ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

Log Management

Document Version: 20211129

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 for WAF

1.1. Overview of the Log Service for WAF feature

Web Application Firewall (WAF) is integrated with Log Service to provide the Log Service for WAF feature. The feature collects and stores access logs and protection logs of domain names that are added to WAF. You can use this feature to query and analyze log data, configure charts to generate, configure alert rules, and deliver log data to downstream services for consumption. This feature allows you to focus on log analysis.

Intended users

- Large-scale enterprises and organizations, such as financial entities and public service sectors that need to meet log storage requirements. The logs include host, network, and security logs of various assets in the cloud.
- Organizations, such as large-scale real estate, e-commerce, financial entities, and public service sectors that have security operations centers (SOCs) and want to collect and manage security and alert logs in a centralized manner.
- 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 (MLPS level 3 or higher).

Scenarios

- Trace web attack logs and identify the source of security threats.
- View requests and query the request status and trends.
- Obtain information about the efficiency of security operations and respond to issues at the earliest opportunity.
- Generate and deliver security network logs to self-managed data and computing centers.

Benefits

- Compliance audits: This feature allows you to store website access logs for more than six months to meet classified protection requirements.
- Flexible configuration:
  - This feature allows you to collect and store web access and protection logs with a few steps.
  - This feature allows you to configure the custom log storage duration and capacity and specify the websites whose logs you want to collect.
  - This feature allows you to modify existing report templates or create custom report templates based on 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 interactive data mining. This allows you to identify and analyze various attacks on your website and access details in real time.
- Real-time alerting: You can customize monitoring and alert rules based on specific metrics. This way, you can respond to exceptions that occur in critical services at the earliest opportunity.

- Collaboration: You can use this feature together with other data solutions such as real-time computing, cloud storage, and visualization to further explore the value of data.

Billing and enabling

Subscription WAF instances that run the Pro edition or higher support the Log Service for WAF feature.

You can use the Log Service for WAF feature only after you enable the feature. When you use the Log Service for WAF feature, you are charged based on the log storage capacity that you purchase. For more information about billing, see Billing.

For more information about how to enable the Log Service for WAF feature, see Enable Log Service for WAF.

Features

Feature	Description
Log collection	After you enable the Log Service for WAF feature, you can enable log collection for domain names that are added to WAF. WAF can collect and store logs for the domain names only after log collection is enabled for the domain names. You can query and analyze the collected log data. For more information about the log fields supported by WAF, see Log fields supported by WAF. You can modify log settings, such as the storage period, optional log fields, and storage type. The storage types are Logs and Block Logs. For more information, see Modify log settings.
Log query and analysis	You can use query statements to query and analyze collected logs. Each query statement consists of a search statement and an analytic statement that uses the standard SQL-92 syntax. The search statement and analytic statement are separated by a vertical bar (|). For more information about search statements, see Search syntax. For more information about analytic statements, see Log analysis overview. By default, analysis results are displayed in tables. You can also choose to view analysis results in charts, such as line charts, column charts, or pie charts. You can create alert rules based on query statements. After an alert rule is created, Log Service regularly checks query and analysis results. If a query and analysis result meets the trigger condition that you specify in the alert rule, Log Service sends an alert notification. For more information, see Log alerts.
Dashboards	A dashboard provides real-time data analysis results. You can view multiple charts that are generated based on query and analysis results on a dashboard. The Log Service for WAF feature provides the following three dashboards based on common business and security scenarios: Operation Center, Access Center, and Security Center dashboards. If you want to view the business and security data of your website, you need only to specify a time range on the dashboards. You do not need to enter a query statement. You can subscribe to dashboards to send dashboard data to specific recipients by using emails.
Management of log storage space	You can query the amount of storage that is occupied by logs on a regular basis. You can also increase the storage capacity or delete the stored logs based on your business requirements.

Feature	Description
Integrate WAF logs into a Syslog server	To meet regulatory and audit requirements, you can use Python programs to deliver logs from WAF to a Syslog server. This allows you to manage all the related logs in your security operations center.

1.2. Billing

This topic describes the billing of the Log Service for WAF feature. You are charged based on the log storage capacity that you purchase.

Overview

The Log Service for WAF feature is available for subscription WAF instances that run the Business or higher edition.

To enable the Log Service for WAF feature, perform the following steps: On the Web Application Firewall buy page, set the **Log Service** parameter to YES. Then, configure the **Log Storage Period** and **Log Storage Size** parameters based on your business requirements. For more information, see Enable Log Service for WAF.

WAF calculates fees based on the log storage capacity that you select and the subscription period of your WAF instance.

Log storage specifications

Specification	Impact on billing	Description	Modification after the Log Service for WAF feature is enabled
Log storage capacity	Yes	When you enable the Log Service for WAF feature, you can specify the log storage capacity based on your business requirements. The log storage capacity is measured in TB. The log storage capacity is charged by using the subscription billing method. The fees displayed on the Web Application Firewall buy page shall prevail.	You can upgrade your WAF instance to increase the log storage capacity. For more information, see Renewal and upgrade. **Notice** If the log storage capacity that you purchase is exhausted and you do not increase the log storage capacity at the earliest opportunity, WAF no longer writes log data to the dedicated Logstore of WAF. Logs that are stored for longer than the storage period that you specify are deleted.
Storage period	No	When you enable the Log Service for WAF feature, you can specify the storage period to 180 days or 360 days.	You can specify a custom storage period that ranges from 30 days to 360 days only for subscription WAF instances that run the Business or higher edition. For more information, see Modify log settings.

Methods to specify the log storage capacity

You can specify the log storage capacity based on the log storage configurations and the daily QPS of your website service.

Log storage configurations include the following items:

- Log type: The log types include full logs and attack logs. If you want to store full logs, you must specify a larger storage capacity than the capacity that is required for attack logs.
- Log storage period: A longer storage period requires a larger log storage capacity.
- Fields contained in logs: WAF log fields are classified into required fields and optional fields. If you want to include more optional fields, you must specify a larger log storage capacity.

If you enable the Log Service for WAF feature for the first time, the following default log storage configurations are used: full log type, 180-day storage period, and only required fields. You can modify log storage configurations by using the **log settings** feature. For more information, see Modify log settings.
For example, the default log storage configurations are used. The following list provides suggestions on how to select the required log storage capacity based on the daily QPS of your website service:

- If the daily average QPS is not greater than 80, we recommend that you select 3 TB of storage capacity.
- If the daily average QPS ranges from 80 to 120, we recommend that you select 5 TB of storage capacity.
- If the daily average QPS ranges from 120 to 260, we recommend that you select 10 TB of storage capacity.
- If the daily average QPS ranges from 260 to 350, we recommend that you select 15 TB of storage capacity.
- If the daily average QPS ranges from 350 to 500, we recommend that you select 20 TB of storage capacity.
- If the daily average QPS ranges from 500 to 1,200, we recommend that you select 50 TB of storage capacity.

> **Note** If you want to customize the log storage configurations, you can estimate the required log storage capacity based on the preceding information.

Billing cycle

The billing cycle of the Log Service for WAF feature varies based on the method that you use to enable the Log Service for WAF feature.

- If you enable the Log Service for WAF feature when you purchase a subscription WAF instance, the billing cycle of the feature is the same as the subscription period that you select for the WAF instance.
- If you upgrade your subscription WAF instance to enable the Log Service for WAF feature, the billing cycle of the feature is equal to the remaining validity period of your WAF instance. The billing cycle is accurate to the minute.

Expiration

If your WAF instance expires, the Log Service for WAF feature also expires. If the Log Service for WAF feature expires, the following issues occur:

- WAF no longer writes log data to the dedicated Logstore.
- Log data is retained only for seven days.
  If you renew your WAF instance within seven days, you can continue to use this feature. Otherwise, all log data is deleted.

1.3. Log fields supported by WAF

This topic describes the log fields supported by Web Application Firewall (WAF).

Table for field retrieval

The following table describes the exclusive fields that are supported by WAF. You can use the names of fields to retrieve the fields that you want to view.

First letter of a field name	Field
a	account_action | account_rule_id | account_test | acl_action | acl_rule_id | acl_rule_type | acl_test | algorithm_action | algorithm_rule_id | algorithm_test | antifraud_action | antifraud_test | antiscan_action | antiscan_rule_id | antiscan_rule_type | antiscan_test
b	block_action | body_bytes_sent | bypass_matched_ids
c	cc_action | cc_rule_id | cc_rule_type | cc_test | content_type
d	deeplearning_action | deeplearning_rule_id | deeplearning_rule_type | deeplearning_test | dlp_action | dlp_rule_id | dlp_test
f	final_action | final_plugin | final_rule_id | final_rule_type
h	host | http_cookie | http_referer | http_user_agent | http_x_forwarded_for | https
i	intelligence_action | intelligence_rule_id | intelligence_test
m	matched_host
n	normalized_action | normalized_rule_id | normalized_rule_type | normalized_test
q	querystring
r	real_client_ip | region | remote_addr | remote_port | request_body | request_length | request_method | request_path | request_time_msec | request_traceid
s	scene_action | scene_id | scene_rule_id | scene_rule_type | scene_test | server_port | server_protocol | ssl_cipher | ssl_protocol | status
t	time
u	ua_browser | ua_browser_family | ua_browser_type | ua_browser_version | ua_device_type | ua_os | ua_os_family | upstream_addr | upstream_response_time | upstream_status| user_id
w	waf_action | waf_rule_id | waf_rule_type | waf_test | wxbb_action | wxbb_invalid_wua | wxbb_rule_id | wxbb_test

Protection log fields

Protection log fields are generated by WAF when client requests match the rules specified in WAF protection features. You can use the protection log fields to analyze attacks on your business. The rules can be used to allow or block requests.

Description of the action field

Field	Description	Sample value
account_action	The action that is performed on the request after an account security rule is triggered. The value is fixed as *block*, which indicates that WAF blocks the client request. For more information about WAF protection actions, see Description of the action field.	block
account_rule_id	The ID of the account security rule that is triggered.	151235
account_test	The protection mode that is used for the request after an account security rule is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
acl_action	The action that is performed on the request after a rule created for the blacklist or custom protection policy (ACL) feature is triggered. Valid values: • *block*: indicates that the request is blocked. • *captcha_strict*: indicates that strict slider CAPTCHA verification is performed. • *captcha*: indicates that common slider CAPTCHA verification is performed. • *js*: indicates that JavaScript verification is performed. • *captcha_strict_pass*: indicates that the client passes strict slider CAPTCHA verification and WAF allows the request from the client. • *captcha_pass*: indicates that the client passes common slider CAPTCHA verification and WAF allows the request from the client. • *js_pass*: indicates that the client passes JavaScript verification and WAF allows the request from the client. For more information about WAF protection actions, see Description of the action field.	block
acl_rule_id	The ID of the rule that is triggered. The rule is created for the blacklist or custom protection policy (ACL) feature.	151235
acl_rule_type	The type of the rule that is triggered. The rule is created for the blacklist or custom protection policy (ACL) feature. Valid values: • *custom*: indicates a rule that is created for the custom protection policy feature. • *blacklist*: indicates a rule that is created for the blacklist feature.	custom

Field	Description	Sample value
acl_test	The protection mode that is used for the request after a rule created for the blacklist or custom protection policy (ACL) feature is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
algorithm_action	The action that is performed on the request after a rule created for the typical bot behavior identification feature is triggered. Valid values: • *block*: indicates that the request is blocked. • *captcha*: indicates that common slider CAPTCHA verification is performed. • *js*: indicates that JavaScript verification is performed. • *captcha_pass*: indicates that the client passes common slider CAPTCHA verification and WAF allows the request from the client. • *js_pass*: indicates that the client passes JavaScript verification and WAF allows the request from the client. For more information about WAF protection actions, see Description of the action field.	block
algorithm_rule_id	The ID of the rule that is triggered. The rule is created for the typical bot behavior identification feature.	151235
algorithm_test	The protection mode that is used for the request after a rule created for the typical bot behavior identification feature is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
antifraud_action	The action that is performed on the request after a rule created for the data risk control feature is triggered. Valid values: • *pass*: indicates that the request is allowed. • *block*: indicates that the request is blocked. • *captcha*: indicates that common slider CAPTCHA verification is performed. For more information about WAF protection actions, see Description of the action field.	block

Field	Description	Sample value
antifraud_test	The protection mode that is used for the request after a rule created for the data risk control feature is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
antiscan_action	The action that is performed on the request after a rule created for the scan protection feature is triggered. The value is fixed as *block*, which indicates that WAF blocks the request from the client. For more information about WAF protection actions, see Description of the action field.	block
antiscan_rule_id	The ID of the rule that is triggered. The rule is created for the scan protection feature.	151235
antiscan_rule_type	The type of the rule that is triggered. The rule is created for the scan protection feature. Valid values: • *highfreq*: indicates a rule that blocks IP addresses from which web attacks are frequently initiated. • *dirscan*: indicates a rule that defends against directory traversal attacks. • *scantools*: indicates a rule that blocks the IP addresses of scanning tools. • *collaborative*: indicates a collaborative defense rule.	highfreq
antiscan_test	The protection mode that is used for the request after a rule created for the scan protection feature is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false

Field	Description	Sample value
block_action	**Notice** This field is no longer valid due to WAF upgrades. The field final_plugin replaces this field. If the block_action field is used in your services, replace the field with final_plugin at the earliest opportunity. The WAF protection feature that is triggered to block the request. Valid values: • *tmd*: indicates HTTP flood protection. The value is equivalent to the *cc* value of final_plugin. • *waf*: indicates web attack protection. The value is equivalent to the *waf* value of final_plugin. • *acl*: indicates the custom protection policy feature. The value is equivalent to the *acl* value of final_plugin. • *deeplearning*: indicates the Deep Learning Engine. The value is equivalent to the *deeplearning* value of final_plugin. • *antiscan*: indicates scan protection. The value is equivalent to the *antiscan* value of final_plugin. • *antifraud*: indicates data risk control. The value is equivalent to the *antifraud* value of final_plugin. • *antibot*: indicates bot management. The value is equivalent to the *intelligence*, *algorithm*, *wxbb*, and *scene* values of final_plugin.	waf
bypass_matched_ids	The ID of the rule that is triggered to allow the request. The rule can be a whitelist rule or a custom protection rule that allows the request. If multiple rules are triggered at the same time to allow the request, this field records the IDs of all the rules. Multiple IDs are separated by commas (,).	283531
cc_action	The action that is performed on the request after a rule is triggered. The rule is created for the HTTP flood protection or custom protection policy (HTTP Flood Protection) feature. Valid values: • *block*: indicates that the request is blocked. • *captcha*: indicates that common slider CAPTCHA verification is performed. • *js*: indicates that JavaScript verification is performed. • *captcha_pass*: indicates that the client passes common slider CAPTCHA verification and WAF allows the request from the client. • *js_pass*: indicates that the client passes JavaScript verification and WAF allows the request from the client. For more information about WAF protection actions, see Description of the action field.	block
cc_rule_id	The ID of the rule that is triggered. The rule is created for the HTTP flood protection or custom protection policy (HTTP Flood Protection) feature.	151234

Field	Description	Sample value
cc_rule_type	The type of the rule that is triggered. The rule is created for the HTTP flood protection or custom protection policy (HTTP Flood Protection) feature. Valid values: • *custom*: indicates a custom protection rule (HTTP Flood Protection). • *system*: indicates an HTTP flood protection rule.	custom
cc_test	The protection mode that is used for the request after a rule is triggered. The rule is created for the HTTP flood protection or custom protection policy (HTTP Flood Protection) feature. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
deeplearning_action	The action that is performed on the request after a rule created for the Deep Learning Engine is triggered. The value is fixed as *block*, which indicates that WAF blocks the request from the client. For more information about WAF protection actions, see Description of the action field.	block
deeplearning_rule_id	The ID of the rule that is triggered. The rule is created for the Deep Learning Engine.	151238
deeplearning_rule_type	The type of the rule that is triggered. The rule is created for the Deep Learning Engine. Valid values: • *xss*: indicates a rule that defends against XSS attacks. • *code_exec*: indicates a rule that defends against specific attacks. The attacks exploit code execution vulnerabilities. • *webshell*: indicates a rule that defends against webshell uploads. • *sqli*: indicates a rule that defends against SQL injection. • *lfilei*: indicates a rule that defends against local file inclusion. • *rfilei*: indicates a rule that defends against remote file inclusion. • *crlf*: indicates a rule that defends against carriage return line feed (CRLF) injection. • *other*: indicates other protection rules.	xss
deeplearning_test	The protection mode that is used for the request after a rule created for the Deep Learning Engine is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false

Field	Description	Sample value
dlp_action	The action that is performed on the request after a rule created for the data leakage prevention feature is triggered. Valid values: • *block*: indicates that the request is blocked. • *mask*: indicates that sensitive data is masked. For more information about WAF protection actions, see Description of the action field.	mask
dlp_rule_id	The ID of the rule that is triggered. The rule is created for the data leakage prevention feature.	151245
dlp_test	The protection mode that is used for the request after a rule created for the data leakage prevention feature is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
final_action	The action that WAF performs on the client request. Valid values: • *block*: indicates that the request is blocked. • *captcha_strict*: indicates that strict slider CAPTCHA verification is performed. • *captcha*: indicates that common slider CAPTCHA verification is performed. • *js*: indicates that JavaScript verification is performed. For more information about WAF protection actions, see Description of the action field. If a request does not trigger a protection feature, the field is not recorded. For example, if a request matches a rule that allows the request or a client passes slider CAPTCHA verification or JavaScript verification, the field is not recorded. If a request triggers multiple protection features at the same time, the field is recorded, and the field includes only the action that is performed. The following actions are listed in descending order of priority: block, strict slider CAPTCHA verification, common slider CAPTCHA verification, and JavaScript verification.	block

Field	Description	Sample value
final_plugin	The protection feature that performs the action specified by final_action on the client request. Valid values: • waf: indicates the Protection Rules Engine • deeplearning: indicates the Deep Learning Engine • dlp: indicates data leakage prevention • account: indicates account security • normalized: indicates the positive security model feature • acl: indicates the blacklist or custom protection policy (ACL) feature • cc: indicates the HTTP flood protection and custom protection policy (HTTP Flood Protection) feature • antiscan: indicates the scan protection feature • scene: indicates the scenario-specific configuration feature • antifraud: indicates the data risk control feature • bot_intelligence: indicates the bot threat intelligence feature • algorithm: indicates the typical bot behavior identification feature • wxbb: indicates the app protection feature To configure the preceding protection features, log on to the Web Application Firewall console and choose **Protection Settings > Website Protection** in the left-side navigation pane. For more information about WAF protection features, see Overview of website protection. If a request does not trigger a protection feature, the field is not recorded. For example, if a request matches a rule that allows the request or a client passes slider CAPTCHA verification or JavaScript verification, the field is not recorded. If a request triggers multiple protection features at the same time, the field is recorded, and the field includes only the protection feature that performs the action specified by final_action.	waf
final_rule_id	The ID of the rule that is applied to the client request. The rule defines the action recorded in the final_action field.	115341
final_rule_type	The subtype of the rule that is applied to the client request. The rule is indicated by final_rule_id. For example, `final_plugin:waf` supports `final_rule_type:sqli` and `final_rule_type:xss`.	xss/webshell

Field	Description	Sample value
intelligence_action	The action that is performed on the request after a rule created for the bot threat intelligence feature is triggered. Valid values: • *block*: indicates that the request is blocked. • *captcha_strict*: indicates that strict slider CAPTCHA verification is performed. • *captcha*: indicates that common slider CAPTCHA verification is performed. • *js*: indicates that JavaScript verification is performed. • *captcha_strict_pass*: indicates that the client passes strict slider CAPTCHA verification and WAF allows the request from the client. • *captcha_pass*: indicates that the client passes common slider CAPTCHA verification and WAF allows the request from the client. • *js_pass*: indicates that the client passes JavaScript verification and WAF allows the request from the client. For more information about WAF protection actions, see Description of the action field.	block
intelligence_rule_id	The ID of the rule that is triggered. The rule is created for the bot threat intelligence feature.	152234
intelligence_test	The protection mode that is used for the request after a rule created for the bot threat intelligence feature is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
normalized_action	The action that is performed on the request after a rule created for the positive security model feature is triggered. Valid values: • *block*: indicates that the request is blocked. • *continue*: indicates that the request is allowed. For more information about WAF protection actions, see Description of the action field.	block
normalized_rule_id	The ID of the rule that is triggered. The rule is created for the positive security model feature.	151266
normalized_rule_type	The type of the rule that is triggered. The rule is created for the positive security model feature. Valid values: • *User-Agent*: indicates a User-Agent-based baseline rule. If the User-Agent field of a request header does not conform to the baseline, an attack may occur. This description applies to other rule types. • *Referer*: indicates a Referer-based baseline rule. • *URL*: indicates a URL-based baseline rule. • *Cookie*: indicates a cookie-based baseline rule. • *Body*: indicates a request body-based baseline rule.	User-Agent

Field	Description	Sample value
normalized_test	The protection mode that is used for the request after a rule created for the positive security model feature is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
scene_action	The action that is performed on the request after a rule created for scenario-specific configuration is triggered. Valid values: • *block*: indicates that the request is blocked. • *captcha*: indicates that common slider CAPTCHA verification is performed. • *js*: indicates that JavaScript verification is performed. • *captcha_pass*: indicates that the client passes common slider CAPTCHA verification and WAF allows the request from the client. • *js_pass*: indicates that the client passes JavaScript verification and WAF allows the request from the client. For more information about WAF protection actions, see Description of the action field.	block
scene_id	The protection mode that is used for the request after a rule created for scenario-specific configuration is triggered.	151235
scene_rule_id	The ID of the rule that is triggered. The rule is created for scenario-specific configuration.	153678
scene_rule_type	The type of the rule that is triggered. The rule is created for scenario-specific configuration. Valid values: • *bot_aialgo*: indicates an intelligent protection rule. • *js*: indicates a rule that blocks script-based bots. • *intelligence*: indicates a rule that blocks attacks based on bot threat intelligence or data center blacklists. • *sdk*: indicates a rule that checks for abnormal signatures of SDK-integrated apps and abnormal device behaviors. • *cc*: indicates an IP address-based throttling rule or a custom session-based throttling rule.	bot_aialgo
scene_test	The protection mode that is used for the request after a rule created for scenario-specific configuration is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false

Field	Description	Sample value
waf_action	The action that is performed on the request after a rule created for the Protection Rules Engine is triggered. The value is fixed as *block*, which indicates that WAF blocks the request from the client. For more information about WAF protection actions, see WAF protection actions.	block
waf_rule_id	The ID of the rule that is triggered. The rule is created for the Protection Rules Engine.	113406
waf_rule_type	The type of the rule that is triggered. The rule is created for the Protection Rules Engine. Valid values: • *xss*: indicates a rule that defends against XSS attacks. • *code_exec*: indicates a rule that defends against specific attacks. The attacks exploit code execution vulnerabilities. • *webshell*: indicates a rule that defends against webshell uploads. • *sqli*: indicates a rule that defends against SQL injection. • *lfilei*: indicates a rule that defends against local file inclusion. • *rfilei*: indicates a rule that defends against remote file inclusion. • *crlf*: indicates a rule that defends against CRLF injection. • *other*: indicates other protection rules.	xss
waf_test	The protection mode that is used for the request after a rule created for Protection Rules Engine is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false
wxbb_action	The action that is performed on the request after a rule created for the app protection feature is triggered. Valid values: • *block*: indicates that the request is blocked because the signature fails verification. • *captcha*: indicates that common slider CAPTCHA verification is performed. • *js*: indicates that JavaScript verification is performed. • *continue*: indicates that the request is allowed because the signature passes verification. For more information about WAF protection actions, see Description of the action field.	block

Field	Description	Sample value
wxbb_invalid_wua	The reason why the client request is considered abnormal based on the rule created for the app protection feature. Valid values: • *wxbb_simulator*: indicates that a simulator is used. • *wxbb_proxy*: indicates that a proxy is used. • *wxbb_root*: indicates that a rooted device is used. • *wxbb_hook*: indicates that hooking is used. • *wxbb_antireplay*: indicates that replay attacks by using the signature string *wToken* are detecterd. • *wxbb_virtual*: indicates that multiboxing is configured for Anti-Bot SDK-integrated apps. • *wxbb_debugged*: indicates that the device is in debug mode. • *wxbb_invalid_sign*: indicates that signature verification fails. The following information describes common causes: ◦ A request does not carry a signature. ◦ The parameter passed when a signature is added is different from the parameter received by WAF. For example, the parameter `a=1&b=2` is passed, but the parameter received by WAF is `b=2&a=1`. The content of the passed parameter is not encoded, but the content received by WAF is Base64-encoded.	wxbb_invalid_sign
wxbb_rule_id	The ID of the rule that is triggered. The rule is created for the app protection feature.	156789
wxbb_test	The protection mode that is used for the request after a rule created for the app protection feature is triggered. Valid values: • *true*: indicates the observation mode. In this mode, logs are recorded. However, protection actions, such as block, are not triggered. • *false*: indicates the prevention mode. In this mode, WAF performs protection actions, such as block, on the request that matches the protection rule.	false

Non-protection log fields

Non-protection log fields include request logic fields that WAF obtains from client requests and supplemental fields that are generated after WAF analyzes the requests. The request logic fields include common request header fields. The supplemental fields record request behavior and also record the actual IP addresses of clients and status codes from origin servers.

Field	Description	Sample value
body_bytes_sent	The number of bytes in the request body. Unit: bytes.	1111
content_type	The type of the requested content.	application/x-www-form-urlencoded

Field	Description	Sample value
host	The Host field of the request header, which contains the domain name or IP address to access. The field value is determined by your business settings	api.example.com
http_cookie	The cookie field of the request header, which contains the cookie information about the client.	k1=v1;k2=v2
http_referer	The Referer field of the request header, which contains the source URL information about the request. If the request does not contain the source URL information, the value of the field is displayed as `-`.	http://example.com
http_user_agent	The User-Agent field of the request header. This field contains information about the browser and operating system.	Dalvik/2.1.0 (Linux; U; Android 10; Android SDK built for x86 Build/QSR1.200715.002)
http_x_forwarded_for	The X-Forwarded_For (XFF) field of the request header. This field is used to identify the actual IP address of the client that is connected to the web server by using an HTTP proxy or a load balancing device.	101.XX.XX.120
https	Indicates whether the request is an HTTPS request. Valid values: • *on*: HTTPS request • *off*: HTTP request	on
matched_host	The domain name that is matched by WAF. The domain name is added to WAF for protection. **Note** Wildcard domains can be added to WAF, and WAF matches a wildcard domain. For example, if the domain name *.aliyun.com is added to WAF and www.aliyun.com is requested, WAF matches the domain name *.aliyun.com.	*.aliyun.com
querystring	The query string in the request. The query string refers to the part that follows the question mark (?) in the requested URL.	title=tm_content%3Darticle&pid=123
real_client_ip	The actual IP address of the client that initiates the request. WAF identifies the actual IP address based on the analysis of the request. If WAF cannot identify the actual IP address of the client, the value of the field is displayed as `-`. For example, if a proxy server is used or the IP field in the request header is invalid, WAF cannot identify the actual IP address of the client.	1.XX.XX.1
region	The ID of the region where the WAF instance resides. Valid values: • *cn*: mainland China • *int*: outside mainland China	cn

Field	Description	Sample value
remote_addr	The IP address that is used to connect to WAF. If WAF is directly connected to a client, this field records the actual IP address of the client. If a Layer 7 proxy, such as Content Delivery Network (CDN), is deployed in front of WAF, this field records the IP address of the proxy.	1.XX.XX.1
remote_port	The port that is used to connect to WAF. If WAF is connected to a client, this field records the port of the client. If a Layer 7 proxy, such as CDN, is deployed in front of WAF, this field records the port of the proxy.	80
request_body	The request body.	i am the request body, encrypted or not!
request_length	The number of bytes in the request. The request includes the request line, request header, and request body. Unit: bytes.	111111
request_method	The request method.	GET
request_path	The requested relative path. The relative path refers to the part between the domain name and the question mark (?) in the requested URL. The relative path does not include the query string.	/news/search.php
request_time_msec	The time that WAF takes to process a request. Unit: milliseconds.	44
request_traceid	The unique identifier that is generated by WAF for each request.	7837b1171541038694343700 9ea1f0
server_port	The requested destination port.	443
server_protocol	The protocol and version that the origin server uses to respond to the request forwarded by WAF.	HTTP/1.1
ssl_cipher	The cipher suite that is used in the request.	ECDHE-RSA-AES128-GCM-SHA256
ssl_protocol	The SSL or TLS protocol and version that are used in the request.	TLSv1.2
status	The HTTP status code that WAF sends in response to the request from the client. *Example*: 200, which indicates that the request is received and accepted.	200
time	The point in time at which the request is initiated. The time follows the ISO 8601 standard in the `yyyy-MM-ddTHH:mm:ss+08:00` format. The time must be in UTC.	2018-05-02T16:03:59+08:00
ua_browser	The name of the browser that initiates the request.	ie9

Field	Description	Sample value
ua_browser_family	The family to which the browser that initiates the request belongs.	internet explorer
ua_browser_type	The type of the browser that initiates the request.	web_browser
ua_browser_version	The version of the browser that initiates the request.	9.0
ua_device_type	The device type of the client that initiates the request.	computer
ua_os	The operating system of the client that initiates the request.	windows_7
ua_os_family	The family to which the operating system of the client belongs.	windows
upstream_addr	The IP address and port number of the origin server. The format is `IP address:Port`. Multiple pairs of IP addresses and ports are separated by commas (,).	1.XX.XX.1:443
upstream_response_time	The time that the origin server takes to respond to the request forwarded by WAF. Unit: seconds.	0.044
upstream_status	The HTTP status code that the origin server sends in response to the request from WAF. *Example*: 200, which indicates that the request is received and accepted.	200
user_id	The ID of the Alibaba Cloud account to which the WAF instance belongs.	17045741********

1.4. Quick start

1.4.1. Enable Log Service for WAF

Web Application Firewall (WAF) is integrated with Log Service to provide the Log Service for WAF feature. The feature collects full logs of the websites that are protected by WAF in a near-real-time manner. You can query and analyze the collected log data, and the results are displayed on dashboards. The feature also helps meet the classified protection requirements for your website as well as your requirements for better website operations and protection. This topic describes how to enable the Log Service for WAF feature.

Prerequisites

- A subscription WAF instance that runs the **Pro** edition or higher is purchased.
  For more information, see Purchase a WAF instance.
- The domain names of your website are added to WAF.
  Before you enable the Log Service for WAF feature, we recommend that you add the domain names of your website to WAF. If the domain names are not added to WAF, the feature does not record logs for the domain names. For more information about how to add domain names to WAF, see Tutorial.
- Log Service is activated.
  If you log on to the Log Service console for the first time, you must activate Log Service as prompted.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Log Management > Log Service**.
4. On the **Log Service** page, click **Upgrade** and complete the upgrade as prompted.

   > **Note** If the **Log Service for WAF** feature is enabled when you purchase your WAF instance, skip this step.

   Upgrade procedure:

   i. On the **Upgrade/Downgrade** page, set **Log Service** to YES. Then, specify **Log Storage Size** based on your business requirements.

   For more information about the parameters that are related to the Log Service for WAF feature, see Purchase a WAF instance.

   ii. Click **Buy Now** and complete the payment.

5. Authorize WAF to access the required cloud services.

   WAF needs to access Log Service to store WAF logs and provide the log query and analysis feature. To use the Log Service for WAF feature, you must authorize WAF to access the required cloud services.

   > **Notice** You need only to authorize WAF once. After you authorize WAF, Alibaba Cloud automatically creates the AliyunServiceRoleForWAF service-linked role. This role allows WAF to access the required cloud services. If the role is created, you do not need to authorize WAF again. You can view the service-linked role on the **Roles** page in the RAM console. For more information, see Authorize WAF to access cloud services.

   Authorization procedure:

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

   ii. In the **Tips** message, click **OK**.

After the Log Service for WAF feature is enabled, Log Service automatically creates a dedicated project and a dedicated Logstore for your WAF instance within the same Alibaba Cloud account. This facilitates log data collection. For more information about the default configurations of the dedicated project and Logstore for WAF, see Dedicated project and Logstore for WAF.

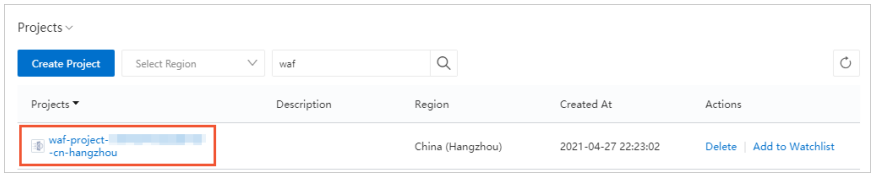
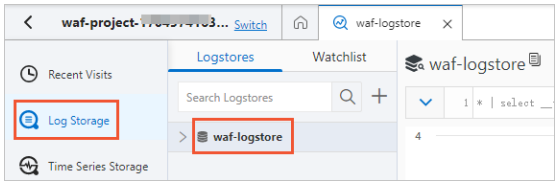
What to do next

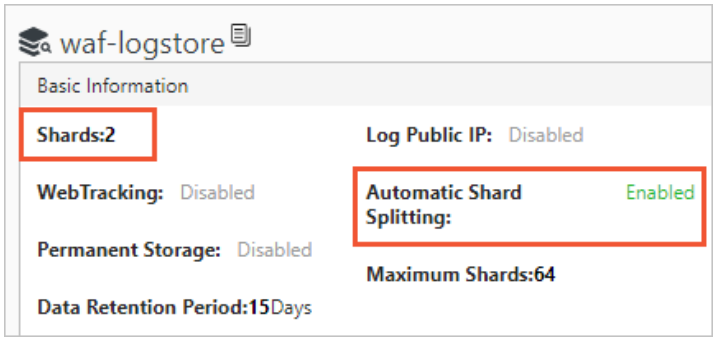
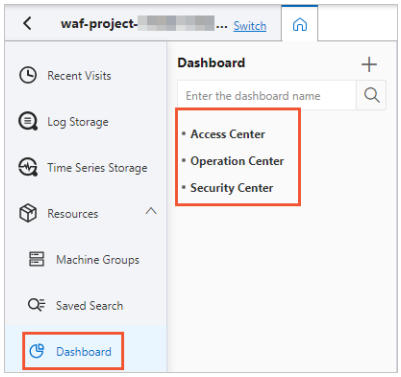
After you enable the Log Service for WAF feature, you must enable log collection for the domain names that you added to WAF. This way, WAF can store the logs of the domain names and provide the log query and analysis feature. For more information about how to enable log collection, see Step 2: Enable the log collection feature.

Dedicated project and Logstore for WAF

The following table describes the default configurations of the dedicated project and Logstore for WAF.

Notice Do not delete or modify the configurations of the default project, Logstore, indexes, or dashboards created by Log Service. Log Service automatically updates and upgrades the log query and analysis feature of WAF on an irregular basis. Log Service also updates the indexes of the dedicated Logstore and the default dashboards for WAF.

Resource type	Description
Project	Log Service automatically creates a dedicated project for WAF. For more information about the project, see Project. Log Service creates the project based on the region of your WAF instance. • For WAF instances in mainland China: The project name is `waf-project-*Alibaba Cloud account ID*-cn-hangzhou`. This project resides in the China (Hangzhou) region. • For WAF instances outside mainland China: The project name is `waf-project-*Alibaba Cloud account ID*-ap-southeast-1`. This project resides in the Singapore (Singapore) region. You can view the dedicated project on the homepage of the Log Service console. If you want to access the project, click the name of the project.  For more information about the project, see Manage a project.
Logstore	A Logstore is automatically created for the dedicated project. For more information about the Logstore, see Logstore. The Logstore name is `waf-logstore`. All logs that are collected by WAF are stored in the Logstore. You can view the Logstore in the dedicated project.  Only WAF logs can be written to the Logstore, and different write methods are supported, such as calling the API or using an SDK. The dedicated Logstore has no limits on features such as queries, statistics, alerting, or streaming consumption. You are not charged for the dedicated Logstore. However, you can use the dedicated Logstore only when Log Service within your Alibaba Cloud account is running as expected. **Note** If Log Service has an overdue payment, the log collection feature of WAF is suspended until you pay the bill. For more information about the Logstore, see 管理Logstore.

Resource type	Description
Shard	By default, the dedicated Logstore contains two shards, and the automatic sharding feature is enabled. You can view the attributes of the shards on the **Logstore Attributes** page.  For more information about the shards, see Manage shards.
Dashboard	By default, the dedicated project contains the following three dashboards: **Operation Center**, **Access Center**, and **Security Center**. For more information, see Dashboards. You can view the dashboards in the dedicated project. For more information about the dashboards, see View dashboards. 

1.4.2. Step 2: Enable the log collection feature

After you enable the Log Service for WAF feature, you can enable log collection for domain names that are added to Web Application Firewall (WAF). After you enable log collection for domain names, the Log Service for WAF feature automatically stores logs of the domain names in the dedicated Logstore for WAF. You can query and analyze the collected log data. This topic describes how to enable log collection for domain names.

Prerequisites

- The Log Service for WAF feature is enabled. For more information, see Enable Log Service for WAF.
- The domain names of your website are added to WAF. For more information, see Tutorial.

Context

Log Service for WAF stores only the logs of the domain names for which log collection is enabled.

After you enable log collection for a domain name, the Log Service for WAF feature automatically stores the logs of the domain name based on the following default configurations.

Default configuration	Modification
By default, the Log Service for WAF feature stores all logs of domain names, including the logs that are generated when WAF allows and blocks requests.	Supported. You can modify the default configuration to store only the logs that are generated when WAF blocks requests.
By default, logs are stored for 180 days.	Supported. You can change the log storage duration. Valid values: 30 to 360. Unit: days. **Notice** You can change the log storage duration for subscription WAF instances that run Business or a higher edition.
By default, WAF logs contain all required fields and some optional fields. For more information, see Log fields supported by WAF.	Supported. You can modify the default configuration to adjust the optional fields that are included in WAF logs.

For more information about how to modify the default configurations, see Modify log settings.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Log Management > Log Service**.
4. Select a domain name from the domain name drop-down list and turn on **Status** to enable log collection for the domain name.

   The domain name drop-down list contains only the domain names that are protected by WAF. If the domain name that you want to select is not added to WAF, add the domain name. For more information, see Tutorial.

   After you enable log collection for the domain name that you select, the Log Service for WAF feature automatically collects the logs of the domain name and stores the logs in the dedicated Logstore. You can repeat the preceding steps to enable log collection for other domain names.

What to do next

After you enable log collection for the domain names, you can query and analyze the collected log data on the **Log Service** page. For more information, see Query and analyze logs.

1.4.3. Query and analyze logs

After you enable log collection for the domain names that are protected by Web Application Firewall (WAF), you can query and analyze the logs of the domain names on the Log Service page in the WAF console. This topic describes how to query and analyze logs on the Log Service page.

Prerequisites

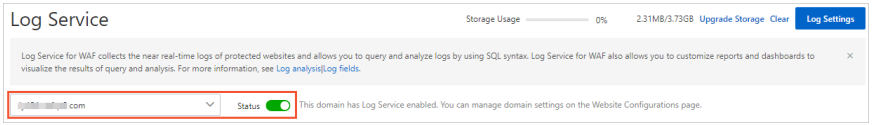
Log collection is enabled for the domain names that are protected by WAF. For more information, see Step 2: Enable the log collection feature.

WAF collects the logs of the domain names only after log collection is enabled for the domain names. This way, you can query and analyze the logs of the domain names.

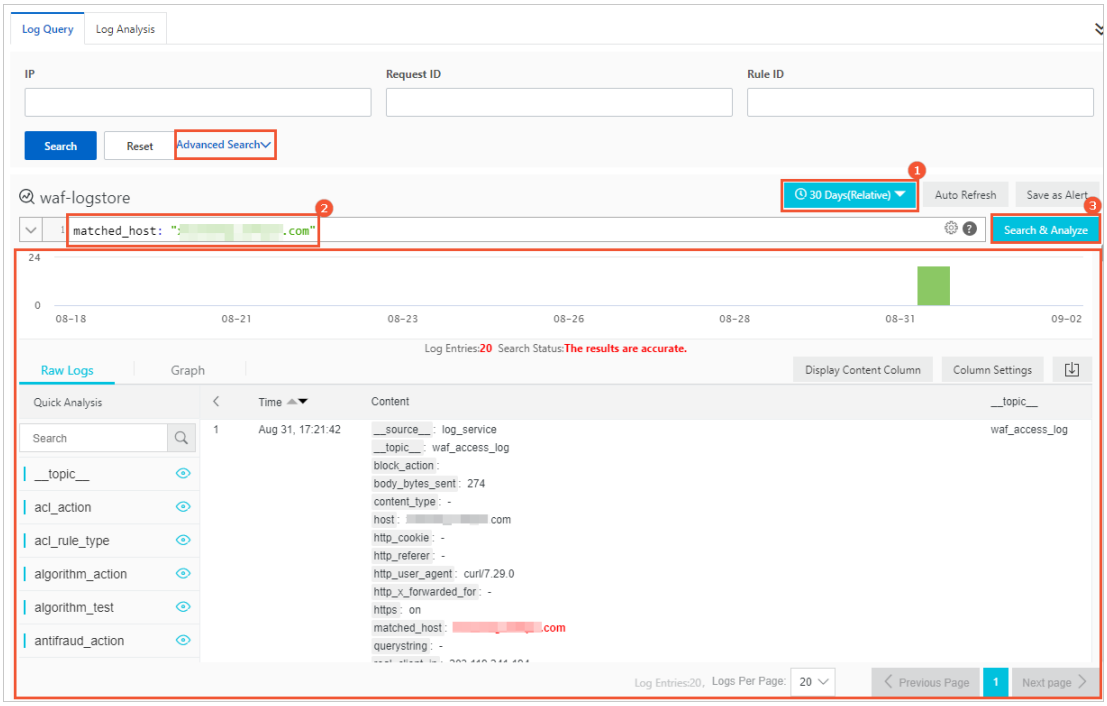
Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Log Management > Log Service**.
4. In the upper section of the **Log Service** page, select the domain name that you want to manage.

> **Notice** Make sure that log collection is enabled for the domain name. Otherwise, WAF does not collect the logs of the domain name, and you cannot query or analyze the logs of the domain name. To enable log collection, turn on **Status**.



5. On the **Log Query** tab, query and analyze the logs of the selected domain name.

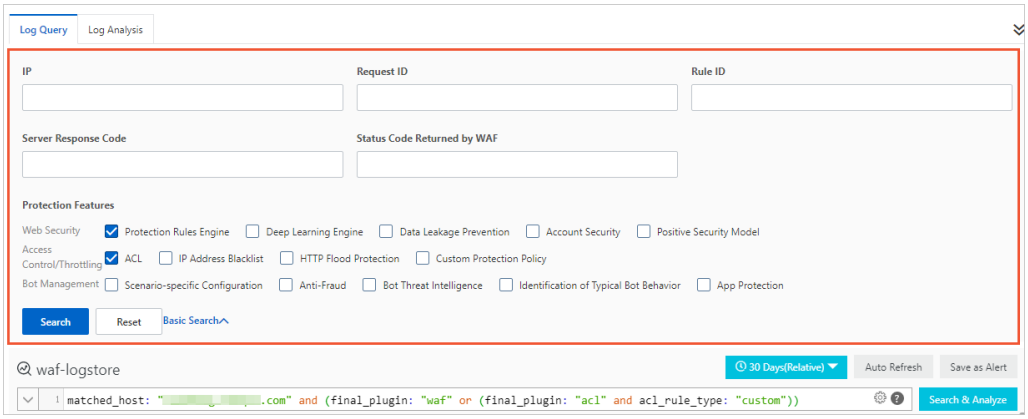


To query and analyze the logs, perform the following steps:

i. Specify the query time range by using the time selector.

ii. Enter a query statement in the search box.

Query statements use the syntax that is specific to Alibaba Cloud Log Service. For more information about the syntax, see 查询语法. The log fields that are included in WAF logs are used as query fields in the query statements. For more information about the log fields that are supported by WAF, see Log fields supported by WAF.
If you do not know the query syntax, we recommend that you use **Advanced Search**. You need only to expand **Advanced Search** above the search box, specify search conditions, and click **Search**. The query statement is automatically generated based on the search conditions in the search box.



The following table describes the search conditions that are supported by Advanced Search.

Search condition	Description
IP	The IP address of the client that sends the request.
Trace ID	The unique ID that is generated by WAF for each request. This ID is provided when WAF returns an error page or a response page that prompts the client to complete slider CAPTCHA verification to the client. You can use this ID to analyze and troubleshoot the error.
Rule ID	The ID of the WAF protection rule that is matched by the request. You can obtain the ID on the **Security Report** page or by choosing **System Management > Protection Rule Group**.
Server Response Code	The HTTP status code that is sent by the origin server as a response to the request forwarded by WAF.
Status Code Returned by WAF	The HTTP status code that is sent by WAF as a response to the request sent by the client.
Protection Features	The type of the WAF protection rule that is matched by the request. For more information about WAF protection rules and their configuration methods, see Overview.

iii. If you want to compute and analyze the query results, you must enter an analytic statement following the search statement in the search box. Otherwise, skip this step.

Analytic statements and search statements are separated by vertical bars (|). The analytic statements use the standard SQL-92 syntax. For more information about the analytic statements, see Log analysis overview.

iv. Click the **Search & Analysis** button.
In the lower section of the page, the query result is displayed in a log distribution histogram and on the **Raw Logs** and **Graph** tabs. You can use the query result to perform additional operations, such as quick analysis, statistical analysis, and alert configuration. For more information, see Manage the query results.

For more information about the examples of log query and analysis, see Query logs.

6. On the **Log Analysis** tab, view the dashboards that are preconfigured by WAF based on log data.

   The dashboards provide a series of charts that are generated based on log data. This way, you can directly view the service and security data of your website. WAF provides the following three preconfigured dashboards:

   - **Operation Center**: displays the service operations metrics of your website, including the request trend and overview of attacks.
   - **Access Center**: displays the access information of your website, such as the access metrics, client distribution, traffic, and performance.
   - **Security Center**: displays the attack information of your website, such as attack metrics, attack trends, and attack source distribution.

   You need only to specify the query time range to search for specific dashboards. You can also subscribe to dashboards to receive dashboard data by using different methods, such as emails or DingTalk messages. For more information about the chart data that is displayed on dashboards and how to subscribe to dashboards, see View dashboards.

Related operations

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

For more information about how to perform query and analysis, see Query logs.

For more information about how to modify the settings of WAF logs, such as storage rules and storage capacity, see Modify log settings.

1.5. Log application tutorial

1.5.1. Query logs

After you enable the log collection feature for the domain names that are added to WAF, you can use the log query feature to query and analyze the logs that are collected in real time. You can configure charts and create alert rules based on the query and analysis results.

Prerequisites

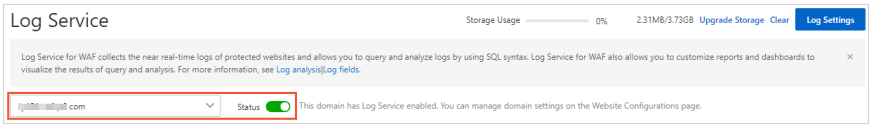
- The Log Service for WAF feature is enabled. For more information, see Enable Log Service for WAF.
- Log collection is enabled for the domain names that are added to WAF. For more information, see Step 2: Enable the log collection feature.

Query and analyze logs

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Log Management > Log Service**.

4. In the upper section of the **Log Service** page, select the domain name that you want to manage.

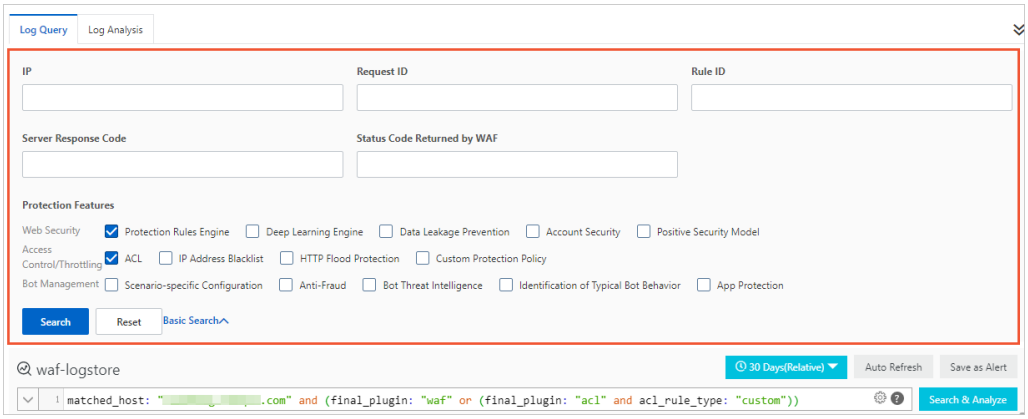
> **Notice** Make sure that log collection is enabled for the domain name. Otherwise, WAF does not collect the logs of the domain name, and you cannot query or analyze the logs of the domain name. To enable log collection, turn on **Status**.



5. On the **Log Query** tab, execute a query statement to query and analyze WAF logs.
   i. Specify the query time range by using the time selector.

ii. Enter a query statement in the search box.

Query statements use the syntax that is specific to Alibaba Cloud Log Service. For more information about the syntax, see 查询语法. The log fields that are included in WAF logs are used as query fields in the query statements. For more information about the log fields that are supported by WAF, see Log fields supported by WAF.
If you do not know the query syntax, we recommend that you use **Advanced Search**. You need only to expand **Advanced Search** above the search box, specify search conditions, and click **Search**. The query statement is automatically generated based on the search conditions in the search box.



The following table describes the search conditions that are supported by Advanced Search.

Search condition	Description
IP	The IP address of the client that sends the request.
Trace ID	The unique ID that is generated by WAF for each request. This ID is provided when WAF returns an error page or a response page that prompts the client to complete slider CAPTCHA verification to the client. You can use this ID to analyze and troubleshoot the error.
Rule ID	The ID of the WAF protection rule that is matched by the request. You can obtain the ID on the **Security Report** page or by choosing **System Management > Protection Rule Group**.
Server Response Code	The HTTP status code that is sent by the origin server as a response to the request forwarded by WAF.
Status Code Returned by WAF	The HTTP status code that is sent by WAF as a response to the request sent by the client.
Protection Features	The type of the WAF protection rule that is matched by the request. For more information about WAF protection rules and their configuration methods, see Overview.

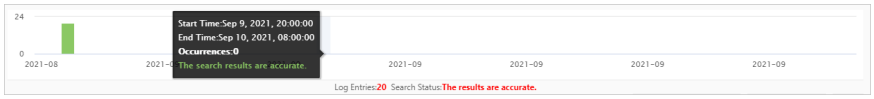
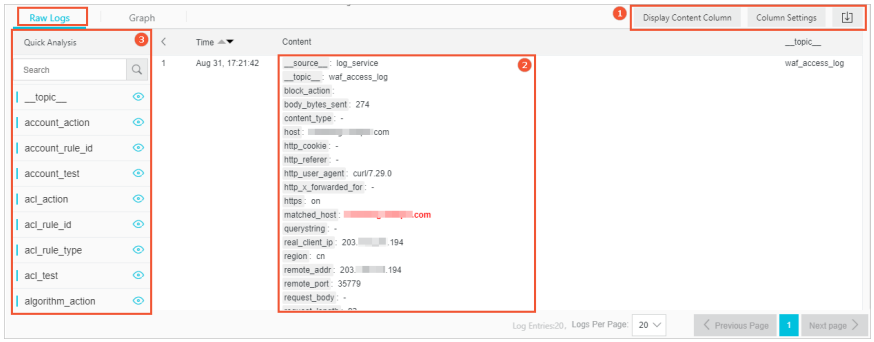
iii. If you want to compute and analyze the query results, you must enter an analytic statement following the search statement in the search box. Otherwise, skip this step.

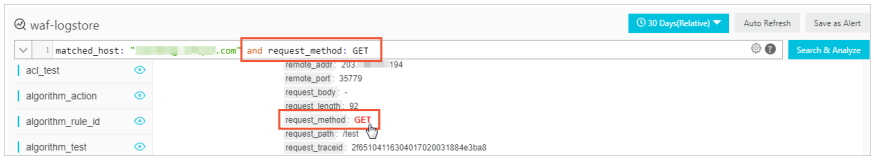
Analytic statements and search statements are separated by vertical bars (|). The analytic statements use the standard SQL-92 syntax. For more information about the analytic statements, see Log analysis overview.

iv. Click **Search & Analyze**.
In the lower section of the page, you can view the query and analysis results in a log distribution histogram and on the **Raw Logs** and **Graph** tabs. You can perform various operations based on the query and analysis results. For example, you can perform quick analysis, configure charts, and create alert rules. For more information, see Perform operations on query and analysis results and Create alert rules.

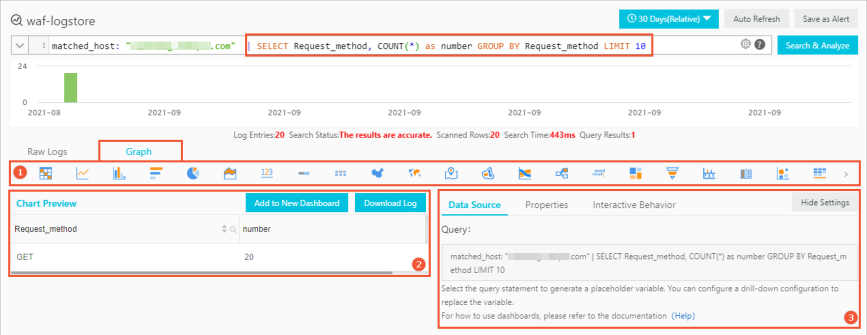
For more information about query statements, see Query and analysis examples.

Perform operations on query and analysis results

Result type	Description
Log distribution histogram	The log distribution histogram is located below the search box and displays the distribution of returned log data by time.  In this section, you can perform the following operations: • Move the pointer over a green rectangle to view the time range during which the log data is generated and the number of logs that are recorded within the time range. • Click a green rectangle to view the log distribution histogram within the specified time range during which the log data is generated.
	The **Raw Logs** tab is located below the log distribution histogram and displays the details about each log by page. The details include the information about fields in the log. The fields are in the key:value format.  In Section 1 of the Raw Logs tab, you can perform the following operations: • **Display Content Column**: You can modify the display mode of the **Content** column in raw logs. For example, you can determine whether to display content in multiple lines, hide the default fields, expand the default levels of JSON, and fold long strings. • **Column Settings**: By default, raw logs display only the **Content** column. If you want to display specified fields in a column, you can click **Column Settings** to configure the specified fields. • Download: You can click the  icon to download logs to your computer. **Download Log in Current Page**, **Download All Logs with Cloud Shell**, and **Download All Logs Using Command Line Tool** are supported. For more information, see Download logs.

Result type	Description
Raw Logs	In Section 2 of the Raw Logs tab, you can query logs based on fields in raw logs. Click the value of a field in the **Content** column to query the logs that contain the field. For example, if you click GET of `request_method: GET`, `and request_method: GET` is automatically appended to the original query statement in the search box. This way, the system queries the results of the original query statement for the logs whose `request_method` is `GET` and returns the logs.  In the **Quick Analysis** section (Section 3) of the Raw Logs tab, you can perform the following operations: You can analyze the distribution of a field over a specified period of time. This helps reduce the time that is required to index critical data. 1. Click the  icon to the right of a field to analyze the distribution of field values. The top 10 values with the most log entries are displayed. For example, if you click the  icon to the right of the `ua_browser` field, the top 10 types of browsers are displayed. 2. Click the  icon to add the analytic statement that is last used to the search box. Then, you are redirected to the **Graph** tab on which you can view charts on analysis results. If the total number of values for a field exceeds 10, you can click **Count Distinct Values** to measure the number of distinct values. For more information about quick analysis, see Quick analysis.

Result type	Description

Graph	The **Graph** tab is located below the log distribution histogram and displays the query and analysis results in charts. To view charts on the **Graph** tab, you must enter an analytic statement that uses the standard SQL-92 syntax in the search box.
	 
	On the Graph tab, you can perform the following operations:
	• Change the chart type in Section 1: Select a chart type based on your business requirements to view the query and analysis results. For more information, see Chart configurations.
	• Preview a chart in Section 2: Preview the chart after you change the chart type. Click **Add to Dashboard** to add the current chart to the dashboard. Click **Download Log** to download logs to your computer. **Download Log in Current Page**, **Download All Logs with Cloud Shell**, and **Download All Logs Using Command Line Tool** are supported. For more information, see Download logs.
	• Modify the settings of a chart in Section 3:
	  ○ On the **Properties** tab, you can set the properties of a chart to be displayed. You can set the X-axis, left Y-axis and right Y-axis, margins, font size, and other parameters. Different types of charts have different properties. This feature is applicable to all query scenarios.
	  ○ On the **Data Source** tab, you can set placeholder variables. For example, you can configure the drill-down event of Chart A to redirect to the dashboard on which Chart B is located. After you configure the drill-down event of Chart A, the placeholder variable is replaced by the variable that you click to trigger the drill-down event and execute the query statement of Chart B. This way, to trigger the drill-down event, you must click the placeholder variable that you configured for Chart B. This feature is applicable to scenarios where you need to configure drill-down events to redirect to destination dashboards. For more information, see Configure a drill-down event for a chart.
	  ○ On the **Interactive Behavior** tab, you can configure drill-down events for a chart. Then, you can click the variable value in the chart to trigger the specified drill-down event. This feature applies when you need to trigger drill-down events for charts. For more information, see Configure a drill-down event for a chart.
	For more information, see Chart overview.

Create alert rules

You can create alert rules based on the current query statement. After you create an alert rule, Log Service checks related query and analysis results on a regular basis. If a query and analysis result meets the trigger condition that you specify in the alert rule, Log Service sends an alert notification. This way, the service status is monitored in real time.

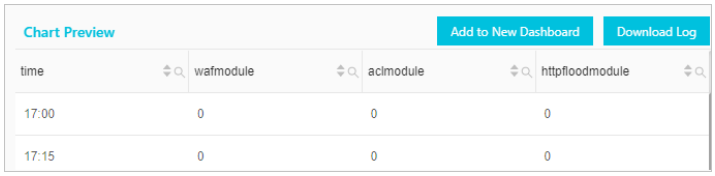
To create an alert rule, you must click **Save as Alert** in the upper-right corner above the search box and complete the **Create Alert** wizard. For more information, see Configure an alert rule.

Query and analysis examples

- Query the number of requests blocked by different WAF protection features every quarter hour. The results include the attack time (time), the numbers of requests blocked by Protection Rules Engine (wafmodule), requests blocked by the IP address blacklist and custom protection policies (aclmodule), and requests blocked by HTTP flood protection and custom protection policies (httpfloodmodule).

```
* |
SELECT
 time_series(__time__, '15m', '%H:%i', '0') as time,
 COUNT_if(final_plugin = 'waf') as "wafmodule",
 COUNT_if(final_plugin = 'acl') as "aclmodule",
 COUNT_if(final_plugin = 'cc') as "httpfloodmodule"
GROUP by
 time
ORDER by
 time
```

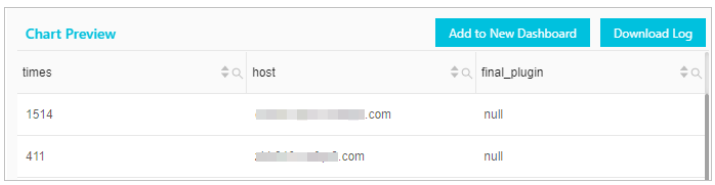
  The following chart displays the results.



- Query the distribution of protection features (final_plugin) that are triggered. The results include the number of times (times) that protection features that are triggered, requested domain names (host), and protection features (final_plugin).

```
* |
SELECT
 count(*) as times,
 host,
 final_plugin
GROUP by
 host,
 final_plugin
ORDER by
 times desc
```

  The following chart displays the results.

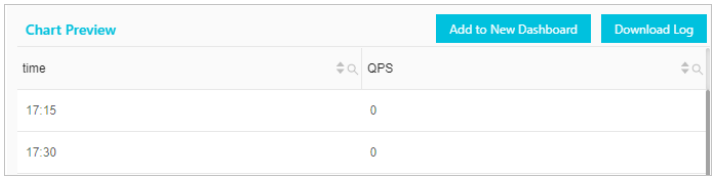


- Query the queries per second (QPS) every quarter hour. The results include the time (time) and QPS

(QPS).

```
* |
SELECT
 time_series(__time__, '15m', '%H:%i', '0') as time,
 count(*) / 900 as QPS
GROUP by
 time
ORDER by
 time
```

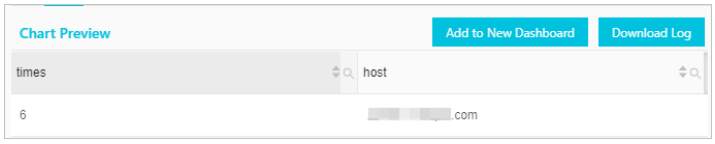
The following chart displays the results.



- Query the domain names that suffer the most HTTP flood attacks. The results include the number of times (times) that HTTP flood attacks are blocked and the targeted domain names (host).

```
*
and acl_action :block |
SELECT
 count(*) as times,
 host
GROUP by
 host
ORDER by
 times desc
```

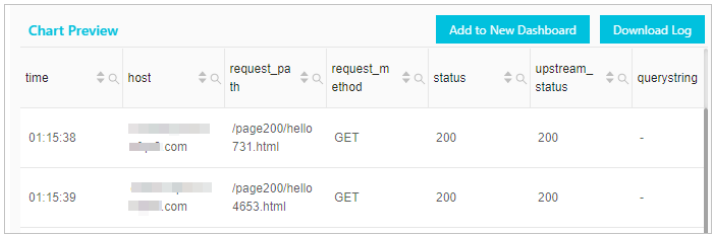
The following chart displays the results.



- Query the log details about requests every second. The results include the request time (time), accessed domain name (host), request path (request_path), request method (request_method), HTTP status code (status) that WAF responds, HTTP status code (upstream_status) that the origin server responds, and query string (querystring).

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

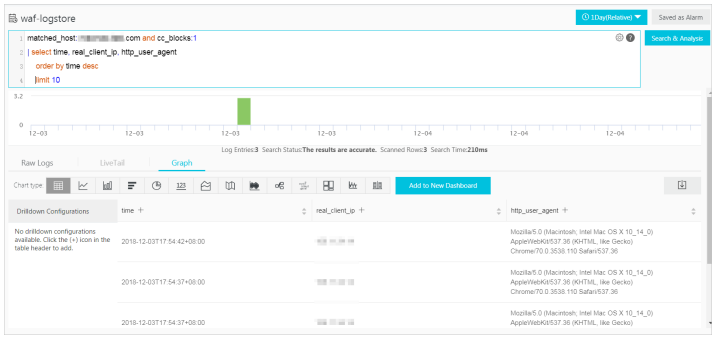
The following chart displays the results.



- Query the latest 10 attacks on the *your_domain_name* website. The results include the attack time (time), actual IP address of the client, (real_client_ip), and client type (http_user_agent).

```
matched_host: your_domain_name
and final_action: block |
SELECT
 time,
 real_client_ip,
 http_user_agent
ORDER by
 time desc
LIMIT
 10
```

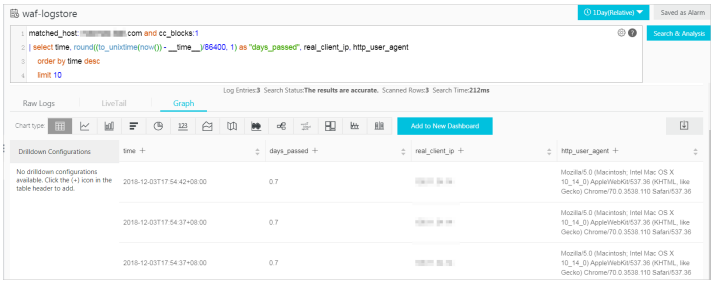
The following chart displays the results.



- Query the number of days (days_passed) that elapsed after an attack on the *your_domain_name* website was blocked by WAF. The value of days_passed is rounded to one decimal place.

```
matched_host: your_domain_name
and final_action: block |
SELECT
 time,
 round((to_unixtime(now())-__time__) / 86400, 1) as "days_passed",
 real_client_ip,
 http_user_agent
ORDER by
 time desc
LIMIT
 10
```

The following chart displays the results.



- Query the trend of the number of attacks on the *your_domain_name* website by day.

```
matched_host: your_domain_name
and final_action: block |
SELECT
 date_trunc('day', __time__) as dt,
 count(1) as PV
GROUP by
 dt
ORDER by
 dt
```

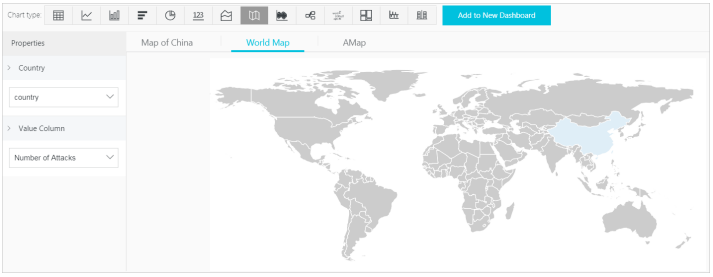
The date_trunc function is used to group the times when attacks occurred by day. For more information about the function, see 日期和时间函数.
The following chart displays the results. We recommend that you use a line chart to display the results.

dt	PV
2018-12-03 00:00:00.000	3

- Query the distribution of countries from which attacks are launched to the *your_domain_name* website.

```
matched_host: your_domain_name
and final_action: block |
SELECT
 ip_to_country(
  if(real_client_ip = '-', remote_addr, real_client_ip)
 ) as country,
 count(1) as "Number of attacks"
GROUP by
 country
```

The `real_client_ip` field in WAF logs indicates the actual IP address of a client. If a proxy server is used or the IP field in a request header is invalid, the actual IP address of the client cannot be obtained. In this case, the value of the `real_client_ip` field is displayed as `-`. You can use the value of the `remote_addr` field as the actual IP address of the client. The remote_addr field indicates the IP address that is used to connect to WAF.
The following chart displays the results. We recommend that you use the world map to display the results.



- Query the distribution of provinces from which attacks are launched to the *your_domain_name* website.

```
matched_host: your_domain_name
and final_action: block |
SELECT
 ip_to_province(
  if(real_client_ip = '-', remote_addr, real_client_ip)
 ) as province,
 count(1) as "Number of attacks"
GROUP by
 province
```

The ip_to_province function is used to obtain information about the provinces in which the actual IP addresses of clients are located. For more information about the function, see IP functions.
The following chart displays the results. If all IP addresses from which attacks are launched are located inside China, we recommend that you use the China map to display the results.

1.5.2. View dashboards

Web Application Firewall (WAF) provides dashboards that display log query and analysis results in charts. Log Service for WAF provides Operation Center, Access Center, and Security Center dashboards based on common service and query scenarios. You can view the service and security data of your website on the dashboards by simply specifying a time range. You do not need to enter a query statement.

Prerequisites

- The Log Service for WAF feature is enabled. For more information, see Enable Log Service for WAF.
- The log collection feature is enabled for the domain names of your website that is protected by WAF. For more information, see Step 2: Enable the log collection feature.

Context

Log Service for WAF provides dashboards for real-time data analysis. You can view multiple charts that are generated based on query and analysis results on a dashboard. After the Log Service for WAF feature and the log collection feature are enabled, you can view the service and security data of your website on the following dashboards, which are predefined by WAF.

Dashboard	Description
Operation Center	Displays the overall situation of the website, such as traffic protection data and overview of attacks.
Access Center	Displays the access information of the website, such as access metrics, access trends, and request distribution.
Security Center	Displays the attack information of the website, such as attack targets, attack trends, and distribution of attack sources.

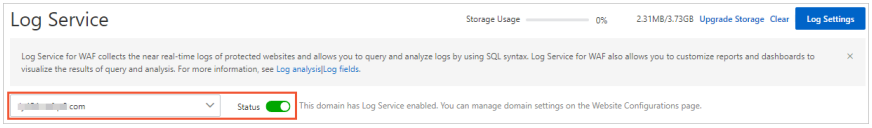
A dashboard consists of multiple charts. For more information about the charts that are supported by WAF, see Charts supported by dashboards.

You can also manually create dashboards based on service-related query and analysis scenarios. You can add custom charts to the dashboards based on your commonly used query statements. For more information, see Overview.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Log Management > Log Service**.
4. In the upper section of the **Log Service** page, select the domain name that you want to manage.

   > **Notice** Make sure that log collection is enabled for the domain name. Otherwise, WAF does not collect the logs of the domain name, and you cannot query or analyze the logs of the domain name. To enable log collection, turn on **Status**.

5. Click the **Log Analysis** tab.
6. Click the dashboard that you want to view and specify a time range in which you want to query the data. You can click the **Operation Center**, **Access Center**, or **Security Center** tab.

   For more information about chart types that are supported by different dashboards, see Charts supported by dashboards.
   For more information about common operations that are supported by dashboards, see What to do next.

What to do next

Operation	Object	Description

Operation	Object	Description
Specify a time range by using a time selector	Dashboard and chart	Each dashboard contains multiple charts. The charts are generated based on raw log data within a specific time range. You can configure a time selector to specify the time range. Time selectors are classified into the following types: • Dashboard time selector: applies to all charts on a dashboard. If you select a time range by using a dashboard time selector, all charts on the dashboard display results based on the selected time range. A dashboard time selector is located in the upper right corner of the dashboard. By default, no time ranges are specified each time you open the **Log Analysis** tab. The time selector displays **Please Select**. You can click **Please Select**. Then, you can select a time range for all charts in the **Time** panel. You can select a relative time or a time frame. You can also specify a custom time range. **Note** The time range setting applies only to the current dashboard. If you switch to another dashboard, you must specify a time range for the dashboard again. • Chart time selector: applies only to a chart on a dashboard. Find a chart, move the pointer over the ⋮ icon in the upper-right corner of the chart, and then select **Select Time Range**. In the **Time** panel, you can select a time range for the chart.
Subscribe to a dashboard	Dashboard	You can subscribe to a dashboard. After you subscribe to the dashboard, the chart data on the dashboard is automatically sent to specified recipients by using emails or DingTalk group messages on a regular basis. In the upper-right corner of a dashboard, click **Subscribe** and complete the **Create Subscription** wizard to subscribe to the current dashboard. For more information, see Subscribe to a dashboard.

Operation	Object	Description
Drill down into data across charts	Chart	By default, drill-down is configured for some charts. This allows you to view underlying data details. Find a chart, move the pointer over the icon in the upper right corner of the chart, and then check whether the  icon is displayed. If the icon is displayed, drill-down is configured for the chart. You can click an underscored number in a chart for which drill-down is configured to view underlying data details. For example, you can identify the domain names that are attacked and the number of attacks after you click the underscored number in the **Attacked Hosts** chart of the **Security Center** dashboard. **Note** You can also switch to the **Raw Logs** tab to view the raw log data. For more information, see Configure a drill-down event for a chart.
Download logs	Chart	Find a chart, move the pointer over the icon in the upper right corner of the chart, and then select **Download Log** to download the data of the chart to your computer as a CSV file.
Preview the query statement of a chart	Chart	Find a chart, move the pointer over the icon in the upper right corner of the chart, and then select the  icon to preview the query statement that is used for the chart.

Charts supported by dashboards

Log Service of WAF provides Operation Center, Access Center, and Security Center dashboards, which display the operations situation, access information, and attack details of a website. Different dashboards provide different charts.

- **Operation Center**: displays the overall situation of a website, such as traffic protection data and overview of attacks.

Chart name	Chart type	Default time range	Description	Example value
User Request	Single value chart	Compared with last day	Displays the numbers of page views (PVs) and unique visitors (UVs).	48,300

Chart name	Chart type	Default time range	Description	Example value
Peak Traffic	Single value chart	Compared with last day	Displays the peak inbound and outbound traffic over the Internet and the peak attack traffic. Unit: Kbit/s.	4.6
Valid Request Ratio	Single value chart	Compared with last hour	Displays the percentage of valid requests that are routed over the Internet and forwarded by WAF.	98.41%
Valid Traffic	Single value chart	Compared with last hour	Displays the amount of network traffic that is forwarded by WAF to the origin server. Unit: MB.	10.7
Request Trend	Line chart	1 week (relative)	Displays the trends in the number of requests, the ratio of valid requests, and the inbound and outbound network bandwidths in Kbit/s.	None
Attack Statistics	Single-value chart, world map, and China map	Compared with last hour	Displays the number of attacks, traffic amount in KB, and attack distribution on the world map and China map.	None
Attacker List	Table	1 hour (relative)	Displays the list of IP addresses from which attacks are launched.	None
Top 100 Attacked Websites	Table	1 hour (relative)	Displays the top 100 domain names that suffered the most attacks.	None

- **Access Center**: displays access information of a website, such as access metrics, access trends, and request distribution.

Chart name	Chart type	Default time range	Description	Example value
PV	Single value chart	1 hour (relative)	Displays the total number of PVs.	100,000
UV	Single value chart	1 hour (relative)	Displays the total number of UVs.	100
Traffic In	Single value chart	1 hour (relative)	Displays the total amount of inbound traffic. Unit: MB.	300 MB

Chart name	Chart type	Default time range	Description	Example value
Peak Network In Traffic	Single value chart	Today (time frame)	Displays the peak rate of inbound traffic. Unit: Kbit/s.	0.5 KB/s
Peak Network Out Traffic	Single value chart	Today (time frame)	Displays the peak rate of outbound traffic. Unit: Kbit/s.	1.3 KB/s
Traffic Network Trend	Area chart	Today (time frame)	Displays the trends of inbound and outbound traffic. Unit: Kbit/s.	None
PV/UV Trends	Line chart	Today (time frame)	Displays the trends of PVs and UVs.	None
Access Status Distribution	Flow chart	Today (time frame)	Displays the trends of requests with different status codes such as 400, 304, and 200. Unit: count/h.	None
Access Source	World map	1 hour (relative)	Displays the distribution of requests by country.	None
Traffic In Source (World)	World map	1 hour (relative)	Displays the distribution of inbound traffic by country.	None
Traffic In Source (China)	China map	1 hour (relative)	Displays the distribution of inbound traffic by province in China.	None
Access Heatmap	AMAP	1 hour (relative)	Displays the heat map that indicates the source distribution of requests by geographical location.	None
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.	None

Chart name	Chart type	Default time range	Description	Example value
Referer	Table	1 hour (relative)	Displays the information about the top 100 Referers that are most frequently forwarded. The information includes Referer URLs, Referer hosts, and the number of times that the Referer is detected.	None
Mobile Client Distribution	Pie chart	1 hour (relative)	Displays the distribution of requests from mobile clients by client type.	None
PC Client Distribution	Pie chart	1 hour (relative)	Displays the distribution of requests from PC clients by client type.	None
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.	None
Accessed Sites	Treemap chart	1 hour (relative)	Displays the top 30 domain names that are most frequently accessed.	None
Top Clients	Table	1 hour (relative)	Displays the information about the top 100 clients that visit your domain names most. The information includes the client IP address, region and city, network information, request method, inbound traffic, number of access errors, and number of attacks.	None
URL With Slowest Response	Table	1 hour (relative)	Displays the information about the top 100 URLs with long response time. The information includes the domain name, URL, average response time, and number of access requests.	None

- **Security Center**: displays attack information of a website, such as attack targets, attack trends, and distribution of attack sources

Chart name	Chart type	Default time range	Description	Example value
Peak Attack Size	Single value chart	1 hour (relative)	Displays the peak attack traffic. Unit: bit/s.	100 Bps
Attacked Hosts	Single value chart	Today (time frame)	Displays the number of websites that are attacked.	3
Source Country Of Attack	Single value chart	Today (time frame)	Displays the number of countries from which attacks are launched.	2
Attack Traffic	Single value chart	1 hour (relative)	Displays the total amount of traffic that is generated by attacks. Unit: bytes.	1 B
Attacker UV	Single value chart	1 hour (relative)	Displays the number of UVs.	40
Attack type distribution	Flow chart	Today (time frame)	Displays the distribution of attacks by attack type.	None
Intercepted Attack	Single value chart	1 hour (relative)	Displays the total number of attacks that are blocked by WAF.	100
CC Attack Interception	Single value chart	1 hour (relative)	Displays the number of HTTP flood attacks that are blocked by WAF.	10
Web Attack Interception	Single value chart	1 hour (relative)	Displays the number of web application attacks that are blocked by WAF.	80
Access Control Event	Single value chart	1 hour (relative)	Displays the number of requests that are blocked by custom protection policies (ACL policies) of WAF.	10
CC Attack (World)	World map	1 hour (relative)	Displays the distribution of HTTP flood attacks by country.	None
CC Attack (China)	China map	1 hour (relative)	Displays the distribution of HTTP flood attacks by province in China.	None
Web Attack (World)	World map	1 hour (relative)	Displays the distribution of web application attacks by country.	None

Chart name	Chart type	Default time range	Description	Example value
Web Attack (China)	China map	1 hour (relative)	Displays the distribution of web application attacks by province in China.	None
Access Control Attack (World)	World map	1 hour (relative)	Displays the distribution of requests that are blocked by custom protection policies (ACL policies) by country.	None
Access Control Attack (China)	China map	1 hour (relative)	Displays the distribution of requests that are blocked by custom protection policies (ACL policies) by province in China.	None
Attacked Hosts	Treemap chart	1 hour (relative)	Displays the websites that are most frequently attacked.	None
CC Attack Strategy Distribution	Pie chart	1 hour (relative)	Displays the distribution of attacks that trigger HTTP flood protection policies.	None
Web Attack Type Distribution	Pie chart	1 hour (relative)	Displays the distribution of web attacks by attack type.	None
Top Attackers	Table	1 hour (relative)	Displays the IP addresses, province information, and carriers of the first 100 clients that launch the most recent attacks. It also displays the number of attacks for each attack type and the amount of traffic generated by these attacks.	None
Attacker Referer	Table	1 hour (relative)	Displays the Referer information of attacks, including Referer URLs, Referer hosts, and the number of times that the Referer is detected.	None

For more information, see Chart overview.

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

A RAM user can query and analyze logs in Web Application Firewall (WAF) only after it is granted the required permissions by using an Alibaba Cloud account.

Context

The following table describes the types of operations and the accounts that are required to perform the operations.

Operation	Required account
Activate Log Service. You need only 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 need only to perform this operation once.	• Alibaba Cloud accounts • RAM users that have the `AliyunLogFullAccess` permission • RAM users that have specific permissions
Query and analyze logs.	• 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 the operation permissions on Log Service to RAM users.	`AliyunLogFullAccess`	For more information about how to grant permissions, see Grant permissions to a RAM user.
Grant the permissions to view logs to RAM users after you use your Alibaba Cloud account to enable Log Service for WAF and authorize WAF to access the required cloud resources.	`AliyunLogReadOnlyAccess`	For more information about how to grant permissions, see Grant permissions to a RAM user.
Grant only the permissions to enable and use Log Service for WAF to RAM users. The RAM users are not granted other management permissions on Log Service.	Permissions that are defined in a custom policy	For more information about how to create a custom policy, see the following procedure.

Procedure

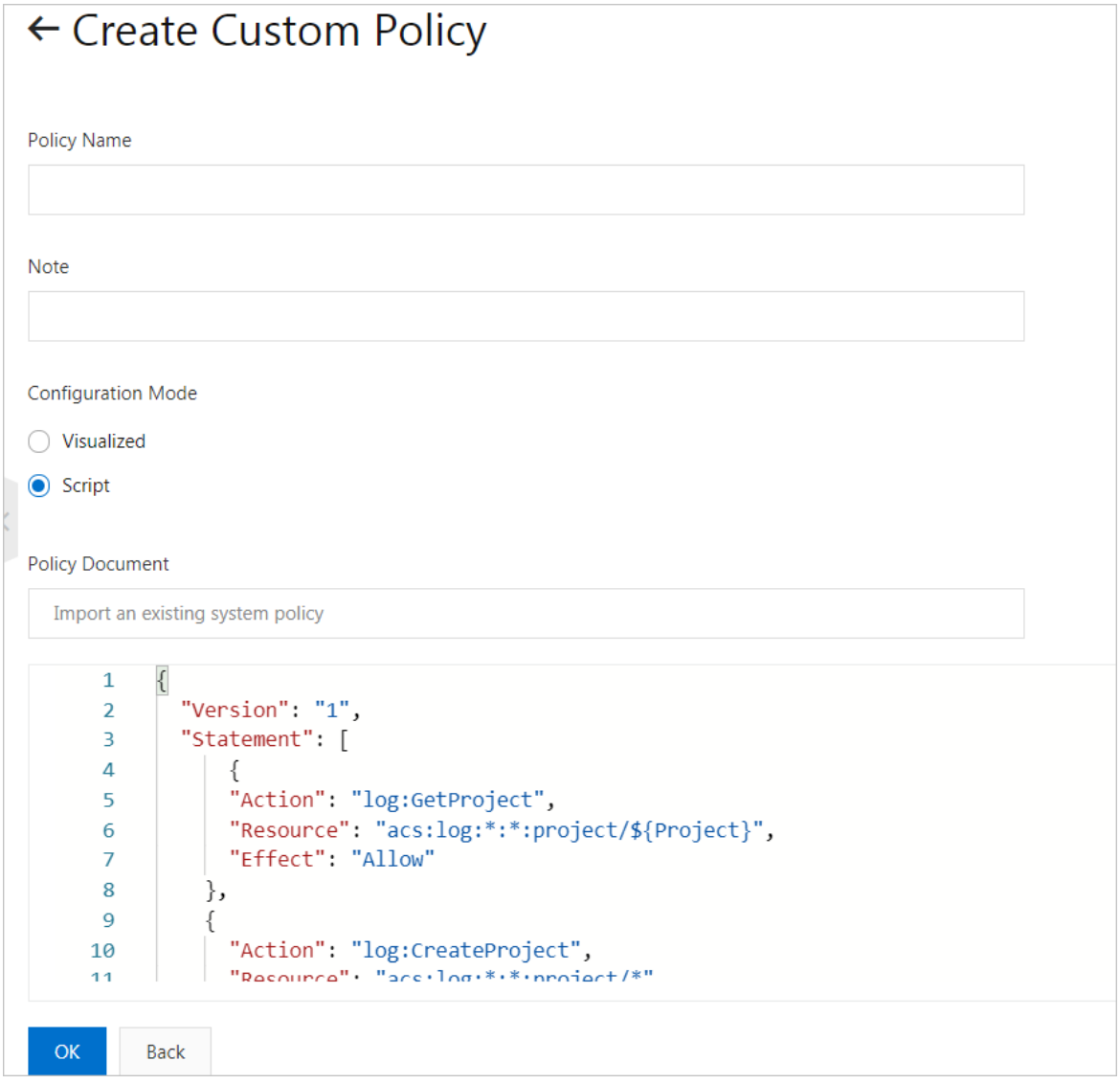
1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.

3. On the **Policies** page, 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.

> **Notice** Replace `${Project}` and `${Logstore}` in the following policy content with the names of the Log Service project and Logstore that are dedicated to 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 page that appears, find the RAM user that you want to authorize and click **Add Permissions** in the Actions column.
8. In the Add Permissions panel, select the custom policy that you create, and click **OK**.
   After the RAM user is authorized, the RAM user can enable and use Log Service for WAF. However, the

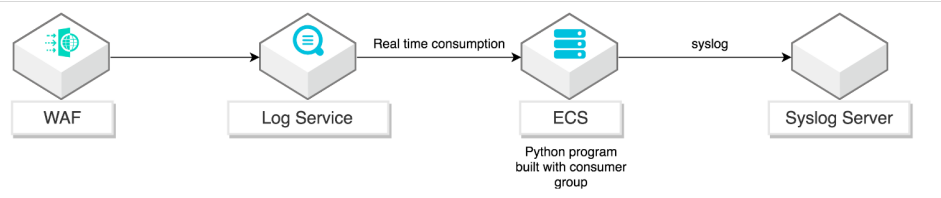
RAM user cannot use other features of Log Service.

1.5.4. 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.



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
  - Step 2: Enable the log collection feature
- 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.

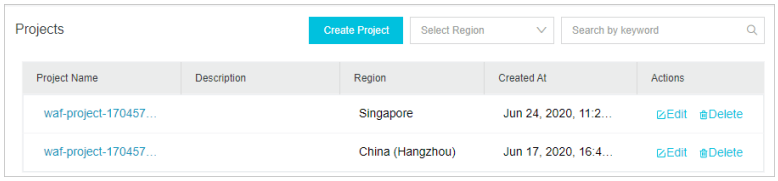
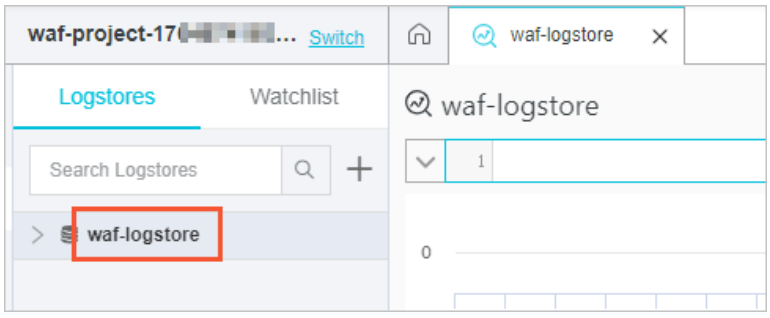
2. Install Python 3, pip, and aliyun-log-python-sdk. For more information about Log Service SDK for Python, see User Guide.

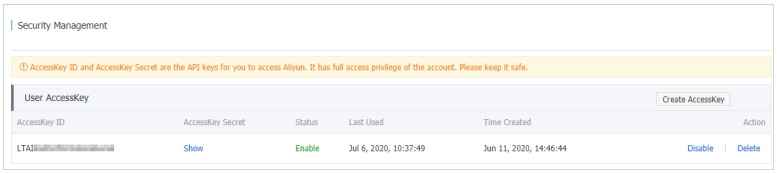
```
apt-get update
apt-get install -y python3-pip python3-dev
cd /usr/local/bin
ln -s /usr/bin/python3 python
pip3 install --upgrade pip
pip install aliyun-log-python-sdk
```

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.

1.6. Log storage management

1.6.1. Modify log settings

After you enable the Log Service for WAF feature, you can modify log settings, such as the log storage period, log fields, and log storage type, on the Log Settings page. The storage types are Logs and Block Logs. To better utilize your log storage capacity, we recommend that you modify log settings based on your business protection and analysis requirements and classified protection requirements.

Prerequisites

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

Context

Log settings take effect for all domain names for which log collection is enabled. For more information about how to enable log collection for domain names, see Step 2: Enable the log collection feature.

You can change the log storage duration for subscription WAF instances that run Business or a higher edition. You can modify log fields and change the log storage type for WAF instances of all editions.

Procedure

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Log Management > Log Service**.
4. In the upper-right corner of the **Log Service** page, click **Log Settings**.
5. On the **Log Settings** page, modify the following settings based on your business requirements.

Parameter	Description

Parameter	Description
Storage Period	The duration for which you want to store logs. Unit: days. Valid values: 30 to 360. Logs that are stored longer than the log storage duration that you specify are deleted. You cannot query or analyze deleted log data. For example, if you set Storage Period to 180 days, logs that are stored for more than 180 days are deleted. **Note** You can change the log storage duration for subscription WAF instances that run Business or a higher edition.
Custom Field Configuration	The log fields that are supported by WAF and included in logs. WAF log fields can be categorized into **Required Fields** and **Optional Fields**. Required fields must be included in WAF logs and cannot be modified. You can include optional fields in WAF logs based on your business requirements. For more information about WAF log fields, see Log fields supported by WAF. To include optional fields in WAF logs, perform the following steps: In the **Optional Fields** section, select the optional fields in the **Available Fields** section and click the rightwards arrow to add the selected fields to the **Selected Fields** section.
Storage Type	The type of logs that you want to store. Valid values: ○ **Logs**: All logs are stored, including logs that are generated when WAF allows and blocks requests. ○ **Block Logs**: Only the logs that are generated when WAF blocks requests are stored.

6. Click **Save**.

Result

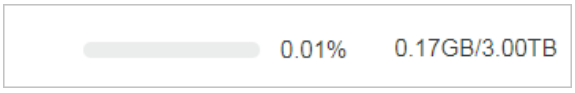
After you modify the log settings, the Log Service for WAF feature stores logs based on the settings that you configured.

1.6.2. 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 and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
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.Full log (unavailable soon)

2.1. 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 seven days.

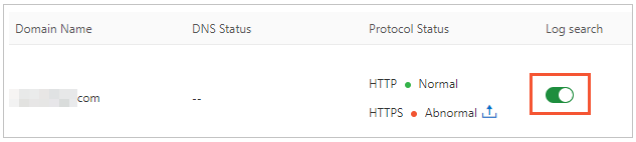
  > **Note** If you want to store logs for 180 days and meet the classified protection requirements, we recommend that you enable Log Service for WAF. For more information, see Enable Log Service for WAF.

- 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 and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
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 of the Log Service for WAF feature.

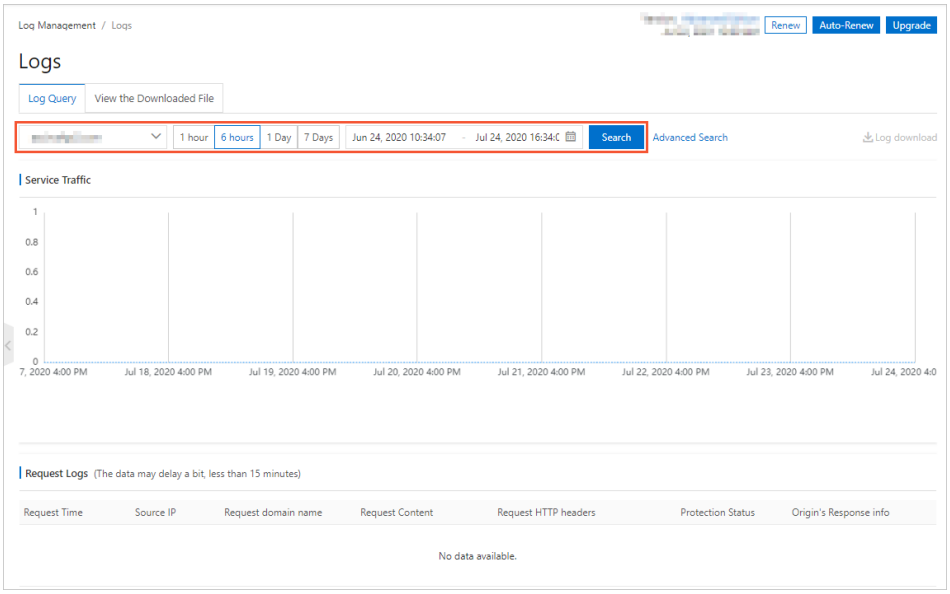


After you turn on **Log search**, WAF logs access requests to your website. Then, you can query the full logs. For more information, see Query full logs.
If the full log feature is no longer required, you can also turn off **Log search** on the **Website Access** page.

> **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.

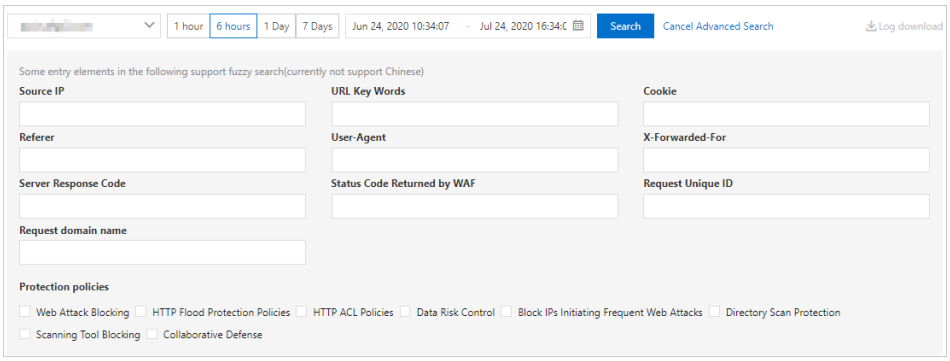
Query full logs

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
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**.

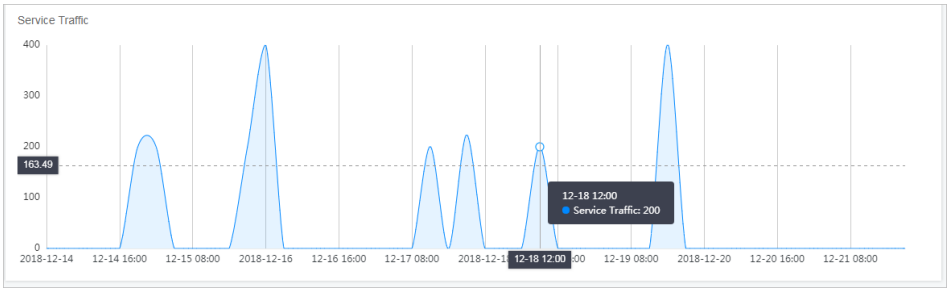


> **Note** If you purchase a subscription WAF instance, you can query logs from the last seven days.

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.



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



   - 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.

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.

Field	Description
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.
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.

Field	Description
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.
Cookie	Cookie HTTP	The Cookie HTTP header. This field provides the source information of the client.

Field	Meaning	Description
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.