

Alibaba Cloud Anti-Bot Service

User Guide

Issue: 20181218

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Note: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Real-time log query and analysis.....	1
1.1 Activate Anti-Bot Log Service.....	1
1.2 Fields in the log entry.....	2

1 Real-time log query and analysis

1.1 Activate Anti-Bot Log Service

With Anti-Bot Log Service, you can collect multiple log entries in real time from your websites that are protected by the Anti-Bot Service. You can also perform real-time log query and analysis and display results in dashboards.

Based on the website access and attack logs, you can do real-time analysis and research in the Anti-Bot Service management console to assist your security managers in configuring protection policies.

Procedure

1. Log on to the [Anti-Bot Service management console](#).
2. Go to **Report > Log Service**, and select the region of your instance.

**Note:**

You need to click **Authorize** and complete the authorization process to authorize Anti-Bot Service to write log entries to your exclusive logstore, if this is the first time that you use Anti-Bot Log Service.

3. Click the site Domain drop-down box, select the website domain for which you want to enable the Log Service, and turn on the status switch.

**Note:**

The Domain drop-down list displays all the website domains that are protected by your Anti-Bot Service instance.

Now, you activate the Log Service for the website domain successfully. Log Service automatically creates a dedicated log library and a dedicated logstore for your Alibaba Cloud account. Anti-Bot Service automatically writes all log entries of activated website domains to the exclusive logstore (antibot-logstore).

Then, you can retrieve and analyze the access logs for the website domains.

Limits and instructions

- Other data cannot be written to the exclusive logstore.

**Note:**


Log entries generated by Anti-Bot Service are stored in the exclusive logstore. You cannot write other data to this logstore by using API, SDK or other methods.

- Basic configurations, such as the storage period of log entries, cannot be modified.
- Do not delete or modify the configurations of the project, logstore, index, and dashboards, which are created by Log Service by default.
- Log Service updates the log query and analysis service on an irregular basis. The index of the exclusive logstore and the default reports are also updated automatically.
- If you want to use the Anti-Bot log query and analysis service with a RAM user, you must grant the required Log Service permissions to the RAM user.

1.2 Fields in the log entry


Anti-Bot Service keeps detailed log entries for your domains, including access requests and attack logs. Each log entry contains dozens of fields. You can perform query and analysis based on specific fields.

Field	Descriptions	Example
__topic__	The topic of the log entry. The value of this field is <code>antibot_access_log</code> , which cannot be changed.	<code>antibot_access_log</code>
<code>antibot</code>	The type of the Anti-Bot Service protection strategy that applies, which includes: <ul style="list-style-type: none"> • <code>ratelimit</code>: Frequency control • <code>sdk</code>: APP protection • <code>intelligence</code>: Crawler intelligence • <code>acl</code>: HTTP ACL policy • <code>blacklist</code>: Blacklist 	<code>ratelimit</code>
<code>antibot_action</code>	The action performed by the Anti-Bot Service protection strategy, which includes: <ul style="list-style-type: none"> • <code>challenge</code>: Verifying using an embedded JavaScript script • <code>drop</code>: Blocking • <code>captcha</code>: Verifying using a slider captcha 	<code>drop</code>

Field	Descriptions	Example
	<ul style="list-style-type: none"> report: Logging the access event 	
antibot_rule	The rule ID of the Anti-Bot Service protection that was triggered.	5472
antibot_verify	<p>The results of the verification methods used in the Anti-Bot Service.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin: 5px 0;">  Note: When the value of the antibot_action field is challenge or captcha, this value is logged. </div> <ul style="list-style-type: none"> challenge_fail: JS verification failed challenge_pass: JS verification passed captcha_fail: slider validation failed captcha_pass: slider validation passed 	challenge_fail
block_action	The interception type of the Anti-Bot Service that was triggered. The value is fixed to <code>antibot</code> .	antibot
body_bytes_sent	The size of the body in the access request, which is measured in Bytes.	2
content_type	The content type of the access request.	application/x-www-form-urlencoded
host	The source website.	api.aliyun.com
http_cookie	The client-side cookie, which is included in the request header.	k1=v1;k2=v2
http_referer	The URL information of the request source, which is included in the request header. - indicates no URL information.	http://xyz.com
http_user_agent	The User Agent field in the request header, which contains information such as the client browser and the operating system.	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)

Field	Descriptions	Example
http_x_forwarded_for	The X-Forwarded-For (XFF) information in the request header , which identifies the original IP address of the client that connects to the web server using a HTTP proxy or load balancing.	-
https	Indicates whether the request is an HTTPS request. <ul style="list-style-type: none"> true: the request is an HTTPS request. false: the request is an HTTP request. 	true
matched_host	The matched domain name (extensive domain name) that is protected by Anti-Bot Service. If no domain has been matched, the value is -.	*.aliyun.com
real_client_ip	The real IP address of the client. If the system cannot get the real IP address, the value is -.	1.2.3.4
region	The information of the region where the Anti-Bot instance is located.	cn
remote_addr	The IP address of the client that sends the access request.	1.2.3.4
remote_port	The port of the client that sends the access request.	23713
request_length	The size of the request, measured in Bytes.	123
request_method	The HTTP request method used in the access request.	GET
request_path	The relative path of the request. The query string is not included.	/news/search.php
request_time_msec	The request time, which is measured in microseconds.	44
request_traceid	The unique ID of the access request.	7837b117154103869434 37009ea1f0

Field	Descriptions	Example
server_protocol	The response protocol and the version number of the origin server.	HTTP/1.1
status	The status of the HTTP response to the client returned by Anti-Bot Service.	200
time	The time when the access request occurs.	2018-05-02T16:03:59+08:00
ua_browser	The information of the browser that sends the request.	ie9
ua_browser_family	The family of the browser that the sent the request.	internet explorer
ua_browser_type	The type of the browser that the sent the request.	web_browser
ua_browser_version	The version of the browser that sends the request.	9.0
ua_device_type	The type of the client device that sends the request.	computer
ua_os	The operating system used by the client that sends the request.	windows_7
ua_os_family	The family of the operating system used by the client.	windows
upstream_addr	A list of back-to-origin IP addresses, separated by commas. The format of an address is <code>IP:Port</code> .	1.2.3.4:443
upstream_ip	The origin IP address that corresponds to the access request. For example, if the origin server is an ECS instance, the value of this field is the IP address of the ECS instance.	1.2.3.4
upstream_response_time	The time that the origin site takes to respond to the Anti-Bot request, which is measured in seconds. "-" indicates the timeout of the request.	0.044
upstream_status	The response status that Anti-Bot receives from the origin server. "-" indicates that no response is received	200

Field	Descriptions	Example
	. The reason can be the response timeout, or the request being blocked by Anti-Bot.	
user_id	Alibaba Cloud account ID.	12345678
wxbb_action	<p>The action performed when the Anti-Bot Service protection type is APP Enhanced protection:</p> <ul style="list-style-type: none"> • <code>close</code>: Blocking, the same as the <code>drop</code> value in the <code>antibot_action</code> field. • <code>test</code>: Logging the access event, the same as the <code>report</code> value in the <code>antibot_action</code> field. • <code>pass</code>: Passing <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Note: If the SDK protection is not integrated, the value is -. </div>	close
wxbb_invalid_wua	APP Enhanced protection strategy type. For details, contact technical support.	valid wua
wxbb_vmp_verify	<p>The result of whether the vmp signature is valid.</p> <ul style="list-style-type: none"> • <code>true</code>: Valid • <code>false</code>: Invalid 	true