ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

System Management

Document Version: 20220630

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}`

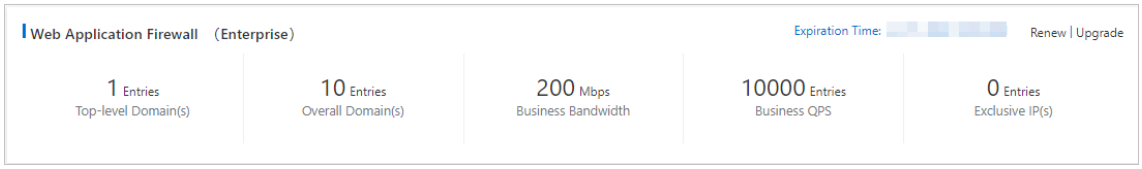
Table of Contents

1.View product information

The Product Information page of Web Application Firewall (WAF) displays the resource details, protection rule updates, feature updates, and WAF CIDR blocks of a WAF instance.

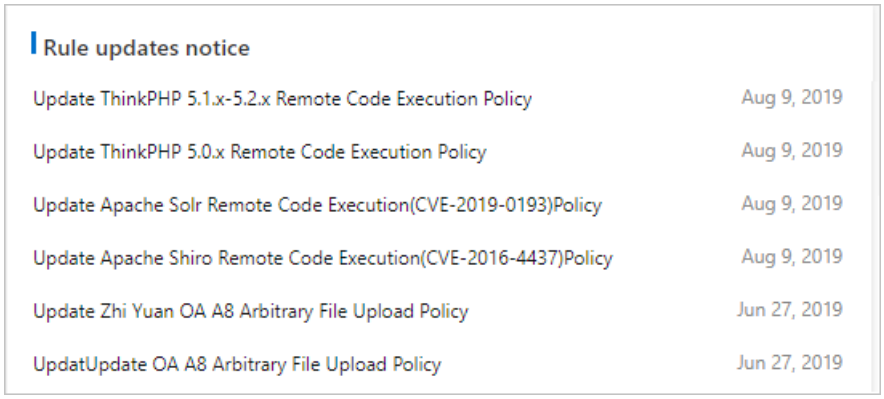
Procedure

1.
2.
3.
4. View the following information on the **Product Information** page:
   - WAF resource details
     - The current WAF version and expiration time (**Renew** and **Upgrade** operations supported)
     - **Top-level Domain(s)**
     - **Overall Domain(s)**
     - **Business Bandwidth**
     - **Business QPS**
     - **Exclusive IP(s)**



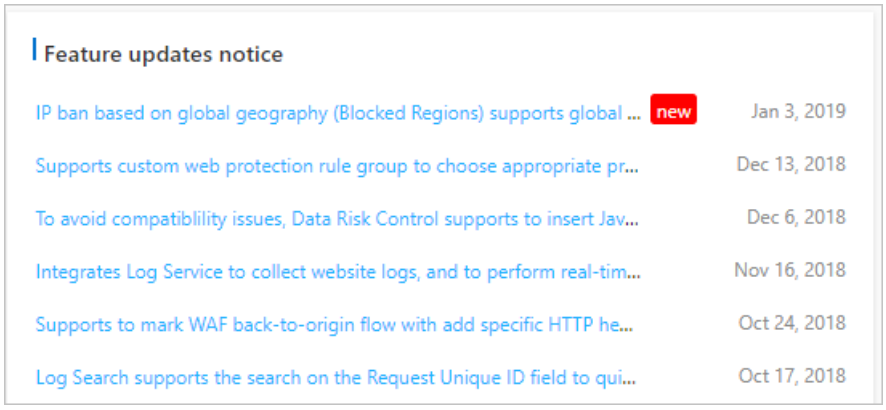
   - **Rule updates notice**

     Displays the latest updates to the built-in protection rules of WAF.



   - **Feature updates notice**

     Displays the latest WAF feature updates. You can click a record to view its details.



- **WAF IP Addresses**

  Displays all WAF CIDR blocks. You can click **Copy All IPs** to copy all IP addresses.

2.Terminate the WAF service

Also, if a subscription WAF instance expires, you can terminate the WAF service to release the instance.

Context

> **Note** Before you can terminate the WAF service, make sure that the DNS records of the websites protected by your WAF instance point to the origin server. After you terminate the WAF service or release your WAF instance, all the configurations of the websites are deleted. If a request is still redirected to your WAF instance, the request cannot be forwarded to the origin server, and the access fails.

Procedure

1.
2.
3. In the upper-right corner of the **Overview** page, click **Terminate WAF Service**.

   > **Note** If you use a subscription WAF instance, the button appears only after the instance expires.

4. Confirm that the DNS records of your websites point to the origin server. Then, click **Confirm**.

3.Create an exclusive cluster

Web Application Firewall (WAF) Exclusive Edition provides virtual exclusive clusters. These exclusive clusters allow you to customize domain name settings and protection settings in WAF based on your business requirements.

Context

If your websites have special requirements, you can create an exclusive cluster and add your website to the exclusive cluster for comprehensive protection.

After you purchase a WAF instance that runs Exclusive Edition, you can create an exclusive cluster and customize the following settings for the exclusive cluster:

- Cluster region: You can select a region for the cluster.
- Cluster ports: An exclusive cluster supports more non-standard ports than a shared cluster does. You can use HTTP ports, HTTPS ports, and HTTP/2 ports as the back-to-origin ports.

  > **Note** The following system ports are not supported: 22, 53, 9100, 4431, 4646, 8301, 6060, 8600, 56688, 15001, 4985, 4986, and 4987.

- SNI support: You can upload a certificate to allow clients that do not support the Server Name Indication (SNI) protocol to access your website.
- Response page: You can specify a static URL that is uploaded to Alibaba Cloud CDN. If a request is blocked, the page that is specified by the URL is displayed.
- TLS security policy: You can specify the TLS versions and cipher suites.
- Persistent connection timeout: You can specify the connection timeout period, request timeout period, and response timeout period.

Create an exclusive cluster

After you purchase a WAF instance that runs Exclusive Edition or upgrade your WAF instance to Exclusive Edition, you can use an exclusive cluster or a shared cluster to protect your website. Before you can use the features of an exclusive cluster, you must create an exclusive cluster based on your business requirements.

1.
2.
3.
4. On the **Exclusive Settings** page, configure the following parameters:
   - Select a region for **Region**.

     > **Note** After you create an exclusive cluster, you cannot change the value of **Region**.

   - Configure **Destination Server Port**. Select a protocol and click **Customize**. Enter the ports that you want to protect and click **Save**. If you add a domain name to the exclusive cluster, you can select a server port that is specified for this cluster.
   - Configure **URL of Blocking Response Page**. Enter the static URL that is uploaded to Alibaba Cloud CDN. If a request is blocked, the page that is specified by the URL is displayed.

- Enter the content of **Certificate file** and **Private key file** to allow clients that do not support the SNI protocol to access your website.
- Configure HTTPS settings.
  - **TLS Version**: The default value is **Support TLS 1.0 and Later (High Compatibility and Low Security)**. You can select Support TLS 1.1 and Later (Moderate Compatibility and Moderate Security) or Support TLS 1.2 and Later (Moderate Compatibility and High Security) based on your business requirements.
  - **Cipher Suite**:
    - If you select **Select cipher suites based on the protocol version. Proceed with caution**, you can customize the TLS versions and cipher suites by domain name. For example, you can separately customize the TLS version. You can also customize a combination of strong encryption algorithms, weak encryption algorithms, or both.
    - If you select **Strong Cipher Suites (Low Compatibility and High Security)**, the following strong cipher suites are supported:
      - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
      - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
      - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
      - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
      - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
      - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
      - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
      - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
      - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
      - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    - If you select **All Cipher Suites (High Compatibility and Low Security)**, all the preceding strong cipher suites and the following weak cipher suites are supported:
      - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
      - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
      - TLS_RSA_WITH_AES_128_GCM_SHA256
      - TLS_RSA_WITH_AES_256_GCM_SHA384
      - TLS_RSA_WITH_AES_128_CBC_SHA256
      - TLS_RSA_WITH_AES_256_CBC_SHA256
      - TLS_RSA_WITH_AES_128_CBC_SHA
      - TLS_RSA_WITH_AES_256_CBC_SHA
      - SSL_RSA_WITH_3DES_EDE_CBC_SHA
- Specify the persistent connection timeout.
  - **Connection Timeout**: Set the connection timeout period to a value between 5 and 3,600 seconds.
  - **Read Timeout**: Set the read timeout period to a value between 120 and 3,600 seconds.
  - **Write Timeout**: Set the write timeout period to a value between 120 and 3,600 seconds.

5. Click **Create**.
   After you perform operations, WAF creates an exclusive cluster. The exclusive cluster is created in about 20 minutes. You can view and modify the settings of the exclusive cluster that you created on the **Exclusive Settings** page.

What's next

After an exclusive cluster is created, you can add websites that have special requirements to the exclusive cluster for custom protection. The following scenarios are supported:

- You can add a website to the exclusive cluster for protection. For more information, see Add a domain name.
- If a website is added to WAF, perform the following operations to enable exclusive cluster protection for the website: Go to the **Website Access** page in the WAF console and set **Protection Resource** to **Exclusive Cluster** for the website.

  You can also change the protection resource of a website from an exclusive cluster to a shared cluster.

  > **Notice** The ports supported by WAF vary based on the cluster type. Before you change the protection cluster type for a website, make sure that the cluster supports the ports of your website.

4.Best practices for WAF exclusive clusters

The exclusive clusters of Web Application Firewall (WAF) support the protection capabilities that are provided by WAF shared clusters. WAF exclusive clusters also support custom configurations to better protect your workloads. For example, exclusive clusters support non-standard ports, Server Name Indication (SNI), custom error pages, flexible HTTPS encryption settings, and custom settings for persistent connection timeout.

If your workloads require these protection configurations, we recommend that you create a WAF exclusive cluster and associate your workloads with the cluster for protection.

Comparison between exclusive clusters and shared clusters

Item	WAF shared cluster	WAF exclusive cluster
Supported regions	Shared clusters are supported by 14 nodes deployed in the following regions: China (Beijing), China (Shanghai), China (Hangzhou), China (Shenzhen), China (Hong Kong), Singapore (Singapore), Malaysia (Kuala Lumpur), US (Virginia), Australia (Sydney), Germany (Frankfurt), India (Mumbai), Indonesia (Jakarta), UAE (Dubai), and Japan (Tokyo). If you associate your workloads with a shared cluster, WAF automatically allocates protection resources from the region that is closest to the location of the origin server. This region is determined based on the IP address of the origin server.	An exclusive cluster includes primary and secondary clusters. You can specify a region for the primary cluster. However, you cannot specify a region for the secondary cluster. **Notice** After the region of the primary cluster is specified, you can no longer change the region. After you associate your workloads with an exclusive cluster, WAF allocates protection resources from the region where the primary cluster resides to protect your workloads. The secondary cluster serves as a backup. If errors occur on the primary cluster, your workloads are switched to the secondary cluster. If your workloads are under attack, the secondary cluster is used to reinforce protection.

Item	WAF shared cluster	WAF exclusive cluster
Supported cluster ports	If your workloads use non-standard ports, you must specify the ports when you add your website to WAF. Shared clusters support specific non-standard ports. For more information, see View the allowed port range.	Exclusive clusters support more non-standard ports than shared clusters. However, exclusive clusters do not support the following system ports: 22, 53, 9100, 4431, 4646, 8301, 6060, 8600, 56688, 15001, 4985, 4986, and 4987. If you want to use a non-standard port in an exclusive cluster, you must enable the port in the exclusive cluster and select the enabled port when you associate your workloads with the exclusive cluster. **Note** An exclusive cluster supports up to 50 non-standard ports. By default, only the ports 80 and 443 are enabled.
SNI	If clients do not support SNI, HTTPS requests may fail after you associate your workloads with a shared cluster. For more information, see HTTPS access exceptions arising from SNI compatibility ("Certificate not trusted").	When you configure an exclusive cluster, you can upload the default certificate. This way, clients that do not support SNI can normally access the websites that are protected by the exclusive cluster.
Error pages	If you use a shared cluster, WAF returns the default error page when it blocks requests.	If you want WAF to return a custom error page, you can use an exclusive cluster and customize the error page. You can upload a custom static page to Alibaba Cloud CDN, and specify the URL of the page in WAF. This improves user experience.
HTTPS encryption settings	Shared clusters do not support custom HTTPS encryption settings.	When you configure an exclusive cluster, you can select TLS versions and cipher suites to enable HTTPS encryption based on your business requirements.
Settings for persistent connection timeout	Shared clusters do not support custom settings for persistent connection timeout.	When you configure an exclusive cluster, you can specify the maximum duration of a persistent connection to improve network resource usage.

Associate workloads with an exclusive cluster

Prerequisites

A WAF instance of the **Exclusive** edition is purchased, or the WAF instance is upgraded to the **Exclusive** edition. For more information, see Purchase a WAF instance and Renewal and upgrade.

Procedure

The following procedure describes how to associate workloads with an exclusive cluster. In the following procedure, the port 90 is used. This port is not within the range of non-standard ports supported by shared clusters. If you want to use WAF to protect the workloads over this port, you must associate the workloads to an exclusive cluster.

1. Create an exclusive cluster.
   i. Log on to the .
   ii. In the top navigation bar, select the resource group to which the instance belongs and the region, **Mainland China** or **Outside Chinese Mainland**, in which the instance resides.
   iii. In the left-side navigation pane, choose **System Management > Exclusive Settings**.
   iv. On the **Exclusive Settings** page, create an exclusive cluster based on your workloads.

   In this example, you must select **HTTP** and enter **90** in the **Destination Server Port** section. For more information, see Create an exclusive cluster.

   v. Click **Save Settings**.
   WAF creates the exclusive cluster based on your settings.
2. Associate the workloads over the HTTP port 90 with the created exclusive cluster.
   - A website is added to WAF.
     a. In the left-side navigation pane, choose **Asset Center > Website Access**.
     b. Find the domain name of the website that you want to add to the exclusive cluster. Then, set **Protection Resource** in the **Quick Access** column to **Exclusive Cluster**.

     > **Note** **Protection Resource** appears only when your WAF instance runs the **Exclusive** edition.

     c. (Optional)Update the website settings based on your business requirements. For example, change the server port to the HTTP port 90. For more information, see Add a domain name.
   - Add a website to WAF.
     a. In the left-side navigation pane, choose **Asset Center > Website Access**.
     b. On the **Domain Names** tab, click **Website Access**.
     c. (Optional)On the **Add Domain Name** page, set **Access Mode** to **CNAME Record**.

     If **CNAME Record** is automatically selected, skip this step.

     d. In the **Enter Your Website Information** step, set **Protection Resource** to **Exclusive Cluster** and enter the server port. In this example, add the HTTP port 90 in **Destination Server Port**.

     > **Note** After you select **Exclusive Cluster**, you can select the server port only from the ports enabled for the exclusive cluster in **Destination Server Port**. For more information, see Create an exclusive cluster.

     For more information about the settings, see Manually add domain name configurations.

     e. Click **Next**. Then, follow the instructions to change the DNS records of the website. After you change the DNS records, WAF can protect your workloads.

     For more information, see Change a DNS record.

3. If the characteristics of the workloads change and the exclusive cluster is affected, update the cluster and website settings. For more information, see Step 1 and Step 2.