ALIBABA CLOUD

Alibaba Cloud

漏洞扫描

FAQ

Document Version: 20210608

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.How do I calculate my quotas if I purchase Cloud Security Scanner by using the pay-as-you-go pricing model?

If you purchase the service in pay-as-you-go mode, the quota for the number of scans is specified. Each IP address or second-level domain consumes one scan. You can repurchase the service to increase the quotas before or after you use up your quotas.

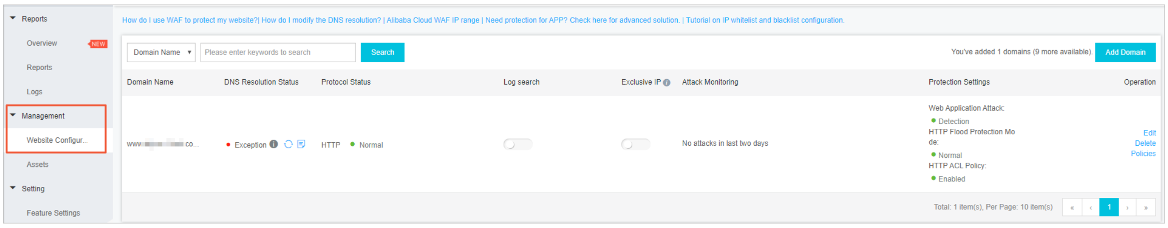
The pay-as-you-go service will be released soon.

2.How to add Cloud Security Scanner to the whitelist of Web Application Firewall (WAF)?

If your host is protected by WAF, you must add the CIDR block of Cloud Security Scanner to the WAF whitelist. If Cloud Security Scanner is not in the WAF whitelist, the accuracy of scan results may be adversely affected.

Procedure

1. Log on to the WAF console.
2. In the left-side navigation pane, click **Management**.



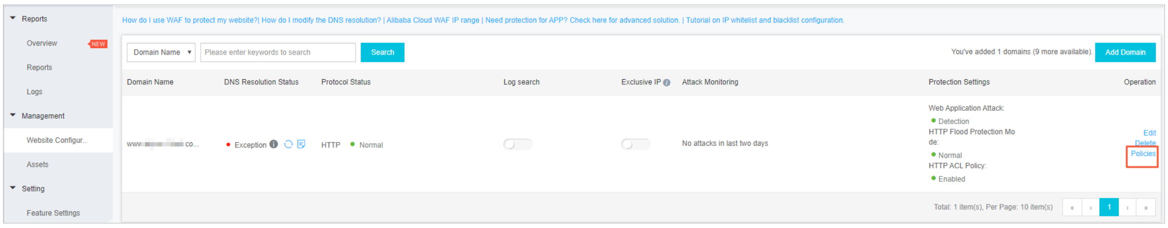
How do I use WAF to protect my website?| How do I modify the DNS resolution? | Alibaba Cloud WAF IP range | Need protection for APP? Check here for advanced solution. | Tutorial on IP whitelist and blacklist configuration.

You've added 1 domains (9 more available).

Domain Name	DNS Resolution Status	Protocol Status	Log search	Exclusive IP	Attack Monitoring	Protection Settings	Operation
www[redacted]co...	● Exception	HTTP ● Normal			No attacks in last two days	Web Application Attack: ● Detection HTTP Flood Protection Mode: ● Normal HTTP ACL Policy: ● Enabled	Edit Delete Policies

Total: 1 item(s), Per Page: 10 item(s) « ‹ 1 › »

3. On the **Website Configuration** page, find the target domain, and then click **Policies** in the **Operation** column.

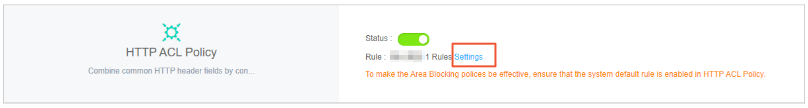

How do I use WAF to protect my website?| How do I modify the DNS resolution? | Alibaba Cloud WAF IP range | Need protection for APP? Check here for advanced solution. | Tutorial on IP whitelist and blacklist configuration.

You've added 1 domains (9 more available).

Domain Name	DNS Resolution Status	Protocol Status	Log search	Exclusive IP	Attack Monitoring	Protection Settings	Operation
www[redacted]co...	● Exception	HTTP ● Normal			No attacks in last two days	Web Application Attack: ● Detection HTTP Flood Protection Mode: ● Normal HTTP ACL Policy: ● Enabled	Edit Delete Policies

Total: 1 item(s), Per Page: 10 item(s) « ‹ 1 › »

4. In the **HTTP ACL Policy** module, click **Settings**.



Status :

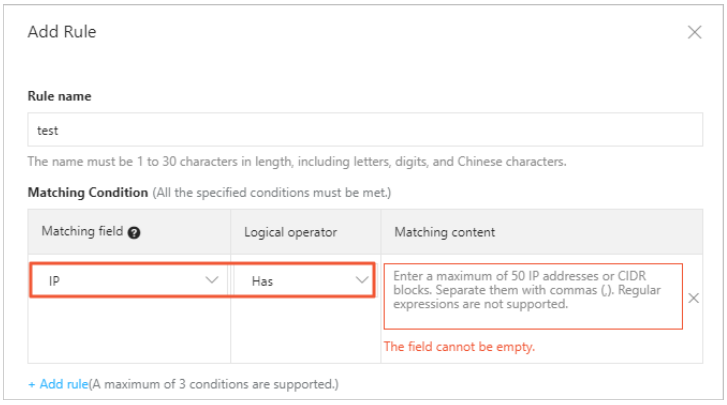
Rule : [redacted] 1 Rules

To make the Area Blocking polices be effective, ensure that the system default rule is enabled in HTTP ACL Policy.

5. In the HTTP ACL Policy table, click **Add Rule** in the upper-right corner. The **Add Rule** dialog box appears.
6. In the **Add Rule** dialog box, set the required parameters.
   - **Rule Name**: Specify a name for the rule.
   - **Matching Field**: In the **Matching Field** drop-list, select **IP** or **User-Agent**, and then enter a criterion into the **Matching Content** input box.

> **Note** For a newly added rule, you only need to configure IP or User-Agent criteria. We recommend that you configure IP address criteria when you add rules.

- Select **IP**.



Add Rule

Rule name

test

The name must be 1 to 30 characters in length, including letters, digits, and Chinese characters.

Matching Condition (All the specified conditions must be met.)

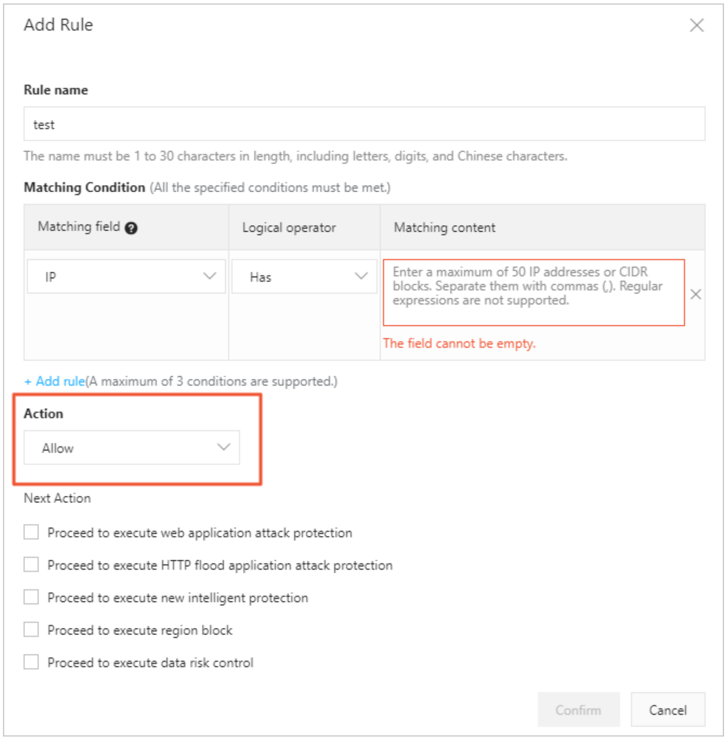
Matching field	Logical operator	Matching content
IP	Has	Enter a maximum of 50 IP addresses or CIDR blocks. Separate them with commas (,). Regular expressions are not supported. The field cannot be empty.

+ Add rule(A maximum of 3 conditions are supported.)

> Note For more information about the IP addresses, submit a ticket.

- If you do not want to configure an IP address whitelist, select **User-Agent**. Submit a ticket to obtain the matching content.

7. In the **Action** drop-down list, select **Allow**.



Add Rule

Rule name

test

The name must be 1 to 30 characters in length, including letters, digits, and Chinese characters.

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
IP	Has	Enter a maximum of 50 IP addresses or CIDR blocks. Separate them with commas (,). Regular expressions are not supported. The field cannot be empty.

+ Add rule(A maximum of 3 conditions are supported.)

Action

Allow

Next Action

□ Proceed to execute web application attack protection

□ Proceed to execute HTTP flood application attack protection

□ Proceed to execute new intelligent protection

□ Proceed to execute region block

□ Proceed to execute data risk control

> Note After you set the **Action** parameter to **Allow**, the rule is configured. Do not select the check boxes under **Next Action**, for example, **Proceed to execute web application attack protection**.

8. Click **Confirm**.

3.How many editions does Cloud Security Scanner offer?

Cloud Security Scanner offers two editions: Professional and Enterprise.

For more information about these editions, see the Editions and features.

4.What are the functions of the asset discovery feature?

This topic describes the advantages of the asset discovery feature provided by Cloud Security Scanner.

- You can use this feature to perform the following operations:
  - Discover all assets that are open to the Internet, detect all subdomains and web server IP addresses under a root domain, and provide detailed asset fingerprint information, such as the middleware, applications, operating systems, ports, and services.
  - Detect the IP address of a domain by subdomain and provide the asset fingerprint information about this domain.
  - Detect a domain by IP address and provide the asset fingerprint information about this domain.
- This feature allows you to create an asset discovery task based on multiple root domains. To create a task, perform the following operations:
  - On the **Assets Management** page, click **Add Asset** in the upper-right corner. In the Add Asset pane, enter multiple root domains in the Asset field, specify Asset Tag, and click Add.
  - Find the added asset and click **Scan** in the Actions column. In the **Create Scan Task** pane, specify Task Name, Schedule Strategy, Effective Period, and Scan Type, select a created asset tag from the **Scan Target** drop-down list, and click Create.

5.How can I scan specified ports or URLs?

In the **Advanced** section of the **Create Scan Task** pane, specify **URLs**. The port information can be included in the entered URL information. If you want to enter multiple URLs, separate them by pressing **Enter**.

After a scan task is created, Cloud Security Scanner executes this task and returns the scan result, which includes the configured asset objects, URLs, or ports.

6.Can Cloud Security Scanner scan assets that are not deployed on Alibaba Cloud?

Yes. Cloud Security Scanner can scan all IP addresses or domains that you can access over the Internet.

7.Can Cloud Security Scanner scan assets over the internal network?

No. Cloud Security Scanner cannot scan assets over the internal network.

8.How can I view URL information in the result of a scan task created based on domains or IP addresses?

This topic describes how to view URL information in the result of a scan task created based on domains or IP addresses.

Procedure

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click Task Management and then click **Task Instances**.
3. On the **Task Instances** page, click the target instance name or scan target in the **Instance Name/Scan Target** column.
4. On the instance details page, click **Details** on the right of **Web Servers** in the **Attack Surfaces** section.
   On the **Attack Surfaces** page, view the detailed URL information.

9.How can I view the scanned items in a scan task created based on a specific domain or IP address?

This topic describes how to view the scanned items in a scan task created based on a specific domain or IP address.

Procedure

1. Log on to the Cloud Security Scanner console.
2. In the left-side navigation pane, click Task Management and then click **Task Instances**.
3. On the **Task Instances** page, click the target instance name or scan target in the **Instance Name/Scan Target** column.
4. On the instance details page, click the number specified for **Checked Items** in the **Instance Overview** section.
   On the **Check Results** page, view the detailed information about the scanned items.