Alibaba Cloud
Web Application Firewall

FAQ

Issue: 20181212

MORE THAN JUST CLOUD | 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 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 `cd /d C:/windows` command to enter the Windows system folder.
`Italics`	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *`{stand | slave}`*

Contents

1 DNS resolution status exception

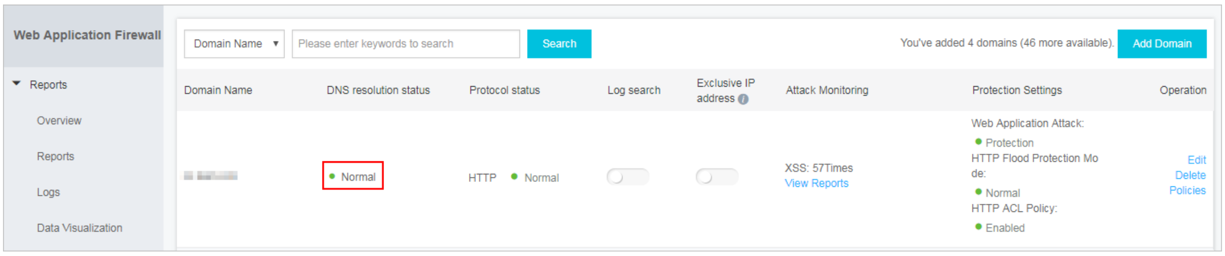
When a website configuration is created in Alibaba Cloud WAF, WAF automatically performs the following checks:

- **Domain to CNAME**: Performed every hour to detect whether the domain name has been resolved to the WAF CNAME address.
- **Web traffic**: Performed every several minutes to detect whether the web traffic to the domain name passes through WAF.

When one of the checks is ok, the DNS resolution status is Normal, which indicates that Alibaba Cloud WAF is perfectly implemented for the website.

To view the **DNS resolution status**, log on to the *Alibaba Cloud WAF console* and go to the **Management** > **Website Configuration** page.

The **Normal** status displays as follows.



You've added 4 domains (46 more available).

Domain Name	DNS resolution status	Protocol status	Log search	Exclusive IP address	Attack Monitoring	Protection Settings	Operation
[redacted]	● Normal	HTTP ● Normal	○	○	XSS: 57Times View Reports	Web Application Attack: ● Protection HTTP Flood Protection Mode: ● Normal HTTP ACL Policy: ● Enabled	Edit Delete Policies

If the DNS resolution status is **Exception**, then Alibaba Cloud WAF may not be correctly configured. This topic explains how does WAF determine the DNS resolution status and lists common exception statuses.

How does WAF determine the DNS resolution status

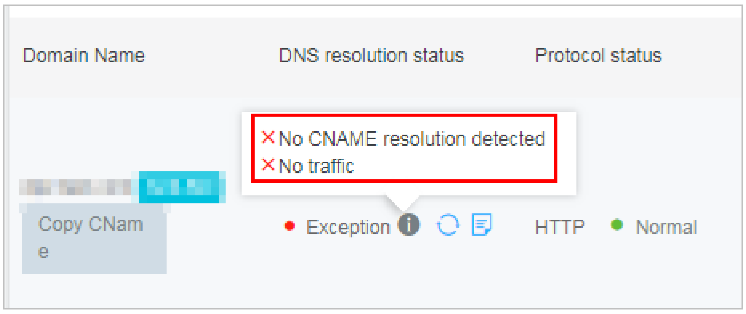
Alibaba Cloud WAF determines the DNS resolution status by the following conditions. When one of the conditions is met, the DNS resolution status is normal.

- Condition A: The domain name is resolved to the WAF CNAME address.
- Condition B: Web traffic of the domain name passes through WAF. When at least 10 requests are detected in the last five seconds, it is ok. Two or three requests per minute is regarded as no traffic. To view the history of web traffic, you can check the Attack protection report of HTTP flood. For more information, see *Attack protection reports*.

We recommend that you use a CNAME record to redirect web traffic to WAF. Using CNAME supports node switch or even redirecting traffic back to source in case of node failure or machine failure, which improves your business's availability and failure recovery capacity. If CNAME record conflicts with your current DNS settings, you can use an A record to do traffic redirection.

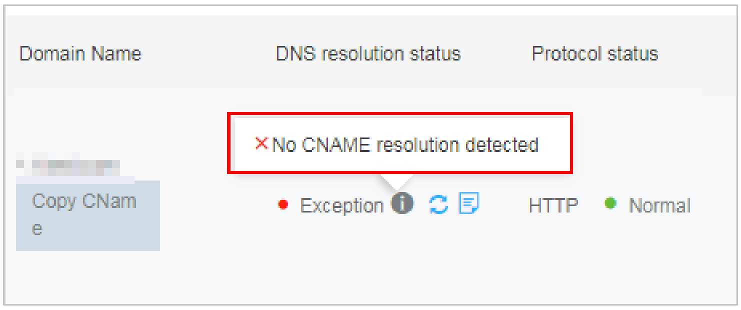
Common exception statues

- For a fully qualified domain name (FQDN, such as example.abc.com), if both the Domain to CNAME and Web traffic checks fail, the exception status displays as follows.



Domain Name	DNS resolution status	Protocol status
[redacted] Copy CName	✕No CNAME resolution detected ✕No traffic ● Exception	HTTP ● Normal

- For a wildcard domain name (for example, *.abc.com), the exception status displays as follows.



Domain Name	DNS resolution status	Protocol status
[redacted] Copy CName	✕No CNAME resolution detected ● Exception	HTTP ● Normal

- When the website is deployed with CDN or other proxy servers in front of WAF, the domain name is resolved to CDN and other proxy server rather than WAF. As a result, the Domain to CNAME check fails. In addition, the CDN-returned traffic received by WAF is low, which may result to the Web traffic check fails. In this case, the exception message does not definitely indicate that WAF is ill-configured.

  For more information about how to deploy WAF and CDN together, see *Deploy WAF and CDN together*.

Manually test if WAF is working

1. Visit a domain name that is configured in Alibaba Cloud WAF, for example, *`www.aliyundemo.cn`*. The webpage can be accessed normally.
2. Add the *`/alert(xss)`* string to the end of the domain name to assemble a testing URL and visit this URL (in this example, *`www.aliyundemo.cn/alert(xss)`*. If you receive a 405 page telling you that this request is blocked by Alibaba Cloud WAF, then WAF is protecting the website.

2 WAF back-to-origin CIDR blocks update

To provide better web application protection for you, Alibaba Cloud Web Application Firewall (WAF) expands the capacity of the global WAF server rooms to further improve service capabilities. After the expansion of the capacity, WAF's WAF back-to-origin CIDR blocks are expanded.

If your origin servers have IP whitelist or security group settings for access control, to only allow accesses from WAF back-to-origin CIDR blocks, you must add the following new WAF back-to-origin CIDR blocks into the whitelist. Otherwise, traffic forwarded by WAF to the origin servers can be blocked by access control policies, and your website cannot be visited as expected.

Note:

Besides adding new back-to-origin CIDR blocks, some existing CIDR blocks are also updated this time. Please verify the new CIDR blocks carefully.

New WAF back-to-origin CIDR blocks for the mainland China instances

121.43.18.0/24, 120.25.115.0/24, 101.200.106.0/24, 120.55.177.0/24, 120.27.173.0/24, 120.55.107.0/24, 123.57.117.0/24, 120.76.16.0/24, 182.92.253.32/27, 60.205.193.64/27, 60.205.193.96/27, 120.78.44.128/26, 118.178.15.0/24, 39.106.237.192/26, 106.15.101.96/27, 47.101.16.64/27, 47.106.31.0/24, 47.98.74.0/25, 47.97.242.96/27, 112.124.159.0/24, 39.96.130.0/24, 39.96.119.0/24, 47.99.20.0/24, 47.104.53.0/26, 47.108.23.192/26

New WAF back-to-origin CIDR blocks for the International instances

47.89.1.160/27, 47.89.7.192/26, 47.88.145.96/27, 47.88.250.0/24, 47.52.120.0/24, 47.254.217.32/27, 47.88.74.0/24, 47.89.132.224/27, 47.91.69.64/27, 47.91.54.128/27, 47.74.160.0/24, 47.91.113.64/27, 149.129.211.0/27, 149.129.140.0/27, 47.89.7.224/27, 8.208.2.192/27

You can also log on to the Web Application Firewall management console, and go to the **Management** > **Website Configuration** page, to check the latest WAF back-to-origin CIDR blocks.