# Alibaba Cloud

Web应用防火墙 Quick Start

Document Version: 20210704

C-J 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.

- You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloudauthorized 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 and/or its affiliates 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				
A 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.				
O 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.				
C) 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 listinstanceid 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.Quick	start		05
---------	-------	--	----

## 1.Quick start

This topic walks you through how to deploy and use Web Application Firewall (WAF). WAF protects your website only after you purchase a WAF instance, add your website to WAF, and configure website protection policies. WAF provides security reports that show attack records and access statistics. This way, you can obtain the security posture of your website.

#### Step 1: Purchase a WAF instance

- 1. Log on to the Web Application Firewall console.
- 2. On the Welcome to Web Application Firewall (WAF) page, click Purchase WAF Subscription to go to the buy page of WAF. If you have purchased a WAF instance, the Welcome to Web Application Firewall page does not appear. For more information, see Step 2: Add a website to WAF.



- 3. On the **Web Application Firewall** buy page, select the product edition and specifications. Then, complete the payment. For more information, see Purchase a WAF instance.
- 4. After you purchase the WAF instance, go back to the WAF console.

#### Step 2: Add a website to WAF

To add a website to WAF, you must add the domain name of the website to your WAF instance and change the DNS record of the domain name to redirect the traffic destined for the website to WAF for protection.

(?) Note Before you can add your website to WAF, make sure that your WAF instance is authorized to access other cloud resources. For more information, see Authorize WAF to access cloud resources.

1. Add the website.

- i. On the Website Access page, click Website Access.
- ii. Set Access Mode to CNAME Record and click the Manually Add tab.

#### iii. Complete the wizard. For more information, see 网站接入.

Notice If you have configured a proxy in front of WAF, select Yes for Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF. Otherwise, WAF cannot obtain the actual IP addresses of clients. Proxies include Anti-DDoS Pro, Anti-DDoS Premium, and Alibaba Cloud CDN.

1	(2)	(3)				
Enter Your Website Information	Change DNS Settings	Add Completed				
Protection Resource		> How to determine the protocol ty	/pe?			
○ Exclusive Cluster ○ Static Back-to-Origin	n in Hybrid Cloud Scenarios 💿 Shared Cluster	> How to obtain the website IP add	Iress?			
* Protocol Type:		Which ports can the Web Application Firewall protect? Click to view				
HTTP HTTPS						
* Destination Server (IP Address): 🕖		Meet Expert	Need Service Configuration?			
IP O Destination Server (Domain Name)		Join the WAF Technical Support DingTalk group	One-on-one consultation with security engineers to solve			
Enter the public IP address of the destination Alibaba Cloud, any other cloud service provid	server for protection, such as 1.1.1.1. The server can be in the lers, IDC rooms, etc.		problems with Web Application Firewall during installation, configuration, etc. Buy			
Enter the IP addresses on a single line, up to 20,	and separated by commas (,).					
* Destination Server Port:						
	Customize					
Load Balancing Algorithm:						
🖲 IP hash ( Round Robin 🥚 Least time	2					
This function is not yet supported by the current	: version. PleaseUpgrade					
Does a layer 7 proxy (DDoS Protection/CDN, e	etc.) exist in front of WAF:					
🗌 Yes 🔘 No						
Request Tag						
Header Field Name						
Do not enter a standard HTTP header, such as Us overwritten.	ser-Agent. Otherwise, the original request header may be					
Header Field Value						
When a request passes through WAF, WAF adds define so that the destination server can use this field already exists, WAF overwrites its value.	to the request the custom header field and its value that you information for statistical purposes. Note: If the custom header					
Resource Group						
Default Resource Group						
Next						

After the website is added to WAF, you can view the CNAME that WAF assigns to the domain name of the website on the **Website Access** page.

Domain Name	DNS Status	Protocol Status	IP V6 Status	Log Service		
-test.ali	Domain Name: CName: 🛛	a. 	, .com	undunwaf3.com		

**Notice** If the website supports HTTPS, you must upload the SSL certificate for the domain name of the website after the website is added. This way, WAF can process HTTPS traffic. For more information, see 网站接入.

- 2. Change the DNS record of the domain name to map the domain name to the CNAME assigned by WAF.
  - If you have not configured a proxy, such as Anti-DDoS Pro, Anti-DDoS Premium, or Alibaba Cloud CDN, in front of WAF, visit the website of your DNS service provider to change the CNAME record.
     If your DNS service provider is Alibaba Cloud DNS, log on to the Alibaba Cloud DNS console and add a CNAME record by using the CNAME assigned by WAF.

Add Record		×
	Type: CNAME- Canonical name $\checkmark$	
	Host: www	
	ISP Line : Default - Return to the default value when the query is not m $\vee$ ?	
	* Value : yundunwaf3.com	
	* TTL: 10 minute(s)	
	Cancel	ОК

For more information, see Change a DNS record.

 If you have configured a proxy, such as Anti-DDoS Pro, Anti-DDoS Premium, or Alibaba Cloud CDN, in front of WAF, log on to the console of the proxy and change the back-to-origin address of the proxy to the CNAME assigned by WAF. This way, WAF can receive the requests destined for the website.

For more information, see Use WAF with Anti-DDoS Pro or Anti-DDoS Premium and Use WAF with CDN.

#### Step 3: Configure website protection policies

After you add the domain name, WAF filters access requests and forwards normal requests to the origin servers. WAF provides multiple features to protect your website against different types of attacks. Among the features, only **Protection Rules Engine** and **HTTP Flood Protection** are enabled by default. The Protection Rules Engine feature protects your website against common web attacks, such as SQL injections, XSS attacks, and webshell uploads. The HTTP Flood Protection feature protects your website against HTTP flood attacks. You must manually enable other features and configure protection rules. For more information, see Overview.

#### Step 4: View security reports

On the **Security Report** page, you can view the attack records and access statistics of the website protected by WAF. For more information, see View security reports.

Security	report										
Web Security	Bot Manageme	ent Access C	ontrol/Throttli	ng							
Web Intrusion Pre	evention Data Le	akage Prevention	Account Sec	urity Positive Secur	ity Model API I	Request Security					
All	~	Yesterday	Today 7 Days	30 Days Oct 7, 20	20 00:00	- Oct 14, 2020 17:38	Ē	Search	<b>1</b>		
Security attack	k type distribution			Top 5 attack sourc	e ips			Top 5 att	ack source regi	ions	
		webshell 27	.43%	67	States)		4	United Sta	tes		438,004
		• Other 21.82%		74			4	United Kingdom		44,82	
	<ul> <li>Local file inclusion 17.89%</li> <li>Code execution 13.37%</li> </ul>		usion 17.89% on 13.37%	106. 46(China (B	eijing))		4	Japan			37,57
SQL injection 10.87%     Remote file inclusion _ 5.58%		108	itates)		з	Germany			34,02		
	• XSS 2.04%		85	k)		3	France			33,41	
Regular Protection	on 🗸 A	u	✓ A	ttack IP	Searc	h					
ttack IP	Region	Time Attacked	Attack Typ	e Attacked UR	L Method	Parameter	Rule	Action	Rule ID	Attack Probability	Actions
3	United States United States	Oct 12, 2020 2 PM	:37 webshell	my	m//? GET		Bloc	k	170024		View Details