value plot	Today (Time Frame)	Displays the percentage of all valid requests. A valid request is a request that is neither an attack nor a request for which the server returns the 400 error. Unit: %.	95
Valid Request Traffic Ratio	Individual value plot	Today (Time Frame)	Displays the percentage of the traffic generated by valid requests. Unit: %.	95
Peak Attack Size	Individual value plot	Today (Time Frame)	Displays the peak throughput of attacks. Unit: bit/s.	100
Attack Traffic	Individual value plot	1 Hour (Relative)	Displays the total amount of traffic that is generated by attacks. Unit: bytes.	30
Attack Count	Individual value plot	1 Hour (Relative)	The total number of attacks.	100

Chart name	Chart type	Default time range	Description	Example value
Peak Network In	Individual value plot	Today (Time Frame)	Displays the peak inbound throughput. Unit: Kbit/s.	100
Peak Network Out	Individual value plot	Today (Time Frame)	Displays the peak outbound throughput. Unit: Kbit/s.	100
Received Requests	Individual value plot	1 Hour (Relative)	Displays the total number of valid requests.	7800
Traffic Received	Individual value plot	1 Hour (Relative)	Displays the total inbound traffic that is generated by valid requests. Unit: MB.	1.4
Traffic Out	Individual value plot	1 Hour (Relative)	Displays the total outbound traffic that is generated by valid requests. Unit: MB.	3.8
Network Traffic In And Attack	Area chart	Today (Time Frame)	Displays the trends of throughput generated by valid requests and attacks. Unit: Kbit/s	-
Request And Interception	Line chart	Today (Time Frame)	Displays the trends of valid requests and the total number of requests that are blocked. Unit: count/h.	-
Access Status Distribution	Flow chart	Today (Time Frame)	Displays the trends of requests with different status codes (such as 404, 304, and 200) returned. Unit: count/h.	-
Attack Source (World)	World map	1 Hour (Relative)	Displays the distribution of attacks by country.	-
Attack Source (China)	Map of China	1 Hour (Relative)	Displays the distribution of attacks by province in China.	-
Attack Type	Pie chart	1 Hour (Relative)	Displays the distribution of attacks by attack type.	-

Chart name	Chart type	Default time range	Description	Example value
Attacked Hosts	Treemap chart	1 Hour (Relative)	Displays the websites that are attacked most.	-

- **Access Center**: displays basic access details such as the number of page views (PVs) and the number of unique visitors (UVs), the access trend, and the distribution of visitors by source.

Chart name	Chart type	Default time range	Description	Example value
PV	Individual value plot	1 Hour (Relative)	Displays the total number of PVs.	100000
UV	Individual value plot	1 Hour (Relative)	Displays the total number of UVs.	100
Traffic In	Individual value plot	1 Hour (Relative)	Displays the total inbound traffic. Unit: MB.	300
Peak Network In Traffic	Individual value plot	Today (Time Frame)	Displays the peak inbound throughput. Unit: Kbit/s.	0.5
Peak Network Out Traffic	Individual value plot	Today (Time Frame)	Displays the peak outbound throughput. Unit: Kbit/s.	1.3
Traffic Network Trend	Area chart	Today (Time Frame)	Displays the trends of inbound and outbound throughput. Unit: Kbit/s.	-
PV/UV Trends	Line chart	Today (Time Frame)	Displays the trends of PVs and UVs. Unit: count/h.	-
Access Status Distribution	Flow chart	Today (Time Frame)	Displays the trends of requests with different status codes (such as 404, 304, and 200) returned. Unit: count/h.	-
Access Source	World map	1 Hour (Relative)	Displays the distribution of requests by country.	-
Traffic In Source (World)	World map	1 Hour (Relative)	Displays the distribution (by country) of inbound traffic from requests.	-

Chart name	Chart type	Default time range	Description	Example value
Traffic In Source (China)	Map of China	1 Hour (Relative)	Displays the distribution (by province in China) of inbound traffic from requests.	-
Access Heatmap	AMAP	1 Hour (Relative)	Displays the heat map that indicates the source distribution of requests by geographical location.	-
Network Provider Source	Pie chart	1 Hour (Relative)	Displays the source distribution of requests by Internet service provider, such as China Telecom, China Unicom, China Mobile, and China Education and Research Network.	-
Referer	Table	1 Hour (Relative)	Displays the information of hosts and redirection frequency and the first 100 Referer URLs from which the hosts are most frequently redirected.	-
Mobile Client Distribution	Pie chart	1 Hour (Relative)	Displays the distribution of requests from mobile clients by client type.	-
PC Client Distribution	Pie chart	1 Hour (Relative)	Displays the distribution of requests from PC clients by client type.	-
Request Content Type Distribution	Pie chart	1 Hour (Relative)	Displays the distribution of requested resources by content type, such as HTML, form, JSON, and streaming data.	-
Accessed Sites	Treemap chart	1 Hour (Relative)	Displays the 30 domains that are accessed most.	-

Chart name	Chart type	Default time range	Description	Example value
Top Clients	Table	1 Hour (Relative)	Displays the information of the top 100 clients that visit your domains on a regular basis. The information includes the client IP address, the region and city, network information, the request method, inbound traffic, the number of incorrect accesses, and the number of attacks.	-
URL With Slowest Response	Table	1 Hour (Relative)	Displays the information of the top 100 URLs with long response time. The information includes the domain, the URL, the average response time, and the number of accesses.	-

- **Security Center**: displays basic metric information of attacks, attack types, attack trend, and attacker distribution.

Chart name	Chart type	Default time range	Description	Example value
Peak Attack Size	Individual value plot	1 Hour (Relative)	Displays the peak throughput of attacks. Unit: bit/s.	100
Attacked Hosts	Individual value plot	Today (Time Frame)	Displays the number of websites that are attacked.	3
Source Country Of Attack	Individual value plot	Today (Time Frame)	Displays the number of countries from which attacks are launched.	2
Attack Traffic	Individual value plot	1 Hour (Relative)	Displays the total amount of traffic that is generated by attacks. Unit: bytes.	1
Attacker UV	Individual value plot	1 Hour (Relative)	Displays the number of UVs.	40

Chart name	Chart type	Default time range	Description	Example value
Attack type distribution	Flow chart	Today (Time Frame)	Displays the distribution of attacks by attack type.	-
Intercepted Attack	Individual value plot	1 Hour (Relative)	Displays the total number of attacks that are blocked by WAF.	100
CC Attack Interception	Individual value plot	1 Hour (Relative)	Displays the number of HTTP flood attacks that are blocked by WAF.	10
Web Attack Interception	Individual value plot	1 Hour (Relative)	Displays the number of web application attacks that are blocked by WAF.	80
Access Control Event	Individual value plot	1 Hour (Relative)	Displays the number of requests that are blocked by the HTTP ACL policies of WAF.	10
CC Attack (World)	World map	1 Hour (Relative)	Displays the distribution of HTTP flood attacks by country.	-
CC Attack (China)	Map of China	1 Hour (Relative)	Displays the distribution of HTTP flood attacks by province in China.	-
Web Attack (World)	World map	1 Hour (Relative)	Displays the distribution of web application attacks by country.	-
Web Attack (China)	Map of China	1 Hour (Relative)	Displays the distribution of web application attacks by province in China.	-
Access Control Attack (World)	World map	1 Hour (Relative)	Displays the distribution (by country) of requests that are blocked by the HTTP ACL policies of WAF.	-

Chart name	Chart type	Default time range	Description	Example value
Access Control Attack (China)	Map of China	1 Hour (Relative)	Displays the distribution (by province in China) of requests that are blocked by the HTTP ACL policies of WAF.	-
Attacked Hosts	Treemap chart	1 Hour (Relative)	Displays the websites that are attacked most.	-
CC Attack Strategy Distribution	Pie chart	1 Hour (Relative)	Displays the distribution of HTTP flood protection policies.	-
Web Attack Type Distribution	Pie chart	1 Hour (Relative)	Displays the distribution of web attacks by attack type.	-
Top Attackers	Table	1 Hour (Relative)	Displays IP addresses, province information, and network providers of the first 100 clients that launch the recent attacks. It also displays the number of attacks and the amount of traffic generated by these attacks.	-
Attacker Referer	Table	1 Hour (Relative)	Displays the Referer information of attack requests, including Referer URLs, Referer hosts, and the number of attacks.	-

1.7. Log fields

WAF keeps detailed log entries for your domains, including access and attack protection logs. Each log entry contains dozens of fields. You can query and analyze specific fields based on your business requirements.

Field	Description	Example
__topic__	The topic of a log entry. This field is fixed to waf_access_log.	waf_access_log

Field	Description	Example
acl_action	The action taken by WAF to respond to the request based on HTTP ACL policies, such as pass, drop, and captcha. Note A null value or a hyphen (-) also indicates the pass action.	pass
acl_blocks	Indicates whether the request is blocked based on the HTTP ACL policies. • If the value is 1, the request is blocked. • If the value is not 1, the request is allowed.	1
antibot	The type of the Anti-Bot Service protection policy that applies. Valid values: • ratelimit: frequency control-based protection • sdk: enhanced app protection • algorithm: algorithm-based protection • intelligence: bot intelligence-based protection • acl: HTTP ACL policy-based protection • blacklist: blacklist-based protection	ratelimit
antibot_action	The action that is taken based on the Anti-Bot Service protection policy. Valid values: • challenge: verification by using an embedded JavaScript script • drop: block • report: record • captcha: slider captcha-based verification	challenge

Field	Description	Example
block_action	The type of the WAF protection feature that implements blocking. Valid values: • tmd: protection against HTTP flood attacks • waf: protection against web application attacks • acl: HTTP ACL policy • geo: region blocking • antifraud: data risk control • antibot: anti-bot	tmd
body_bytes_sent	The size of the HTTP message body sent to the client. Unit: bytes.	2
cc_action	The action taken for protection against HTTP flood attacks. Valid values: none, challenge, pass, close, captcha, wait, and login.	close
cc_blocks	Indicates whether the request is blocked by the HTTP flood protection feature. • If the value is 1, the request is blocked by the HTTP flood protection feature. • If the value is not 1, the request is allowed.	1
cc_phase	The HTTP flood protection policy that is triggered. Valid values: seccookie, server_ip_blacklist, static_whitelist, server_header_blacklist, server_cookie_blacklist, server_args_blacklist, and qps_overmax.	server_ip_blacklist
content_type	The content type of the access request.	application/x-www-form-urlencoded
host	The origin server.	api.aliyun.com
http_cookie	The Cookie HTTP header. This field includes information about the client.	k1=v1;k2=v2
http_referer	The Referer HTTP header. This field includes the source URL information. The value of this field is displayed as a hyphen (`-`) when there is no source URL information.	http://xyz.com

Field	Description	Example
http_user_agent	The User-Agent HTTP header. This field contains information such as the client browser and the operating system.	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)
http_x_forwarded_for	The X-Forwarded-For (XFF) HTTP header. This field identifies the original IP address of the client that connects to the web server by using an HTTP proxy or load balancing.	-
https	Indicates whether the request is an HTTPS request. Valid values: • true: The request is an HTTPS request. • false: The request is an HTTP request.	true
matched_host	The matched domain name that is protected by WAF. The domain name may be a wildcard domain name. The value of this field is displayed as a hyphen (`-`) when there are no matched domain names.	*.aliyun.com
querystring	The query string in the request URL.	title=tm_content%3Darticle&pid=123
real_client_ip	The real IP address of the client. If the real IP address cannot be obtained, the value of this field is displayed as a hyphen (`-`).	1.2.3.4
region	The region where the WAF instance resides.	cn
remote_addr	The IP address of the client that sends the access request.	1.2.3.4
remote_port	The port of the client that sends the access request.	3242
request_length	The size of the access request message. Unit: bytes.	123

Field	Description	Example
request_method	The HTTP request method.	GET
request_path	The relative path of the access request. The query string is not included.	/news/search.php
request_time_msec	The request processing duration. Unit: milliseconds.	44
request_traceid	The unique ID of the access request that is recorded by WAF.	7837b11715410386943437009ea1f0
server_protocol	The type and version number of the protocol that is used for the responses from the origin server.	HTTP/1.1
status	The HTTP status code returned by WAF to the client.	200
time	The time when the access request is initiated.	2018-05-02T16:03:59+08:00
ua_browser	The information of the browser that sends the access request.	ie9
ua_browser_family	The family of the browser.	internet explorer
ua_browser_type	The type of the browser.	web_browser
ua_browser_version	The version of the browser.	9.0
ua_device_type	The type of the client device.	computer
ua_os	The operating system of the client.	windows_7
ua_os_family	The family of the client operating system.	windows
upstream_addr	The list of back-to-origin IP addresses, separated with commas (,). Each IP address is in the `IP:Port` format.	1.2.3.4:443
upstream_ip	The IP address of the origin server where the requested resource resides. For example, if the origin server is an ECS instance, the value of this field is the IP address of the ECS instance.	1.2.3.4

Field	Description	Example
upstream_response_time	The duration used by the origin server to respond to the request from WAF. Unit: seconds. If the value of this field is displayed as a hyphen (-), the response times out.	0.044
upstream_status	The HTTP status code that WAF receives from the origin server. If the value of this field is displayed as a hyphen (-), the request is blocked by WAF or the response from the origin server times out.	200
user_id	The ID of the Alibaba Cloud account.	12345678
waf_action	The action that is taken for protection against web attacks. Valid values: • block: The request is blocked. • bypass or other values: The request is allowed.	block
web_attack_type	The type of the web attack. Valid values: xss, code_exec, webshell, sqli, lfilei, rfilei, and other.	xss
waf_rule_id	The ID of the matched WAF rule.	100

1.8. Export log data

This topic describes how to export log query results to your local device by using Log Service for WAF.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Log Service** .
4. On the Log Service page, click the **Log Query** tab, enter a query statement, and click **Search & Analyze**.
5. On the **Raw Logs** tab, click the download icon

   

   on the right.

   > **Note** The download icon is not displayed if no query result is found.

6. In the **Log Download** dialog box, select **Download Log in Current Page** or **Download all logs**

in the CLI console.

- **Download Log in Current Page**: After you select this radio button, click **OK** to export raw log data that is queried on the current page as a CSV file to your local device.
- **Download all logs in the CLI console**
  a. Install the CLI. For more information, see User Guide.
  b. Go to the Security Management page and view and record the AccessKey ID and AccessKey secret of the current user.
  c. Click **Copy command** and paste the command in the CLI, replace `AccessID obtained in step 2` and `AccessKey obtained in step 2` with the AccessKey ID and AccessKey secret of the current user, and run the command.

  All raw log data that is recorded by WAF is automatically downloaded and saved to the *download_data.txt* file in the directory where the command was run.

1.9. Use advanced management

Log Service for WAF supports the advanced management feature. You can click Advanced Settings in the upper-right corner of the Log Service page in the WAF console to go to the Log Service console. In the Log Service console, you can set alerts and notifications, set real-time log subscription and consumption, deliver log data, and integrate Log Service with other services for data visualization.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Log Service** .
4. On the Log Service page that appears, click **Advanced Settings** in the upper-right corner.

   Click Advanced Settings
5. In the message that appears, click **OK**.

Result

In the Log Service console, you can perform the following operations on the dedicated Logstore and project of WAF:

- Set alerts and notifications.
- Set real-time log subscription and consumption.
- Deliver log data to other Alibaba Cloud storage services in real time.
- Integrate Log Service with other services for data visualization.

1.10. Grant log query and analysis permissions to a RAM user

A RAM user can use the log query and analysis function of WAF only after the Alibaba Cloud account grants the required permissions to the RAM user.

Context

The following table describes the types of operations and accounts that are required to enable and use the log query and analysis function.

Operation type	Required account
Activate Log Service. You only need to perform this operation once.	Alibaba Cloud accounts
Authorize WAF to write log data to the dedicated Logstore in Log Service in real time. You only need to perform this operation once.	• Alibaba Cloud accounts • RAM users that have the `AliyunLogFullAccess` permission • RAM users that have specific permissions
Use the log query and analysis function.	• Alibaba Cloud accounts • RAM users that have the `AliyunLogFullAccess` permission • RAM users that have specific permissions

You can grant permissions to RAM users based on your business requirements.

Scenario	Permission	Procedure
Grant all operation permissions of Log Service to RAM users.	`AliyunLogFullAccess`	For more information about how to grant permissions, see Grant permissions to a RAM user.
Grant log viewing permissions to RAM users after you use your Alibaba Cloud account to enable the log query and analysis function of WAF and complete the cloud resource access authorization.	`AliyunLogReadOnlyAccess`	For more information about how to grant permissions, see Grant permissions to a RAM user.
Grant only the permissions to enable and use the log query and analysis function of WAF to RAM users. The RAM users are not granted other management permissions on Log Service.	Permissions that are defined in a custom permission policy	For more information about how to customize a permission policy, see the following operation procedure.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Policies** under **Permissions**.
3. On the page that appears, click **Create Policy**.
4. On the Create Custom Policy page, specify the **Policy Name** and **Note** parameters.
5. Select **Script** for **Configuration Mode** and enter the following policy content.

> **Note** Replace `${Project}` and `${Logstore}` in the following policy content with the names of the dedicated project and Logstore in Log Service for WAF.

```
{
 "Version": "1",
 "Statement": [
   {
   "Action": "log:GetProject",
   "Resource": "acs:log:*:*:project/${Project}",
   "Effect": "Allow"
  },
  {
   "Action": "log:CreateProject",
   "Resource": "acs:log:*:*:project/*",
   "Effect": "Allow"
  },
  {
   "Action": "log:ListLogStores",
   "Resource": "acs:log:*:*:project/${Project}/logstore/*",
   "Effect": "Allow"
  },
  {
   "Action": "log:CreateLogStore",
   "Resource": "acs:log:*:*:project/${Project}/logstore/*",
   "Effect": "Allow"
  },
  {
   "Action": "log:GetIndex",
   "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
   "Effect": "Allow"
  },
  {
   "Action": "log:CreateIndex",
```

```
    "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
    "Effect": "Allow"
   },
   {
    "Action": "log:UpdateIndex",
    "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
    "Effect": "Allow"
   },
   {
    "Action": "log:CreateDashboard",
    "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
    "Effect": "Allow"
   },
   {
    "Action": "log:UpdateDashboard",
    "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
    "Effect": "Allow"
   },
   {
    "Action": "log:CreateSavedSearch",
    "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
    "Effect": "Allow"
   },
   {
    "Action": "log:UpdateSavedSearch",
    "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
    "Effect": "Allow"
   }
  ]
}
```

6. Click **OK**.
7. In the left-side navigation pane, choose **Identities** > **Users**. On the Users page, find the RAM user to which you want to grant permissions and click **Add Permissions** in the Actions column.
8. In the Add Permissions pane that appears, select the custom permission policy that you created, and then click **OK**.
   The RAM user can enable and use the log query and analysis function of WAF. However, the RAM user cannot use other functions of Log Service.

1.11. Change log storage duration

After you enable the Log Service for Web Application Firewall (WAF) feature, you can set the maximum log storage duration to 180 days or 360 days. You can set the maximum log storage duration based on the log storage capacity and your actual needs. This topic is suitable only for users who have purchased subscription-based WAF instances. The edition of the instances must be Business or above.

Prerequisites

- A WAF instance is purchased and the instance meets the following requirements:
  - The WAF instance uses the subscription billing method.
  - The edition of the instance is **Business** or above.

    Note If the WAF instance is of the Pro edition or lower, you cannot change the log storage period.

- The Log Service for WAF feature is enabled. For more information, see Enable Log Service for WAF.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Log Service** .
4. In the upper-right corner of the **Log Service** page, move your pointer over **Log Storage Period**, specify the log storage duration, and then click **Save**.
   - If you set **Log Storage Period** to **360 Days** when you enable the Log Service for WAF feature, the default log storage duration is 360 days. You can click **30**, **90**, **180**, or **360** to specify the log storage duration to 30 days, 90 days, 180 days, or 360 days. You can also click **Custom** and enter an integer within the range of 30 to 360.
   - If you set **Log Storage Period** to **180 Days** when you enable the Log Service for WAF feature, the default log storage period is 180 days. You can click **30**, **90**, or **180** to specify the log storage duration to 30 days, 90 days, or 180 days. You can also click **Custom** and enter an integer within the range of 30 to 180.

     Note When you enable the Log Service for WAF feature, you can set **Log Storage Period** to **180 Days** or **360 Days**. The maximum value cannot be changed. If you want to change the maximum value of Log Storage Period, click **Upgrade**.

Result

After the log storage duration is changed, Log Service for WAF only stores logs within the specified duration and automatically deletes expired logs.

1.12. Manage log storage space

This topic describes how to manage log storage space. After you activate Log Service for Web Application Firewall (WAF), the system allocates log storage space based on the storage capacity that you select. You can view the usage of log storage space on the Log Service page in the WAF console.

View the usage of log storage space

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Log Service** .
4. On the **Log Service** page that appears, view the usage of log storage space in the upper-right corner.

> **Note** The usage of log storage space displayed in the WAF console is not updated in real time. The actual usage is updated every two hours. Before you exceed your allocated log storage space, we recommend that you expand your log storage space.

Expand the log storage space

In the upper-right corner of the **Log Service** page, click **Upgrade Storage**. On the page that appears, select a larger storage capacity and pay for the order.

> **Note** If you exceed your allocated log storage space, WAF cannot write new log data into a dedicated Logstore.

Clear your log storage space

You can delete all log data based on your business requirements. For example, you can delete all log data generated during the test phase to save space for useful log data that is generated during the service production.

> **Note** After Log Service for WAF is activated, you can clear your log storage space for four times in total.

Click **Clear** in the upper-right corner of the **Log Service** page. In the message that appears, click **OK** to delete all log data.

> **Warning** You cannot recover log data that is deleted. Proceed with caution.

2.Integrate WAF logs into a Syslog server

This topic describes how to use Python Program to integrate Web Application Firewall (WAF) logs into a Syslog server to meet regulatory and audit requirements. This allows you to manage all the related logs in your security operations center.

Background information

The following figure shows the integration architecture.

Architecture

Log Service is an end-to-end logging service developed by Alibaba Cloud and is widely used by Alibaba Group in big data scenarios. Log Service allows you to complete the collection, consumption, delivery, query, and analysis of log data without the need for development. This improves the O&M efficiency and the operational efficiency and delivers capabilities of processing a large number of logs in the Data Technology (DT) era. WAF is integrated with Log Service. The Log Service for WAF feature allows you to collect, query, and analyze website access logs. For more information, see Overview.

Python Program is a program running on ECS instances to deliver WAF logs to a Syslog server. The consumer library is an advanced mode provided for LogHub consumers. It uses consumer groups to manage the consumption end. Compared with the mode in which data is read by using SDKs, the consumer library enables you to focus only on the business logic. You do not need to concern about the implementation details of Log Service or the fault tolerance among multiple consumers. For more information, see Use consumer groups to consume logs.

The Syslog server centrally manages log messages. It can receive data from multiple Syslog sources.

Prerequisites

- Log Service for WAF is enabled. The log collection feature is enabled for your domain name. For more information, see the following topics:
  - Enable Log Service for WAF
  - Enable log collection
- A Linux ECS instance with the following recommended configurations is deployed:
  - Ubuntu operating system
  - 2.0 GHz processor or above, with eight cores
  - 32 GB of memory
  - Available disk space greater than 2 GB (More than 10 GB of available disk space is recommended.)
- A Syslog server is deployed, and the UDP port 514 is enabled on the server to receive Syslog data.

Procedure

Install Log Service SDK for Python on your ECS instance and configure Python Program to deliver WAF logs to the Syslog server. Perform the following steps:

1. Connect to the ECS instance by using SSH or in the ECS console. For more information, see Connect to an ECS instance.
2. Install Python 3, pip, and aliyun-log-python-sdk. For more information about Log Service SDK for Python, see User Guide.

```
apt-get update
apt-get install -y python3-pip python3-dev
cd /usr/local/bin
ln -s /usr/bin/python3 python
pip3 install --upgrade pip
pip install aliyun-log-python-sdk
```

3. Run the following command to download the latest integration sample code from GitHub:

```
wget https://raw.githubusercontent.com/aliyun/aliyun-log-python-sdk/master/tests/consumer_group_examples/sync_data_to_syslog.py
```

4. Replace Log Service and Syslog parameters in Python Program. The following table describes the parameters.

Parameter	Meaning	Description
SLS Project	Log project name	A project is the basic unit to isolate and control resources in Log Service. You can log on to the Log Service console to view the log projects of WAF. The name of a WAF log project starts with `waf-project`. Projects that reside in the **China (Hangzhou)** region are the log projects of WAF instances in mainland China. Projects that reside in the **Singapore** region are the log projects of WAF instances outside mainland China. 
SLS Endpoint	Log Service endpoint	The Log Service endpoint is a URL used to access a project and logs in the project. The endpoint varies based on the Alibaba Cloud region where the project resides and the project name. To view the URL, see Endpoints.
SLS Logstore	Logstore	A Logstore is a unit in Log Service to collect, store, and query log data. Each Logstore belongs to a single project. Each project can have multiple Logstores. You can log on to the Log Service console and click a WAF log project to view the Logstore name. 

Parameter	Meaning	Description
SLS AccessKey ID and AccessKey Secret	AccessKey pair	An AccessKey pair consists of an AccessKey ID and an AccessKey secret and is designed to access your cloud resources by using APIs instead of the console. You can use the AccessKey pair to sign API requests so that the requests can pass the security authentication in Log Service. For more information, see AccessKey. You can log on to the User Management console to view the information of your AccessKey pair.
Syslog Host	Syslog host	The IP address or hostname of the Syslog server.
Syslog Port	Syslog port	The port used to receive Syslog data. The UDP port 514 and the TCP port 1468 are supported.
Syslog protocol	Syslog protocol	The UDP or TCP protocol that is used to receive Syslog data. The parameter value varies based on the configurations of the Syslog server.
Syslog separator	Syslog delimiter	The delimiter used to separate Syslog key-value pairs.

The following code provides an example of how to configure Python Program:

- Log Service configurations

```
endpoint = os.environ.get('SLS_ENDPOINT', 'http://ap-southeast-1.log.aliyuncs.com')
accessKeyId = os.environ.get('SLS_AK_ID', 'Your AccessKey ID')
accessKey = os.environ.get('SLS_AK_KEY', 'Your AccessKey secret')
project = os.environ.get('SLS_PROJECT', 'waf-project-548613414276****-ap-southeast-1')
logstore = os.environ.get('SLS_LOGSTORE', 'waf-logstore')
consumer_group = os.environ.get('SLS_CG', 'WAF-SLS')
```

- Syslog configurations

```
settings = {
            "host": "1.2.xx.xx",
            "port": 514,
            "protocol": "udp",
            "sep": ",",
            "cert_path": None,
            "timeout": 120,
            "facility": syslogclient.FAC_USER,
            "severity": syslogclient.SEV_INFO,
            "hostname": None,
            "tag": None
        }
```

5. Start Python Program. Assume that Python Program is saved as `sync_data_to_syslog.py`. Run the following command to start it:

   ```
   python sync_data_to_syslog.py
   ```

   The following command output shows that logs are delivered to the Syslog server after the start of Python Program:

   ```
   *** start to consume data...
   consumer worker "WAF-SLS-1" start
   heart beat start
   heart beat result: [] get: [0, 1]
   Get data from shard 0, log count: 6
   Complete send data to remote
   Get data from shard 0, log count: 2
   Complete send data to remote
   heart beat result: [0, 1] get: [0, 1]
   ```

You can query WAF logs in the Syslog server.

3.Use full logs

After you enable the full log feature, Web Application Firewall (WAF) logs all access requests to your website. You can search for and locate request logs with a few clicks. This facilitates operations and security management.

> **Notice** The full log feature is available only to existing users who have enabled this feature. For new users, the full log feature is no longer provided. If you want to use the website access logs, we recommend that you enable Log Service for WAF. For more information, see Enable Log Service for WAF.

Background information

The full log feature facilitates the following O&M tasks:

- Check whether a request is intercepted or allowed by WAF.
- Check whether request interception is triggered by ACL rules for web attack protection or HTTP flood attack protection, or custom ACL rules.
- Query the time taken by the origin server to respond to a request and check whether the response times out.
- Query a request by using a combination of the following conditions: source IP address, URL keyword, Cookie, Referer, User-Agent, X-Forwarded-For (XFF), and HTTP status code.

Usage notes

- If you enable the full log feature, WAF logs all the web requests that pass through WAF. POST requests are not logged.
- A subscription WAF instance stores all web access logs from the last month.

  > **Note** If you want to store logs for 180 days and meet the classified protection requirements, we recommend that you enable Log Service for WAF. For more information, see Enable Log Service for WAF.

- A WAF instance allows you to enable the full log feature for a maximum of 100 domains.

Enable the full log feature

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Asset Center** > **Website Access**.
4. Find the target domain and turn on **Log search**.

   > **Note** **Log search** is available only to existing users who have enabled the full log feature. Other users can view only **Log Service**. For more information about Log Service for WAF, see Overview.

   Log search

After you turn on **Log search**, WAF logs access requests to your website. Then, you can query the full logs. For more information, see Query full logs.

If the full log feature is no longer required, you can also turn off **Log search** on the **Website Access** page.

> **Note** After you turn off **Log search**, WAF does not log access requests to your website. Even if you turn on **Log search** later, you cannot query access request logs from the period when the switch is turned off.

Query full logs

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **International**, in which the instance is deployed.
3. In the left-side navigation pane, choose **Log Management** > **Logs**.
4. On the **Log Query** tab, select the target domain and time range, and click **Search**.

   Query full logs

   > **Note** If you purchase a subscription WAF instance, you can query logs from the last month.

   You can also click **Advanced Search** to specify more filter conditions. For more information about the filter fields supported in Advanced Search, see Advanced search conditions.

   Advanced Search
5. View details about the returned logs.
   - In the **Service Traffic** section, view the access request trends from the specified time range.

     Service Traffic
   - In the **Request Logs** section, view the access request records that meet the specified conditions.

     For example, the following figure shows the records of access requests that are intercepted based on ACL rules. For more information about log fields, see Access log fields.

     Request Logs
6. (Optional)Download the logs.You can download the logs to your computer as required.
   i. In the upper-right corner of the **Log Query** tab, click **Log download**.
   ii. After the download task is created, click the **View the Downloaded File** tab to download the logs to your computer in the required format.

   > **Note** You can download a maximum of 20 million logs in a single download task. If you want to download more logs, create more tasks.

Advanced search conditions

Field	Description
Source IP	The source IP address of the client.
URL Key Words	The URL of the access requests. Note You can enter forward slashes (/) in this field. For example, enter `/ntis/cashier`.
Cookie	The Cookie HTTP header. This field provides the source information of the client.
Referer	The Referer HTTP header. This field provides the source URL of the client.
User-Agent	The User-Agent HTTP header. This field includes the client information, such as the browser and operating system.
X-Forwarded-For	The X-Forwarded-For HTTP header.
Server Response Code	The status code that the origin server returns to WAF. It contains a maximum of three digits and supports fuzzy search. For example, if you enter `4*` for search, the system returns all status codes that start with 4. Note • Asterisks (`*`) can be used to match 0 or multiple digits. However, you cannot enter a number that starts with an asterisk (`*`). • You can enter a hyphen (`-`) to search for access requests that do not have status information.
Status Code Returned by WAF	The status code that WAF returns to the client. It contains a maximum of three digits and supports fuzzy search. For example, if you enter `4*` for search, the system returns all status codes that start with 4. Note • Asterisks (`*`) can be used to match 0 or multiple digits. However, you cannot enter a number that starts with an asterisk (`*`). • You can enter a hyphen (`-`) to search for access requests that do not have status information.

Field	Description
Request Unique ID	The specific access request. If an access request is intercepted, you can enter its ID for search.
Request domain name	If you have enabled the full log feature for wildcard domains, you can specify this field to search for first-level subdomains.
Protection policies	The protection policies to apply. Valid values: **Web Attack Blocking**, **HTTP Flood Protection Policies**, **HTTP ACL Policies**, **Data Risk Control**, **Block IPs Initiating Frequent Web Attacks**, **Directory Scan Protection**, **Scanning Tool Blocking**, and **Collaborative Defense**.

Access log fields

Field	Meaning	Description
Time	Access time	The time when the access request was initiated. This field is a UTC time record in the log file.
Domain	Access domain	The domain that is requested.
Source_IP	Source IP address	The source IP address of the client.
IP_City	Region of the source IP address	The region in which the source IP address is located. If the source IP address is located in mainland China, this field can be accurate to the city level.
IP_Country	Country of the source IP address	The country in which the source IP address is located.
Method	Access request method	The request method specified in the request line.
URL	Access request URL	The URL of the requested resource specified in the request line.
Https	Access request protocol	The protocol of the access request specified in the request line.
Referer	Referer HTTP	The Referer HTTP header. This field provides the source URL of the client.
User-Agent	User-Agent HTTP	The User-Agent HTTP header. This field includes the client information, such as the browser and operating system.
X-Forwarded-For	X-Forwarded-For HTTP	The X-Forwarded-For HTTP header. This field identifies the real IP address of the client that connects to the web server by using an HTTP proxy or load balancing device.

Field	Meaning	Description
Cookie	Cookie HTTP	The Cookie HTTP header. This field provides the source information of the client.
Attack_Type	Protection status	The result after WAF processes the access request: • 0: No attacks are detected. • 1: Rules are triggered to protect against web application attacks. • 2: Rules are triggered to protect against HTTP flood attacks. • 3: Rules are triggered to implement precise access control. • 4: Policies are triggered to block requests from specified regions. • 5: Policies are triggered to control data risks. • 6: Rules are triggered to block IP addresses from which scanning attacks are frequently initiated. • 7: Rules are triggered to protect against directory traversal attacks. • 8: Policies are triggered to implement collaborative protection. • 9: Rules are triggered to block scanning tools.
Status	Response status code	The status code that WAF returns to the client.
Upstream_Status	Response status code of the origin server	The status code that the origin server returns to WAF. If the value of this field is a hyphen (`-`), the request is blocked by WAF or the response from the origin server times out.
Upstream_IP	IP address of the origin server	The IP address of the origin server for the access request. For example, if the origin server of WAF is an ECS instance, the value of this field is the IP address of the ECS instance.
Upstream_Time	Response time of the origin server	The time taken by the origin server to respond to a request from WAF. If the value of this field is a hyphen (`-`), the response times out.