Global Application Acceleration Platform

Operation Guide

Product Documentation

Contents

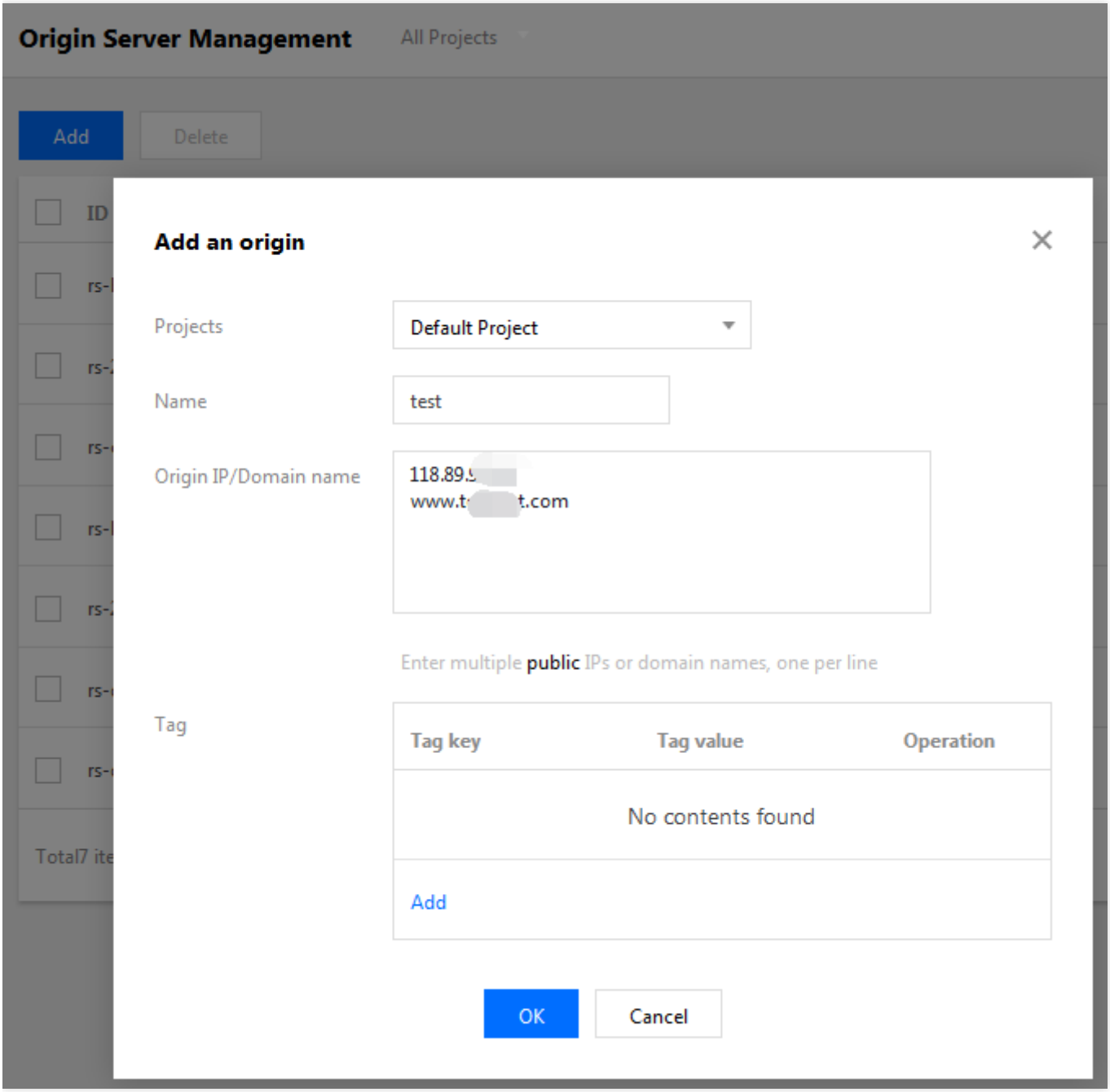
Operation Guide
Origin Server Management

Last updated：2021-12-14 13:00:48

Adding an Origin Server

Log in to the GAAP console. On the "Origin Server Management" page, click **Add** to add information about all the servers that need access acceleration. You can enter the origin server IP or domain name, and separate multiple

origin servers by the Enter key. The origin server IP supports IPv4 and IPv6 addresses.

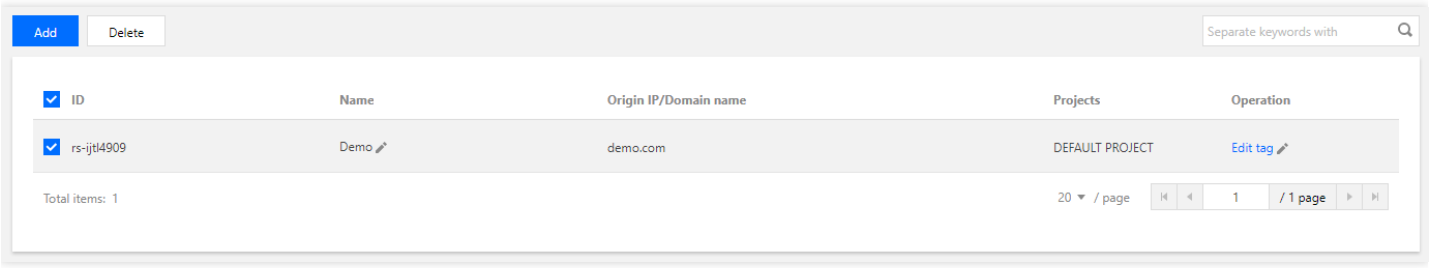


Deleting an Origin Server

Log in to the GAAP console. On the **Origin Server Management** page, select the origin server you want to remove, and click **Delete**.

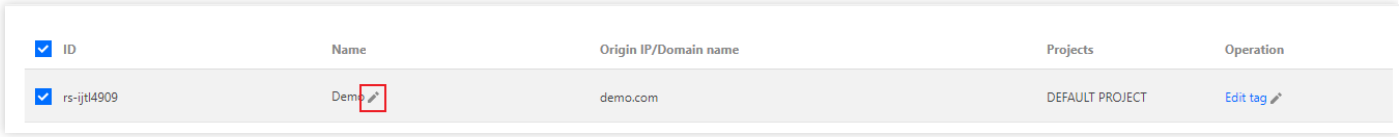
Note：

If the origin server to be removed is bound to the existing connection, unbind them before deletion.

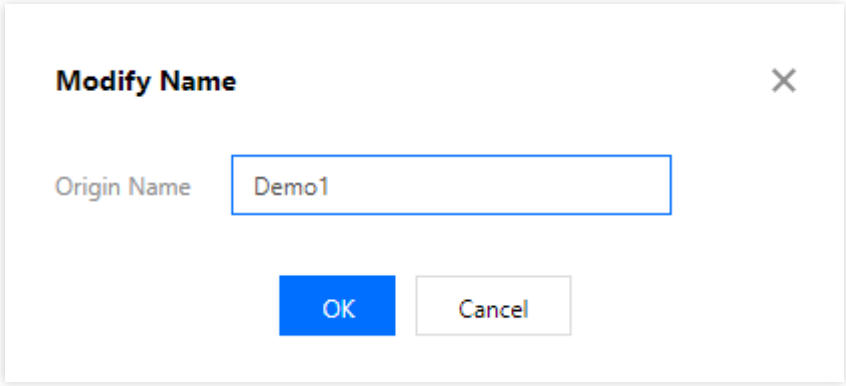


Modifying the Name

1. Log in to the GAAP console. On the **Origin Server Management** page, click the edit icon on the right of the origin server name to modify it.



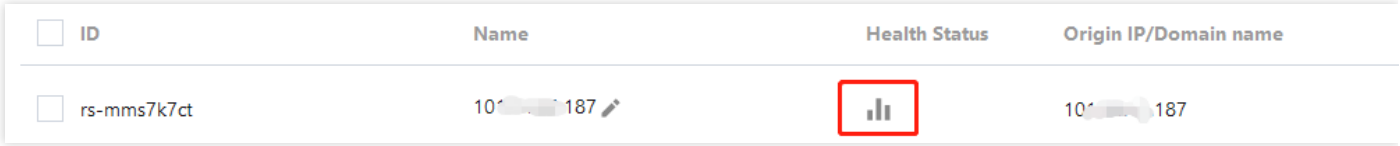
2. In the pop-up dialog, enter a new name and click **OK**.



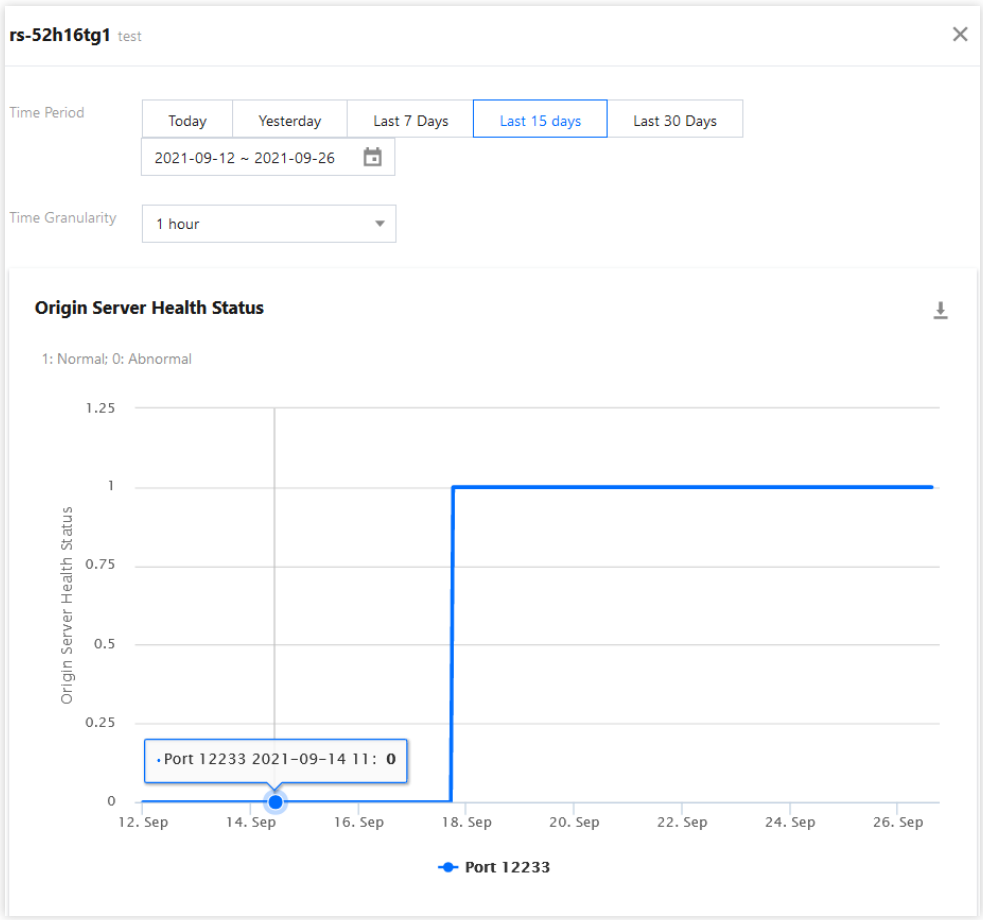
Viewing the Health Status

1. Log in to the GAAP console. On the **Origin Server Management** page, click the icon on the right of the origin server that is healthy.

> Note：
> This feature is unavailable if the origin server is not bound to a listener.

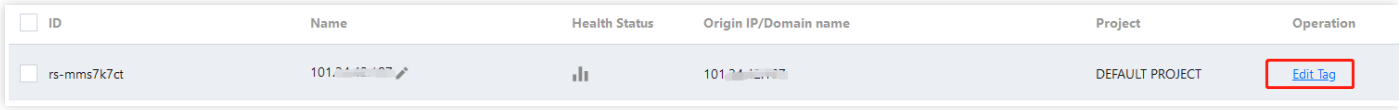


2. On the pop-up window in the top right corner, you can view the health status of the origin server during different periods and granularities. `1` indicates the origin server is normal while `0` means it is abnormal.

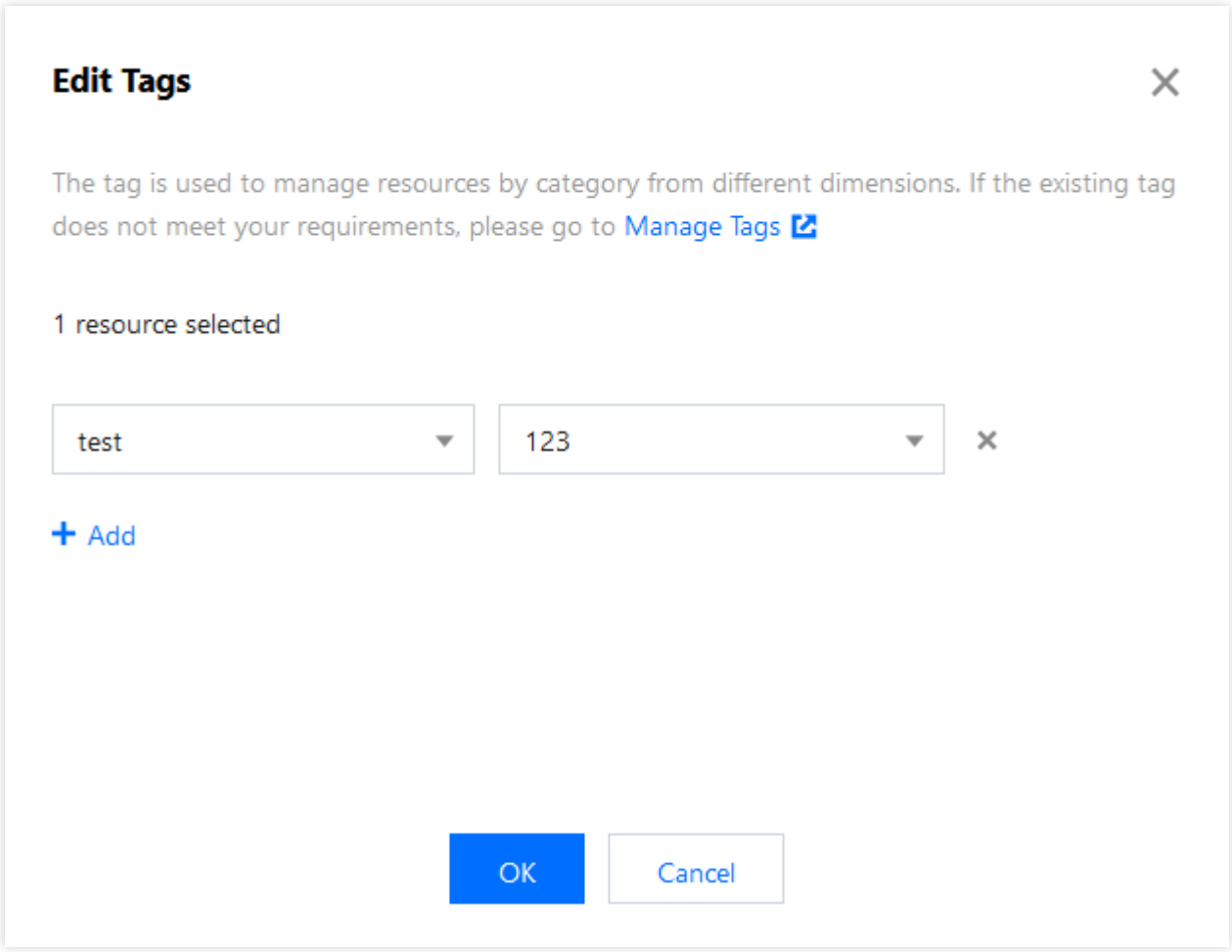


Editing the Tag

1. Log in to the GAAP console. On the **Origin Server Management** page, click **Edit Tag** on the right of the origin server.



2. Select tags to categorize and manage origin servers in multiple dimensions. Click **OK**.



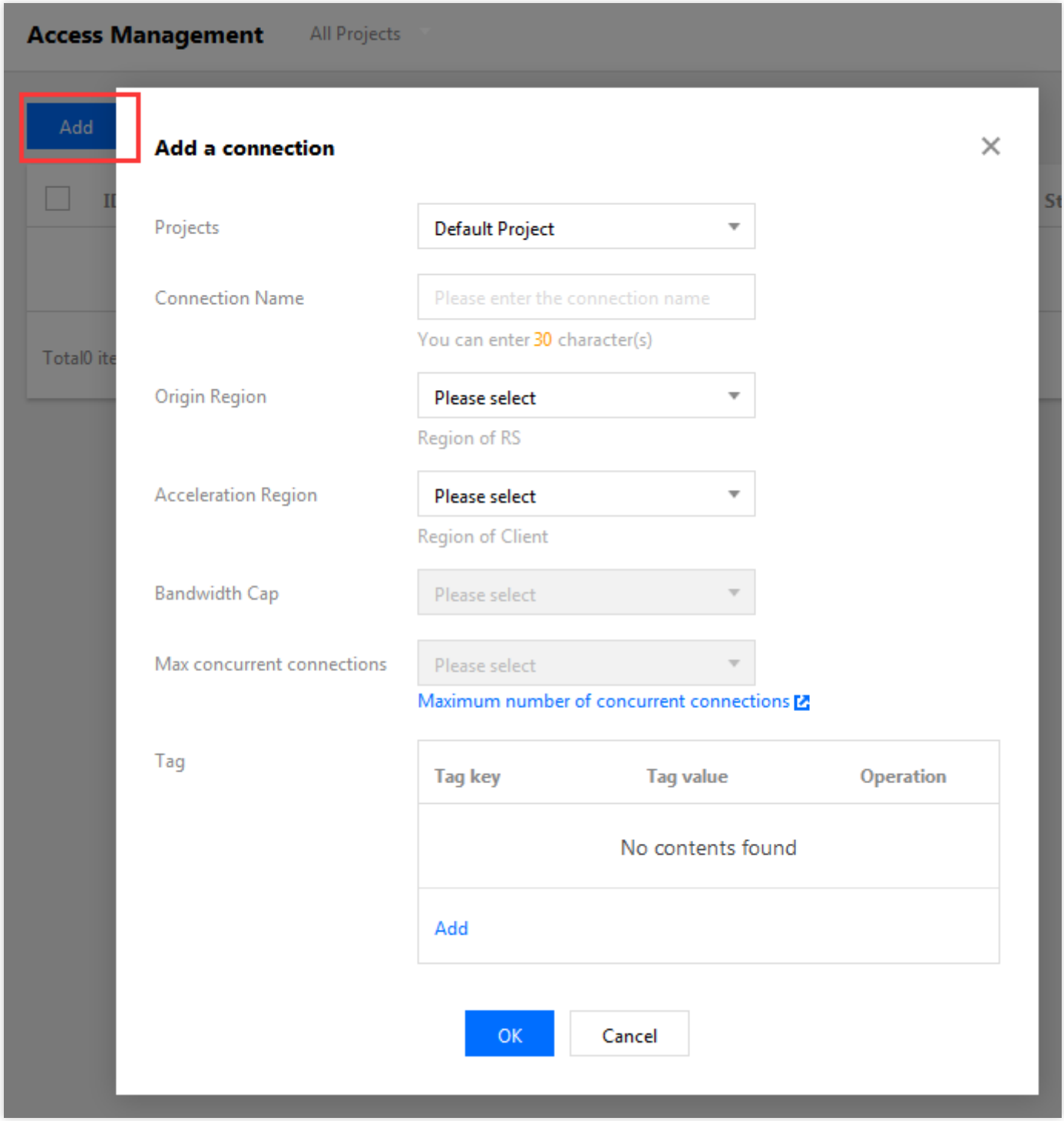
Access Management
Connection Management

Last updated：2022-03-16 18:16:01

Adding a Connection

1. Log in to the GAAP console, enter the **Access Management** page and click **Add**.

2. In the pop-up window, enter the connection information.



- **Project**: The project to which the connection belongs, which can be changed.
- Connection Name: It can contain up to 30 letters and regular symbols.
- **IP Version**: Supports IPv4 or IPv6. IPv6 is only supported for regions in the Chinese mainland.
- HTTP3: Once enabled, the connection supports transfer over the HTTP3 (QUIC) protocol, and only HTTP/HTTPS listeners can be configured (this cannot be **enabled or disabled** after successful connection creation).

- Access Node: Select a node in the client region or the region closest to the client.

  Note：
  - If you need to provide dedicated BGP network access in Hong Kong (China), select "Hong Kong" as the **acceleration region** and select **Dedicated BGP**.
  - A non-BGP node network is available in the Chinese mainland. If you need it, submit a ticket to contact us.

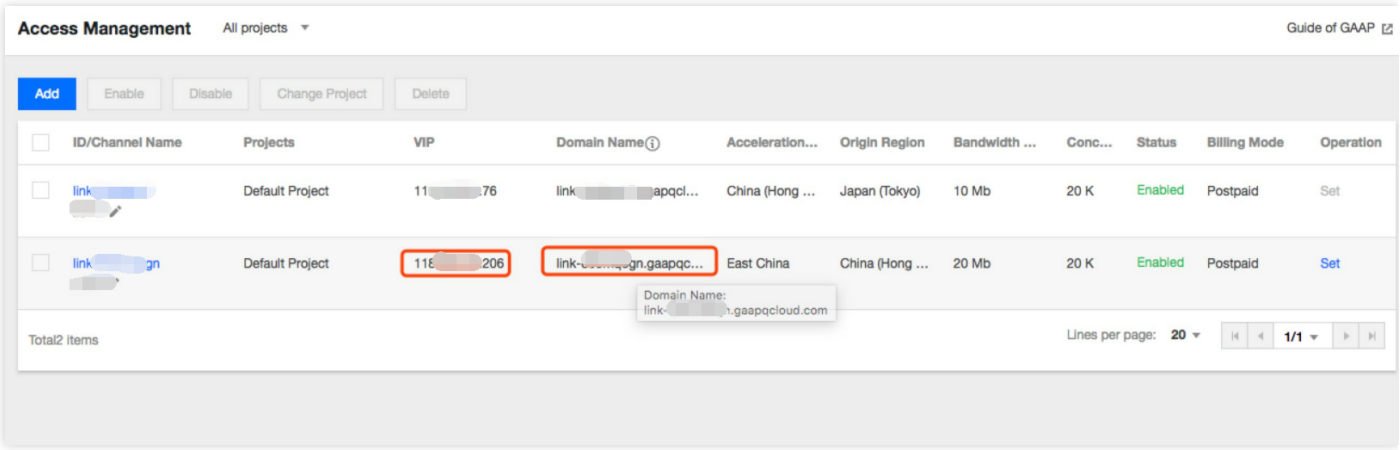
- Origin-Pull Node: Select a node in the destination server region or the region closest to the destination server.

  Note：
  No direct connection can be established between Taiwan (China) and the Chinese mainland.

- **Bandwidth Cap**: Maximum bandwidth of a connection, which is 10000 Mbps (1000 Mbps for some connections).
- **Maximum Concurrent Connections**: Maximum number of concurrent connections for a connection, which is 1 million (300,000 for some connections).
- **Tag**: Supports classifying connections. This is an optional item.
- Fees: The corresponding connection fees and bandwidth fees will be displayed below according to the bandwidth and concurrency you select.
  a. Connection fees: Billed by day until the connection is deleted. Note that connection fees will still be charged for one day even if the connection is deleted less than one day after creation.
  b. Bandwidth fees: Billed by the daily outbound/inbound bandwidth peak.

3. Click **OK**.

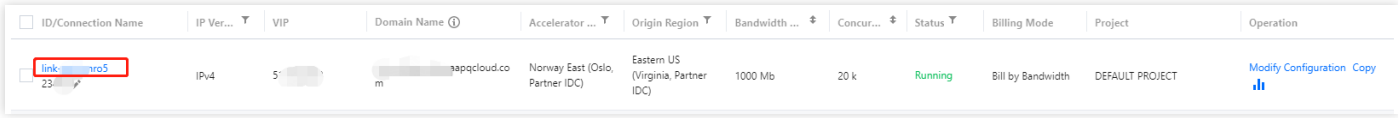
4. On the **Access Management** page, view the connection list information.



- **ID/Connection Name**: ID and name of a connection. The connection name can be changed.
- **VIP**: IP address accessed by the client.
- **Domain Name**: Domain name accessed by the client, which is assigned by the system and automatically bound to the VIP.
- **Status**: Only the acceleration connections in the **Running** status can work normally.

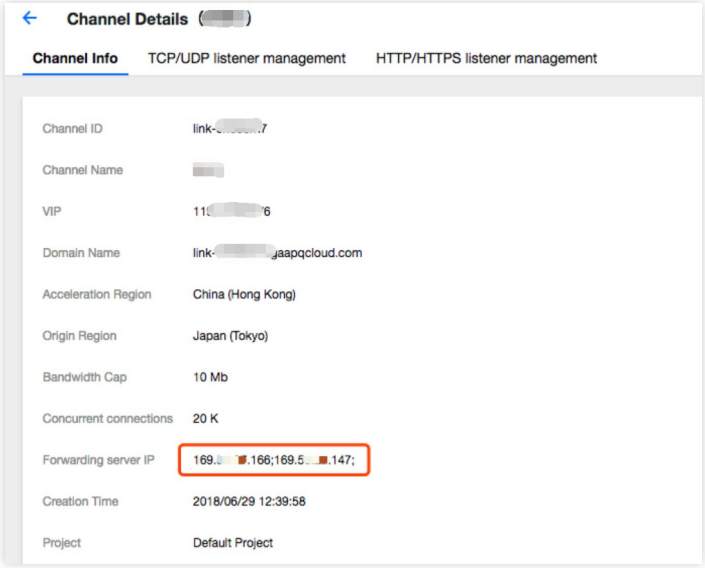
Viewing Connection Information

1. Log in to the GAAP console, enter the **Access Management** page and click **ID/Connection Name** of a connection.



2. On the **Connection Info** tab, you can view the connection details. **Forwarding server IP** refers to the IP of the forwarding node at the end of the acceleration connection, which is responsible for forwarding the data of the connection to the origin server over the public network. If you want multiple connections to use the same domain

name, click **Not Associated** to redirect to the Unified Domain Name page for configuration.



TCP/UDP Listener Management

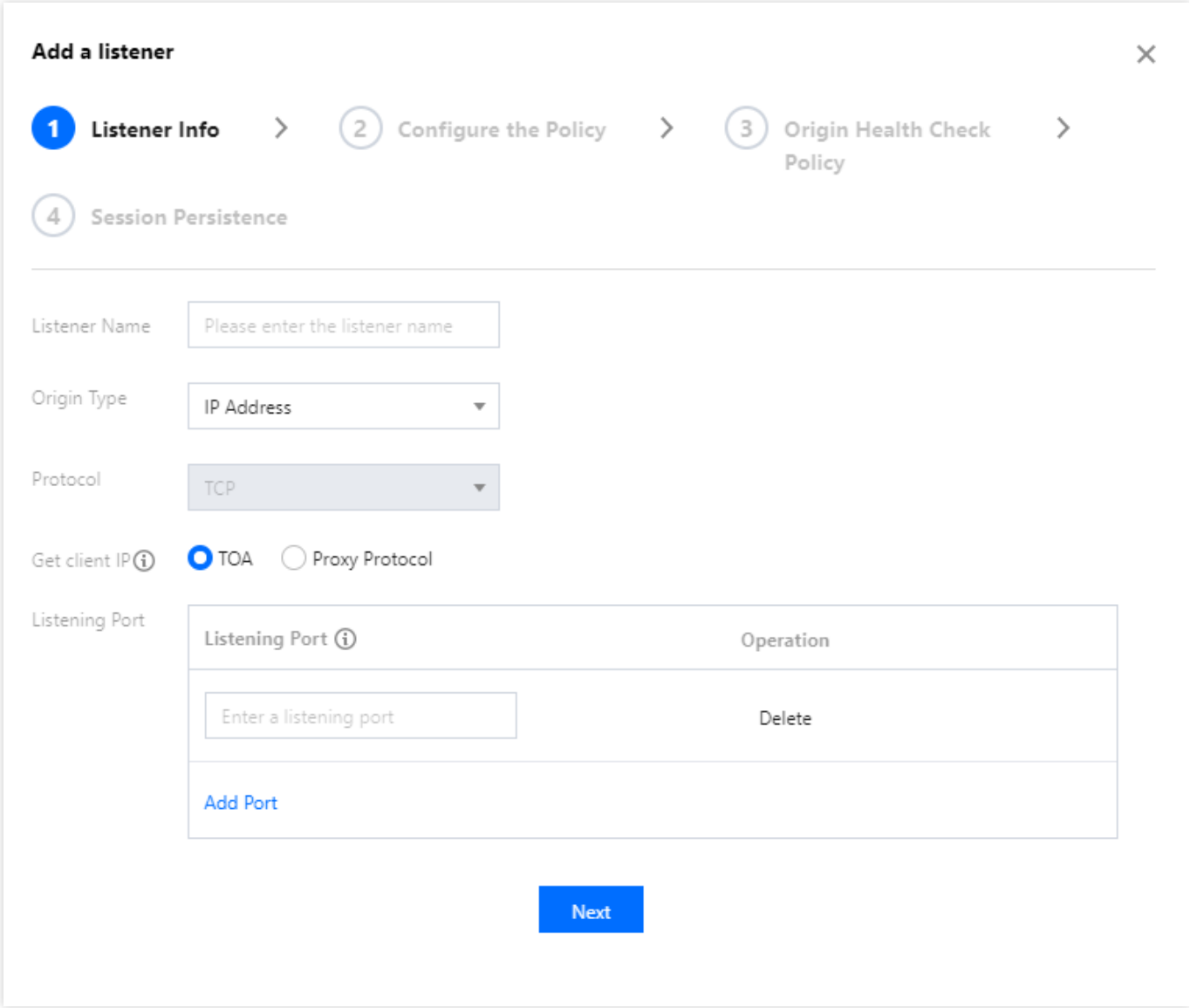
Last updated：2021-12-22 12:30:09

Creating TCP/UDP Listener

1. Log in to the GAAP console, enter the **Access Management** page, and click the **ID/Connection Name** of the specified connection.

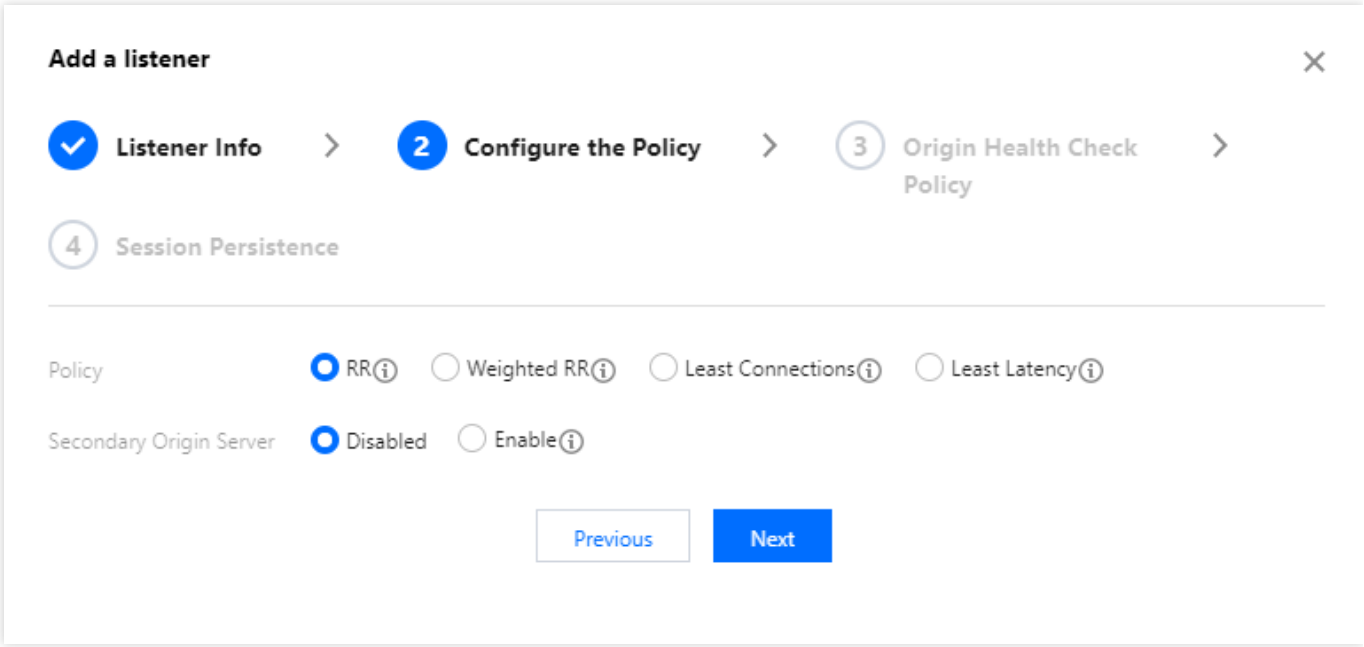
2. On the page that appears, select **TCP/UDP Listener Management** > **Create**. The specific configuration is as follows:

i. Configure the listener information to set the protocol-port mapping.



- Origin Server Type: this can be an IP address or a domain name, but only one type can be selected for one listener. (Note: currently, the domain name type is not supported for IPv6 connections).
- Get Client IP: you can select either TOA or Proxy Protocol to get the user's real IP. For more information, see Basic Principle.
- Listening Port: this is the access port of the acceleration connection VIP. Valid port range: 1–64999 (port 21 is currently unavailable). A single port or a range of consecutive ports is supported. The port must be unique. A maximum of 20 consecutive ports can be added at a time, such as 8000–8019.

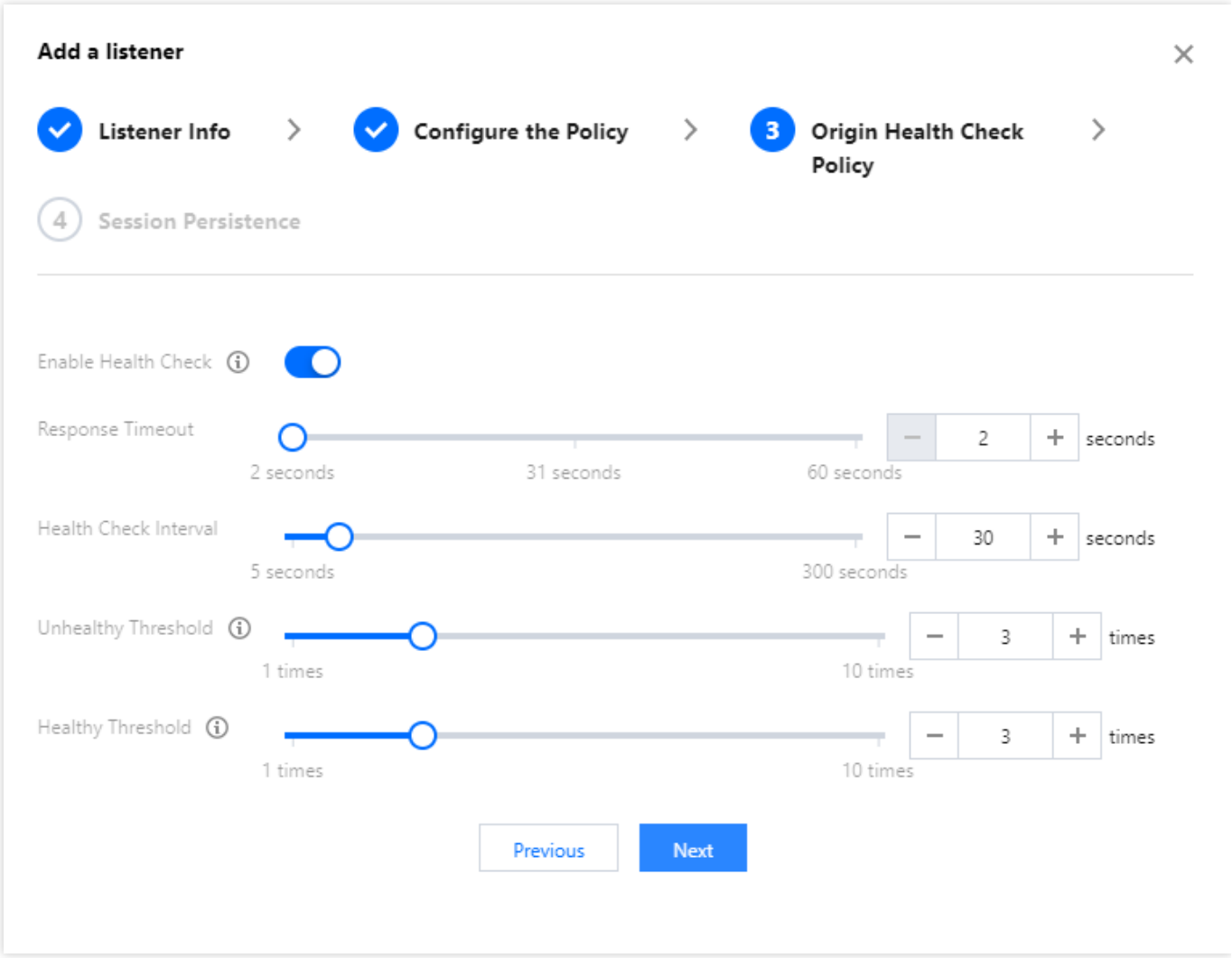
ii. Configure the origin server processing policy; that is, if a listener is bound to multiple origin servers, you need to select a scheduling policy for origin servers.



- RR: multiple origin servers perform origin-pull according to the RR policy.
- Weighted RR: multiple origin servers perform origin-pull according to the weight ratio (you can set the weight of each origin server when binding the listener).
- Least Connections: this means scheduling the origin server with the least number of connections first.
- Least Latency: this means scheduling the origin server with the least latency first.
- Secondary Origin Server: you can choose whether to enable primary/secondary origin server switch (to enable this feature, you must enable origin server health check).

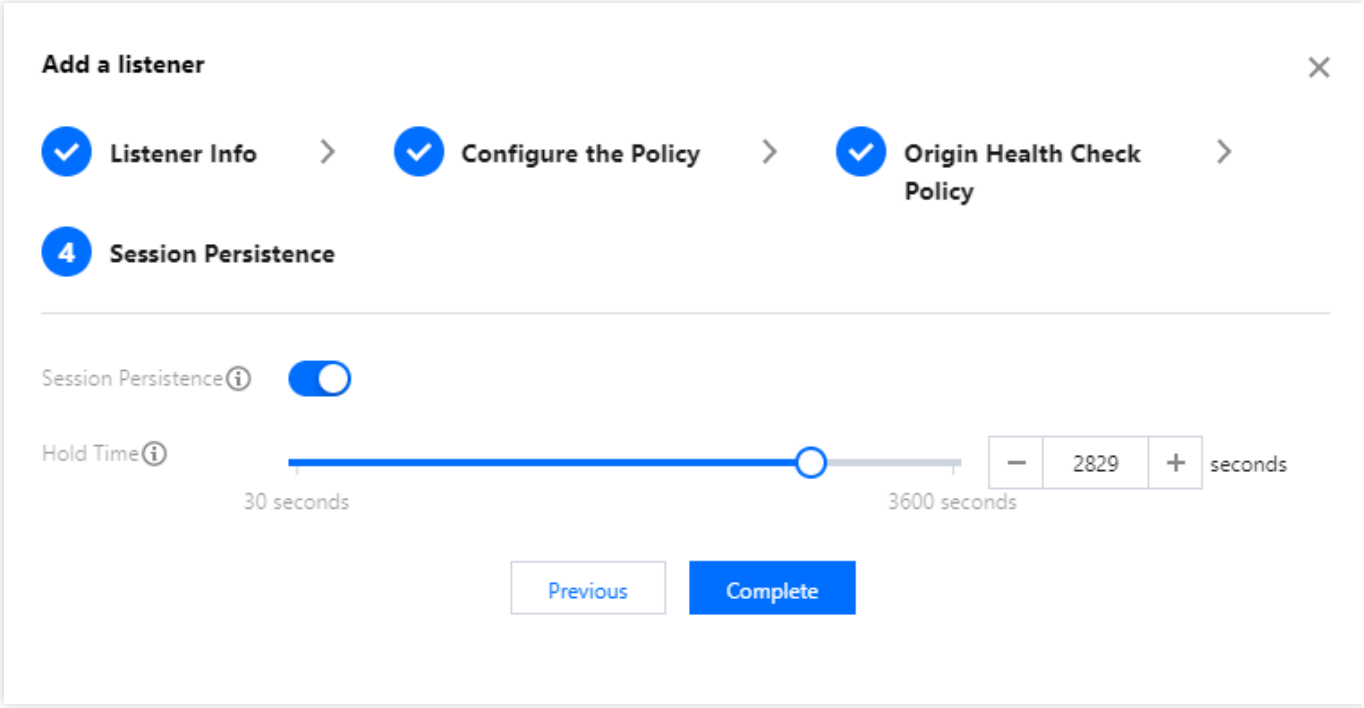
> Note:
> Listeners with domain name-type origin servers only support **RR** and **Least Connections** as the scheduling policy and do not support secondary origin servers.

iii. If a TCP listener is used, you can cofigure health check policies to automatically detect and remove exceptional origin servers. If the secondary origin server is enabled, you will be unable to disable the health check.



- Response Timeout: origin server response timeout period.
- Health Check Interval: the interval between two consecutive health checks.
- Unhealthy Threshold: it indicates the number of consecutive failed checks performed by the monitor before the origin server is considered unhealthy. If an origin server is considered unhealthy during a health check, no more data packets will be forwarded to it until it returns to normal status.
- Healthy Threshold: it indicates the number of consecutive successful checks performed by the monitor before the origin server is considered healthy. If an origin server is considered healthy during a health check, data packets will be forwarded to it again.

iv. Choose whether to enable session persistence.



- Session Persistence: user requests from the same IP will access the same origin server.
- Hold Time: session persistence duration. When the listener has no requests for a period longer than the hold time, session persistence will be automatically disconnected.

3. Click **Complete**.

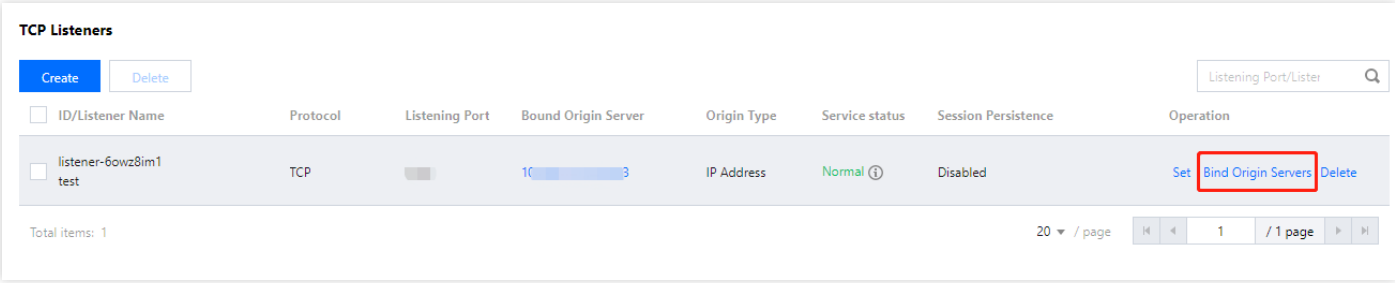
Configuring TCP/UDP Listener

Click the **TCP/UDP Listener Management** tab and click **Settings** in the **Operation** column of a listener to rename it or modify its scheduling policy and health check parameters.

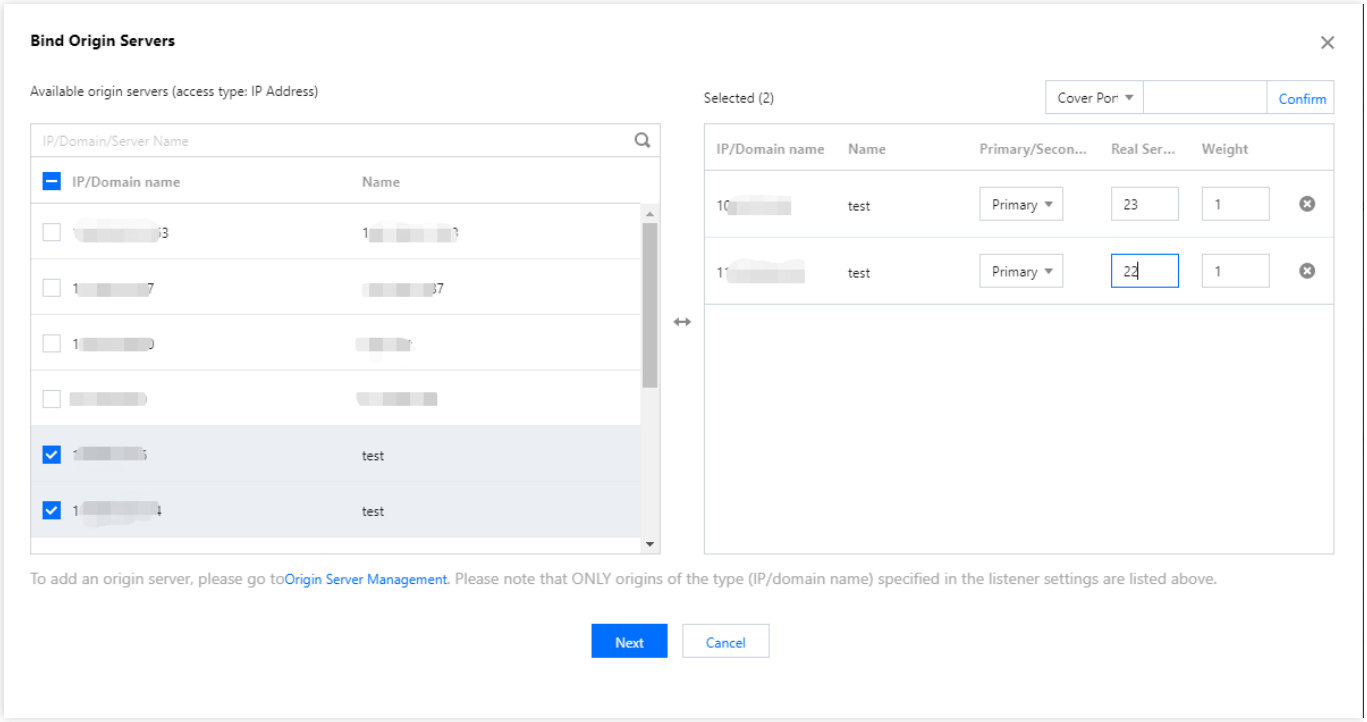
Binding Origin Server

1. Select the **TCP/UDP Listener Management** tab and click **Bind Origin Server** in the **Operation** column of a created "TCP/UDP listener" to bind or unbind one or more origin servers. If no origin server information is found as displayed in the console, it may be that the origin server type is invalid or the origin server is not added to Origin

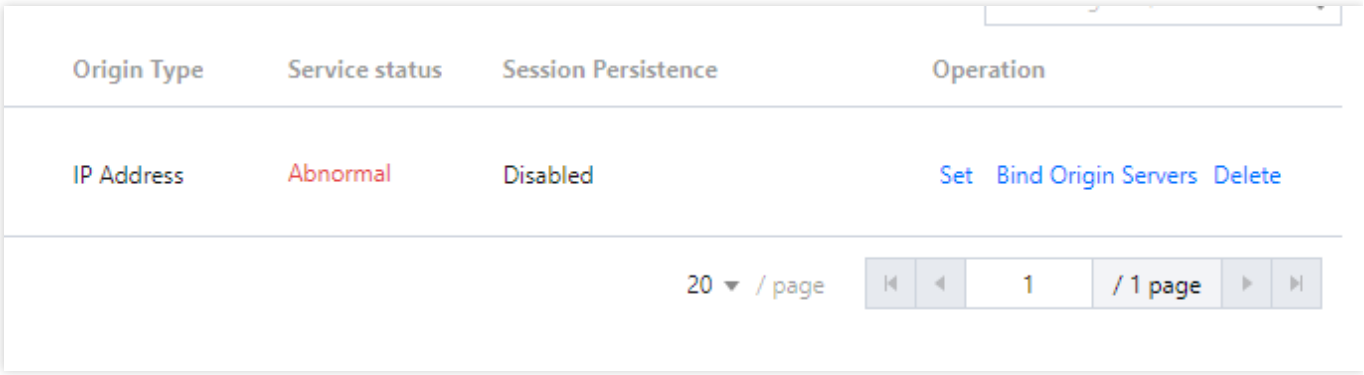
Server Management.



2. Select an origin server and configure an origin-pull port.
   - If primary/secondary RR is enabled for a listener, you need to set the **Primary Origin Server** and **Secondary Origin Server** on the **Bind Origin Server** page.
   - If you want to set the ports of multiple origin servers, you can use the **Cover Port**/**Complement Port** features in the top-right corner. Regardless of the origin server ports you previously set, the **Cover Port** feature will set the destination origin servers you select to the port number you entered. If no port has been set for any of the selected destination origin servers, you can use the **Complement Port** feature for a unified setting to reduce the repetitive workload.
   - If the listener policy is **Weighted RR**, you can set the weight (1–100) of an origin server when binding it. The origin server is scheduled based on the ratio of its weight to the total weight. For example, if the weight of origin server 1 is 60 and that of origin server 2 is 80, then the scheduling ratio will be 60/(60 + 80) = 42.8% for origin server 1 or 57.2% for origin server 2.

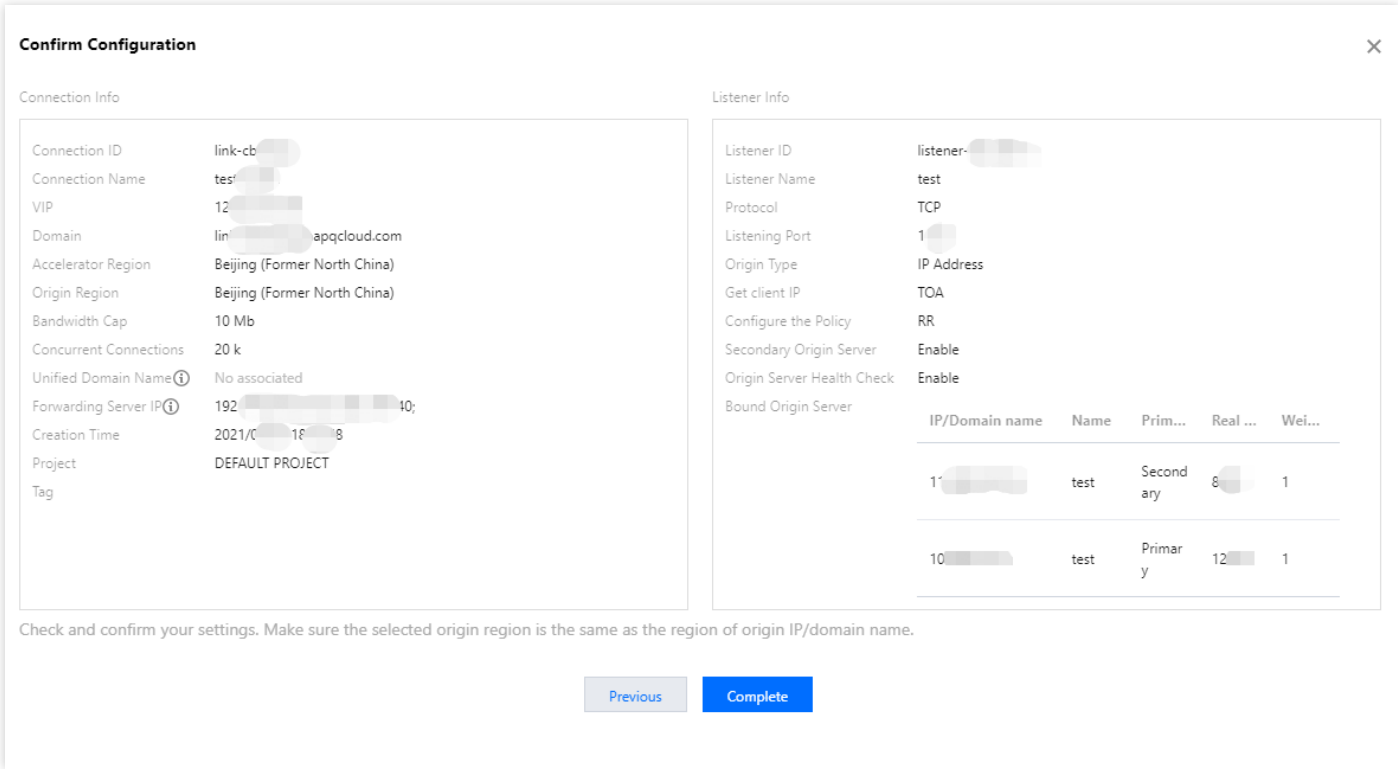


- If enabled, a health check will start when the origin server is bound. You can determine whether the origin server is normal by checking the listener status. An acceleration connection will only forward packets to origin servers in normal status. Packets will not be forwarded to exceptional origin servers until they return to normal status during the health check.
- If you don't enable the health check, or if you use a UDP listener, the acceleration connection will always forward packets regardless of the status of the origin server.



3. Confirm the configuration.

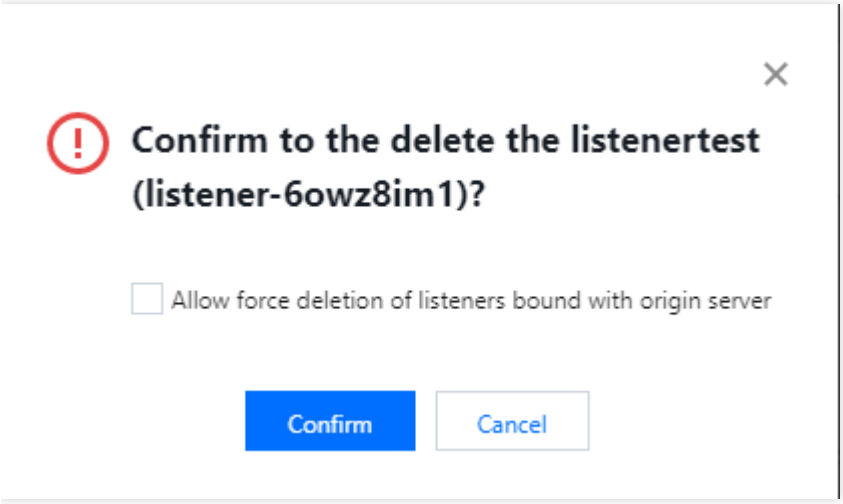
   After completing the origin server configuration, click **Next** to enter the configuration confirmation page, where you can view the currently configured connection information and listener details.



4. Click **Complete**.

Deleting TCP/UDP Listener

Open the **TCP/UDP Listener Management** tab and click **Delete** in the **Operation** column of the specified listener to be deleted. If the listener is bound to an origin server, you need to select **Allow force deletion of listeners with bound origin servers** first. After deletion, the acceleration service for the listener's port will stop.

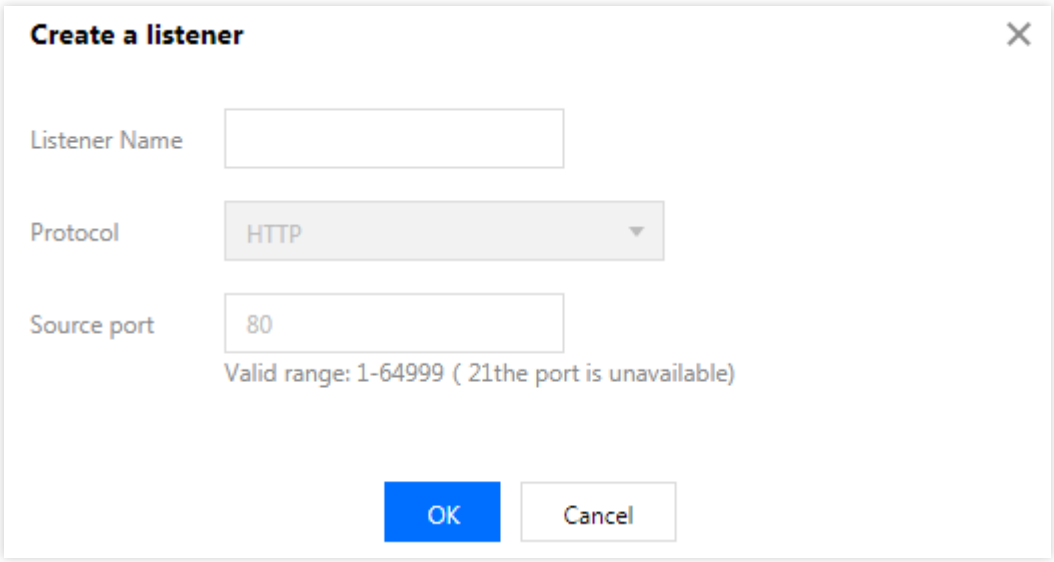


HTTP/HTTPS Listener Management

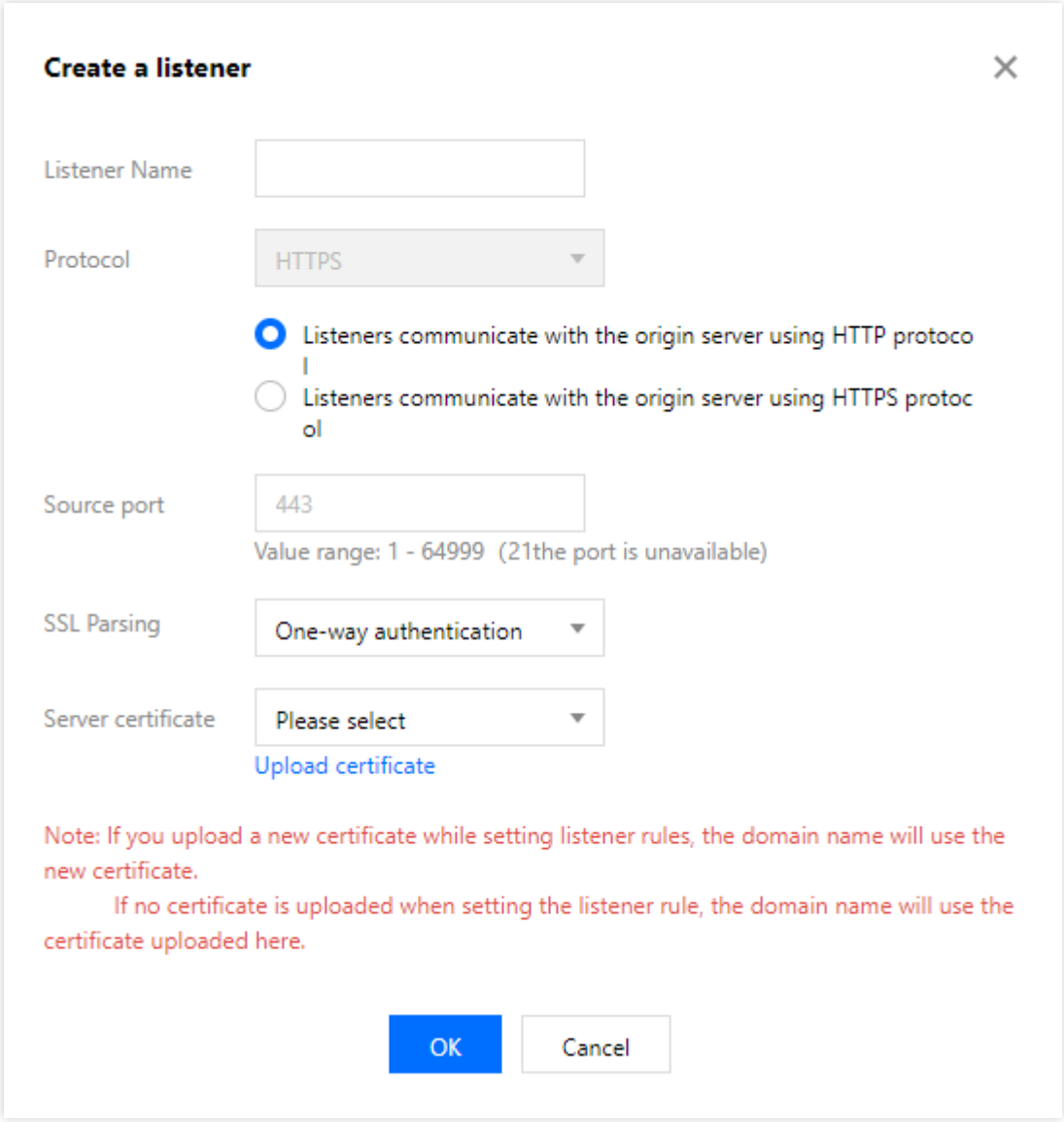
Last updated：2022-06-20 15:51:05

Adding an HTTP/HTTPS Listener

1. Log in to the GAAP console. Enter the **Access Management** page. Click the **ID/Connection Name** of the specific connection.
2. On the page that appears, select **HTTP/HTTPS Listener Management** > **Create**. You can select either the HTTP or HTTPS protocol. (Note: currently, HTTP/HTTPS listener configuration is not supported for IPv6 connections.)
3. The specific configuration is as follows:
   i. If **HTTP** is selected, only the listener port number is required, and the listener will forward packets using the HTTP protocol by default.



ii. If **HTTPS** is selected, certificates and additional information need to be configured, as shown below:



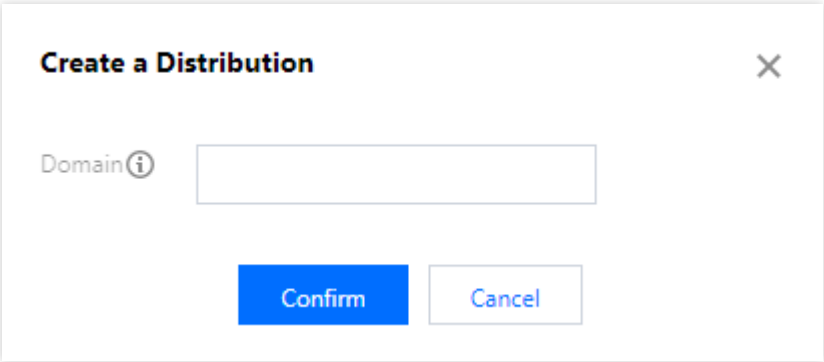
- **Listeners communicate with the origin server using HTTP protocol** means that the HTTPS protocol is used between the client and the acceleration connection VIP, while the HTTP protocol is used between the VIP and the origin server, which requires an HTTP port to be opened on the origin server;
  Listeners communicate with the origin server using HTTPS protocol means that the HTTPS protocol is used between the client and the origin server, which requires an HTTPS port to be opened on the origin server.
- **SSL Parsing**: Both one-way and two-way authentication are supported.
- **Server/Client Certificate**: Upload/Update a certificate in **Certificate Management** of the GAAP console, and then select the certificate when creating/modifying an HTTPS listener. For more information, see Certificate Management.

Configuring an HTTP/HTTPS Listener

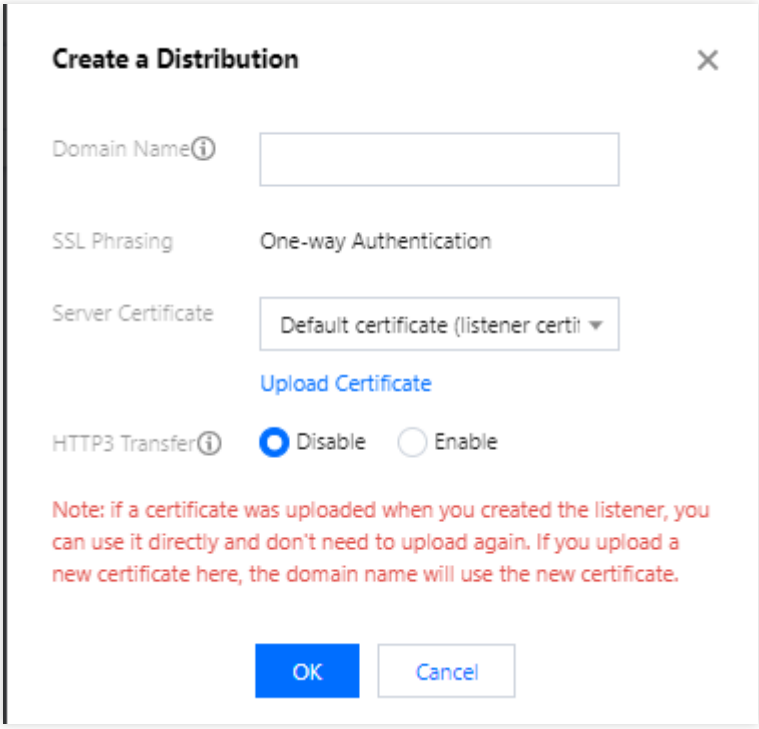
Under the **HTTP/HTTPS Listener Management** tab, click **Set a rule** in the operation column to enter the domain name and URL management page.

Creating a distribution

1. To add a domain name for an HTTP listener, enter a valid domain name. It must be 3 to 80 characters containing [a-z], [0–9], [.-]. Only exact match is supported.



2. To add a domain name for an HTTPS listener, enter a valid domain name and select the corresponding server certificate.



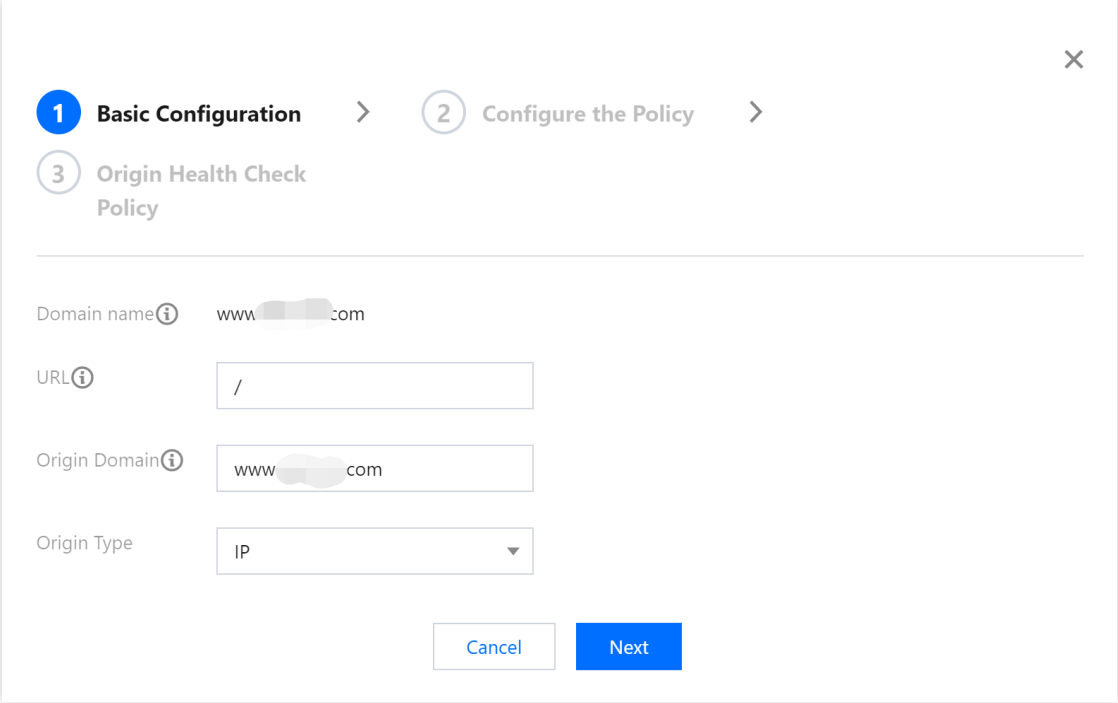
- **Domain**: 3 to 80 characters containing [a-z], [0–9], [.-]. Only exact match is supported.

- **Server Certificate**: by default, it is the certificate used to create the listener. If you upload another certificate, the domain name is authenticated with the uploaded certificate.
- **HTTP3 Transfer**: enables it to support QUIC. If the client does not support this protocol, HTTP2.0 and previous versions will be used for access.

Adding a rule

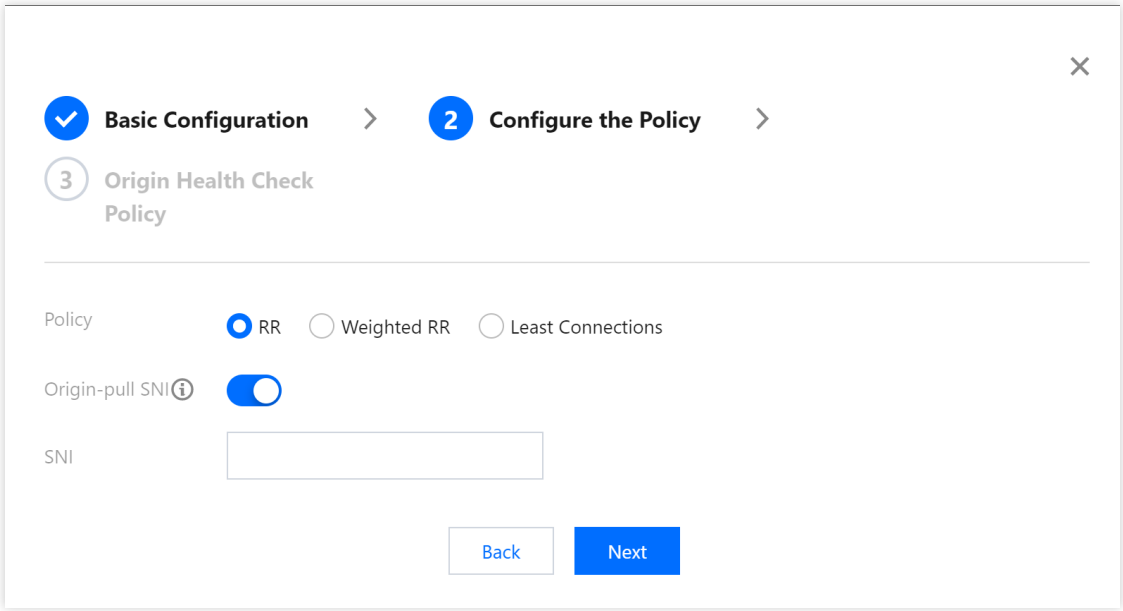
After adding a domain name, click **Add Rule** to add the corresponding URL and select the origin server type. You can add up to 20 URL rules for one domain name as shown below:

1. Basic configuration:



- **URL**: It contains 1-80 characters in the following types: [a-z], [0–9], and [_.-/].
- **Origin Domain**: The host field of the origin-pull request can be modified.
- **Origin Server Type**: It supports an IP or a domain name. A listener supports only one type.

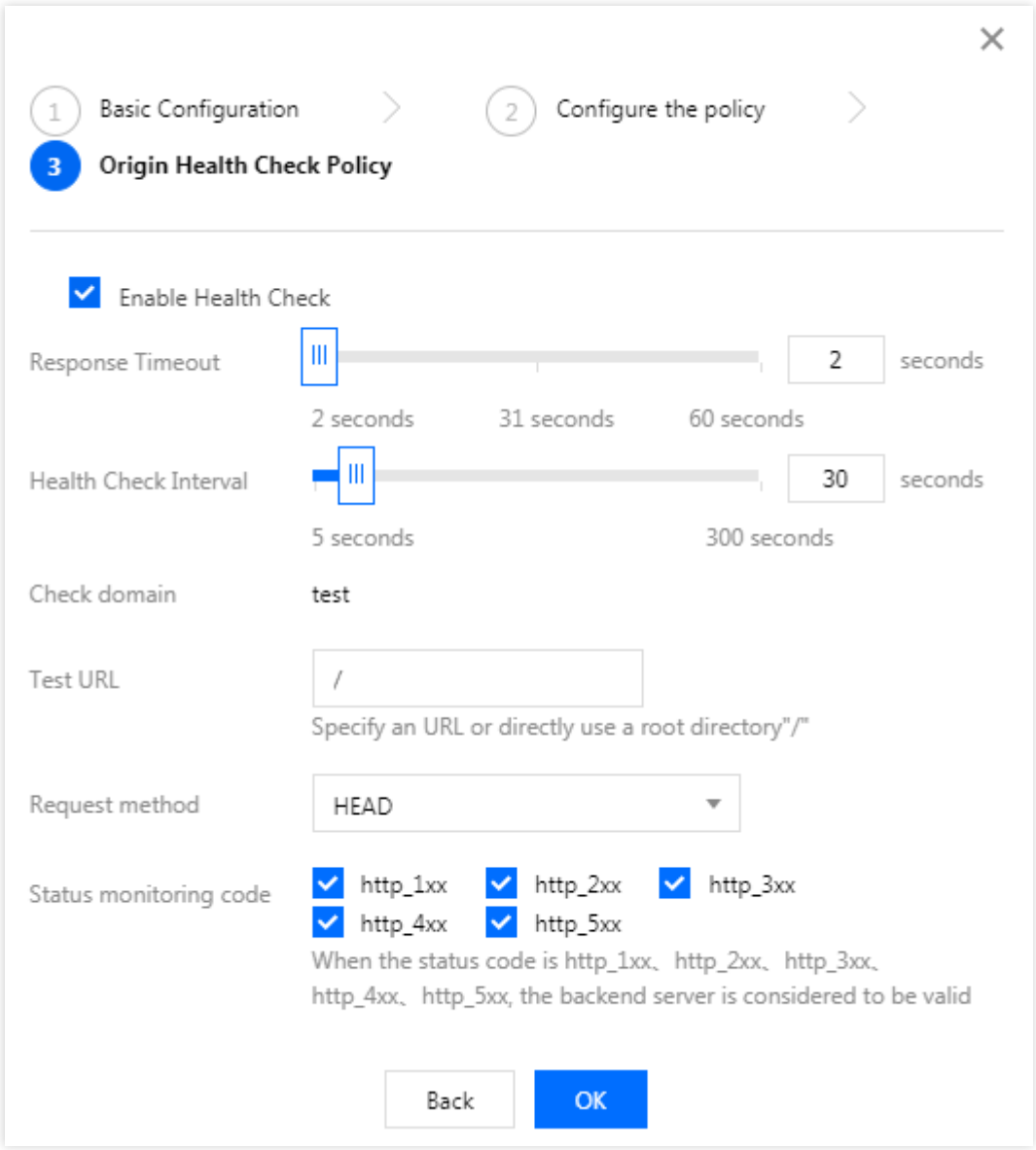
2. Processing policy for the origin server:
   Configure the origin server processing policy, that is, if a listener is bound with multiple origin servers, you need to select a scheduling policy for origin servers.



- **RR**: Multiple origin servers perform origin-pull according to the RR policy.
- **Weighted RR**: Multiple origin servers perform origin-pull according to the weight ratio (this configuration is not supported if the origin server type is a domain name).
- **Least Connections**: It schedules the origin server with the least number of connections first.
- **Origin-pull SNI**: It forwards SNI to the origin server before an SSL connection is established, and based on the SNI value the origin server returns a certificate.

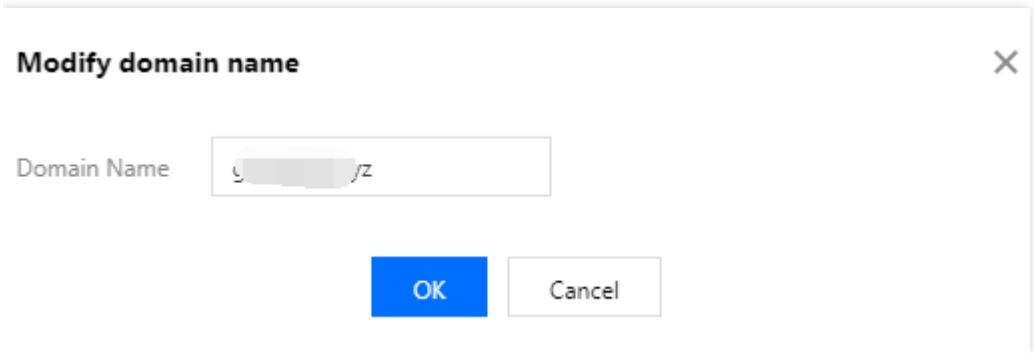
3. Origin health check mechanism:
   The health check mechanism can be enabled. For the current domain name, you can configure an independent check URL. HEAD and GET request methods are supported. Check status codes include http_1xx, http_2xx, http_3xx, http_4xx, and http_5xx, and one or multiple codes can be selected. When a specified status code is detected, the listener considers that the backend origin server is normal. If no status code is detected, the listener

considers that the backend origin server has an exception.



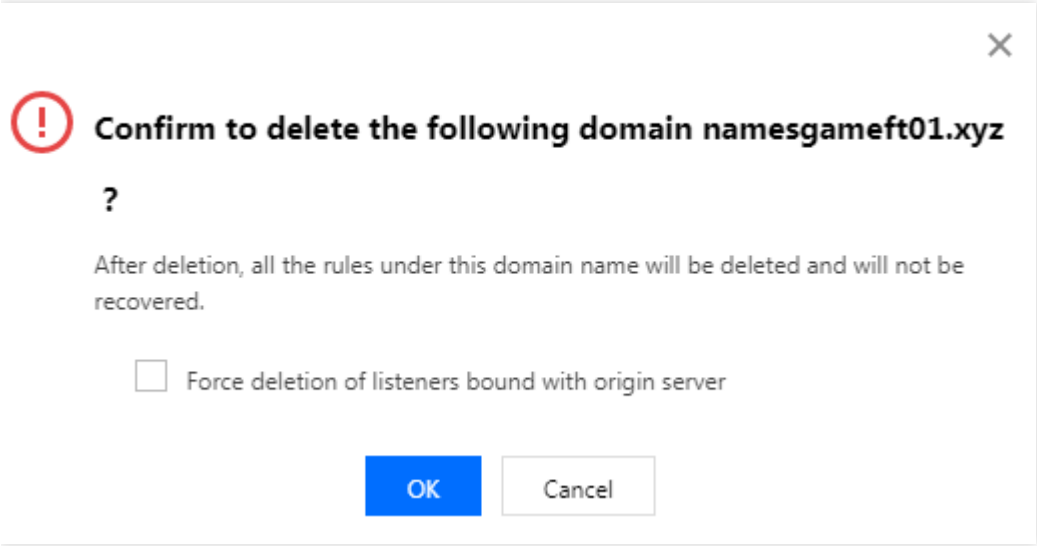
Modifying a domain name

After adding a domain name, you can click **Modify Domain Name** to modify the domain name.



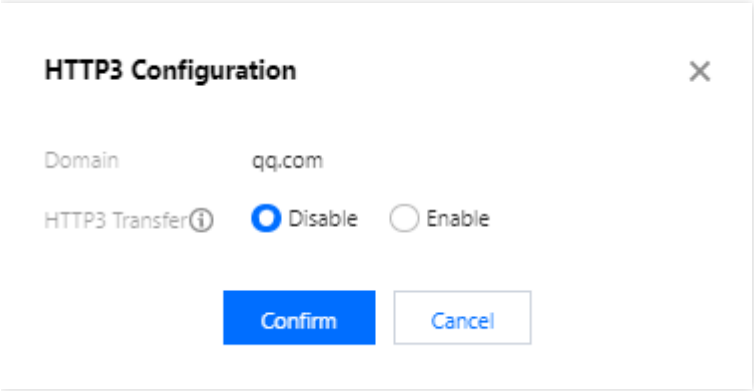
Deleting a domain name

After adding a domain name, you can click **Delete** to delete the domain name. If a rule under the domain name has been bound to an origin server, you need to select **Force deletion of listeners bound with origin server**.



HTTP3 configuration

The HTTP3 configuration controls whether to support HTTP3 (QUIC). Currently, HTTP3 can only be configured for HTTPS listeners.



Modifying a rule

Refer to the **Adding a rule** section above. The main difference is that the domain name and origin server type cannot be modified.

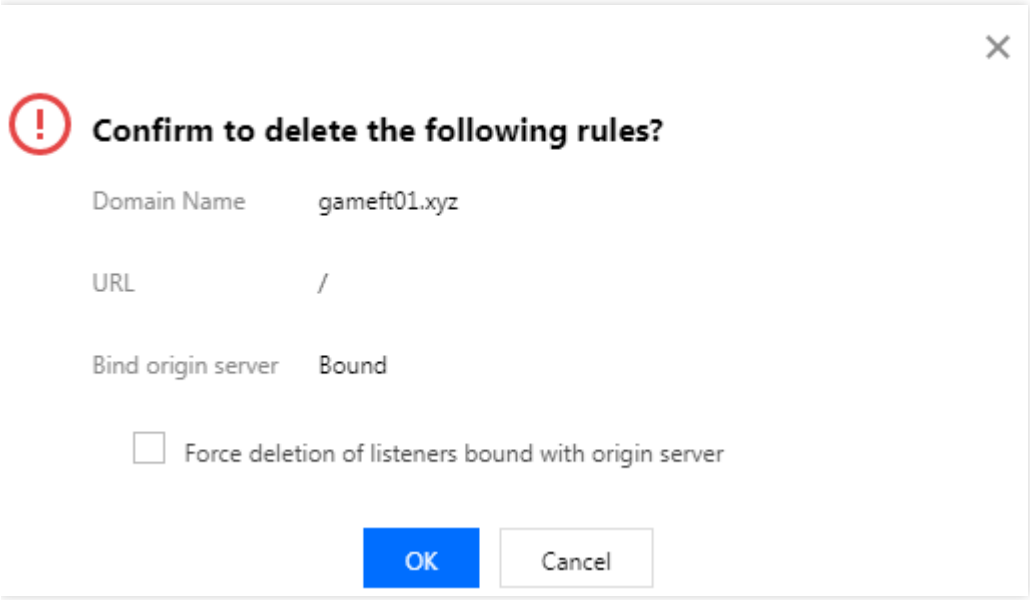
Binding an origin server

For more information, see Binding Origin Server. You can bind different ports to different origin servers. For more information on the **Cover Port** and **Complement Port** features, see Binding TCP/UDP Listener to Origin Server.

Note：
A rule can be bound to up to 100 origin servers.

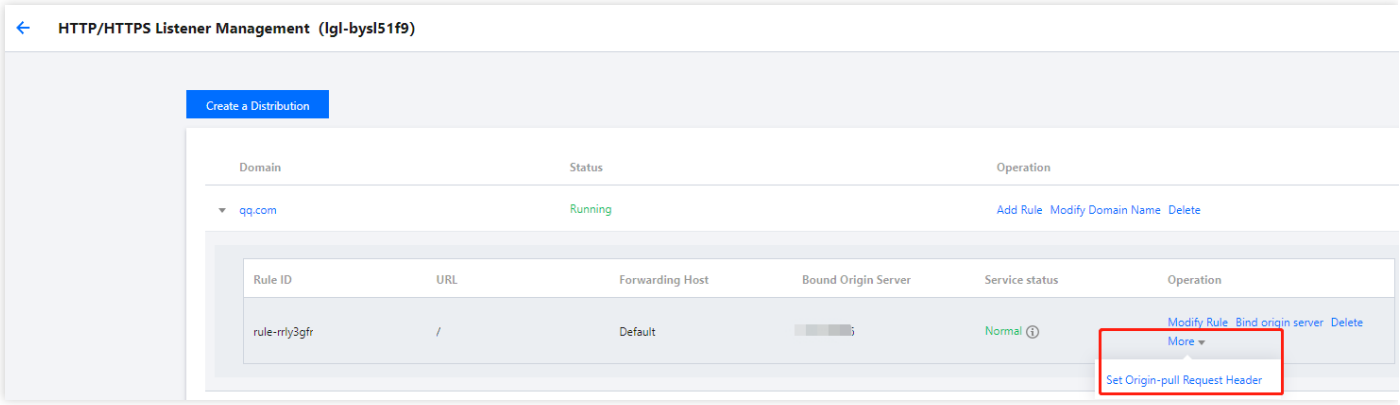
Deleting a rule

After adding a rule, you can click **Delete** to delete the rule. If the rule has been bound to an origin server, you need to select **Force deletion of listeners bound with origin server** first.



Configuring origin-pull request header

1. After adding a rule, you can select **More** in the **Operation** column of the rule and click **Set Origin-Pull Request Header**.



2. Click **Add Parameter** and enter the request header's name and value. The `$remote_addr` variable can be used to specify the real client IP carried in the request header (by default, the `X-Forwarded-For` header carries the client IP for origin-pull). To use other variables with `$`, please submit a ticket.

Note：

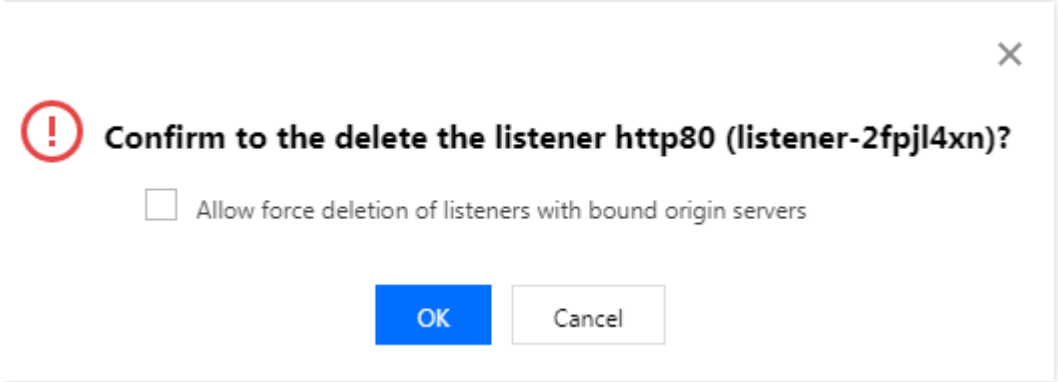
1. The `Key` value of the HTTP header name can contain 1–100 digits (0–9), letters (a–z, A–Z), and special symbols (-, _, :, and space). The `Value` can contain 1–100 characters;
2. Up to 10 origin-pull HTTP request headers can be configured for each rule;
3. The standard headers listed below cannot be set/added/deleted in a self-service manner.

www-authenticate	authorization	proxy-authenticate	proxy-authorization
age	cache-control	clear-site-data	expires
pragma	warning	accept-ch	accept-ch-lifetime
early-data	content-dpr	dpr	device-memory
save-data	viewport-width	width	last-modified
etag	if-match	if-none-match	if-modified-since
if-unmodified-since	vary	connection	keep-alive
Accept	accept-charset	expect	max-forwards
access-control-allow-origin	access-control-max-age	access-control-allow-headers	access-control-allow-methods
access-control-expose-headers	access-control-allow-credentials	access-control-request-headers	access-control-request-method
origin	timing-allow-origin	dnt	tk
content-disposition	content-length	content-type	content-encoding
content-language	content-location	forwarded	x-forwarded-host
x-forwarded-proto	via	from	host
referer-policy	allow	server	accept-ranges
range	if-range	content-range	cross-origin-embedder-policy
cross-origin-opener-policy	cross-origin-resource-policy	content-security-policy	content-security-policy-report-only
expect-ct	feature-policy	strict-transport-security	upgrade-insecure-

			requests
x-content-type-options	x-download-options	x-frame-options(xfo)	x-permitted-cross-domain-policies
x-powered-by	x-xss-protection	public-key-pins	public-key-pins-report-only
sec-fetch-site	sec-fetch-mode	sec-fetch-user	sec-fetch-dest
last-event-id	nel	ping-from	ping-to
report-to	transfer-encoding	te	trailer
sec-websocket-key	sec-websocket-extensions	sec-websocket-accept	sec-websocket-protocol
sec-websocket-version	accept-push-policy	accept-signature	alt-svc
date	large-allocation	link	push-policy
retry-after	signature	signed-headers	server-timing
service-worker-allowed	sourcemap	upgrade	x-dns-prefetch-control
x-firefox-spdy	x-pingback	x-requested-with	x-robots-tag
x-ua-compatible	max-age		

Deleting an HTTP/HTTPS Listener

Open the **HTTP/HTTPS Listener Management** tab, click **Delete** on the right of the selected listener. If the listener has been bound with the origin server, you need to check **Allow force deletion of listeners bound with origin servers** first. After it is deleted, acceleration of the listener port will stop.



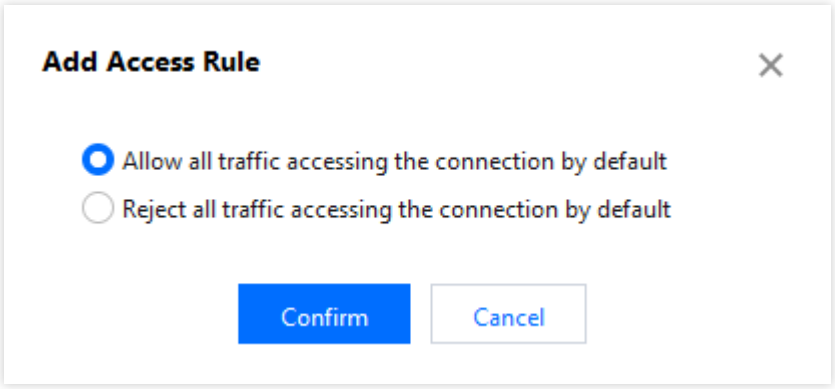
Security Protection

Last updated：2023-06-07 15:03:59

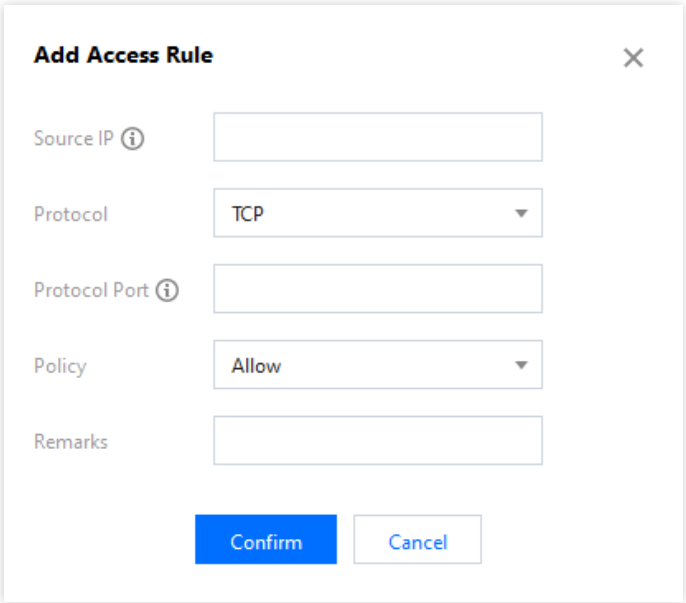
Global Application Acceleration Platform (GAAP) provides a basic security protection plan by default (2 Gbps of bandwidth for general users and 10 Gpbs for VIP users). For higher level of protection, go to **Assets on Cloud** to upgrade in the Anti-DDoS Pro console.

The GAAP console also allows you to configure a blocklist/allowlist. You can configure it as follows:

1. Log in to the GAAP console, enter **Access Management** page, and click **ID/Connection Name** of the selected connection.
2. Select **Attack Defense** > **Add Rule**, and perform the following configuration steps:
   i. Add an access rule and choose to allow or deny all traffic accessing the connection by default.



   ii. Add a source IP, select a protocol and add a protocol port. Then choose **Allow** or **Reject** to process access



   from the IP.

Note：

i. A maximum of 100 access rules can be added.

3. Click **Confirm**.

Access Acceleration Connection

Last updated：2021-12-14 13:00:48

TCP/UDP Protocol

Acceleration connection can be accessed by the following ways:

- The client accesses the "VIP + port" of the acceleration connection.
- The client accesses the "domain name + port" of the acceleration connection.
- If the client originally accesses a domain name, configure a cname to resolve this domain name to that of the acceleration connection, or modify the local host of the client to resolve the original domain name to the acceleration connection's VIP.
  If the origin server needs to get the real client IP (TCP protocol only), TOA module should be installed. For more information, please see Get Real Client IPs (TCP).

HTTP/HTTPS Protocol

Configure a cname to resolve the domain name accessed by the client to acceleration connection's domain name, or modify the local host of the client to resolve the domain name to be accessed by the client to the acceleration connection's VIP, so that the client can access the connection with `protocol + URL` to achieve acceleration. The origin server can directly get the real client IP from the `x-forward-for` field in the HTTP request header.

Connection Group Management

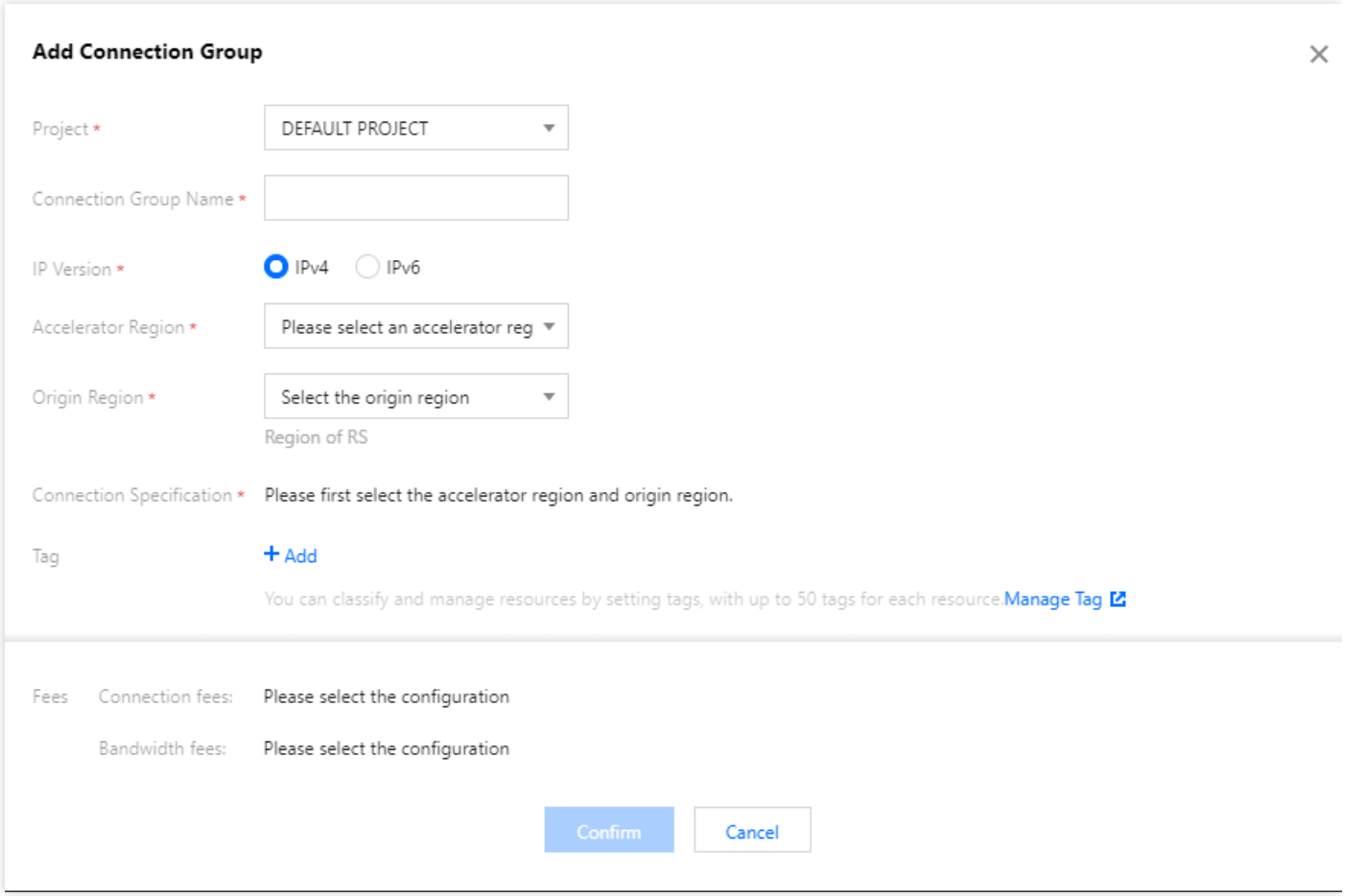
Last updated：2021-12-14 13:00:48

Creating Connection Group

If you need to accelerate access in multiple regions with the same origin server region and listener configuration, you can configure and manage connections in batches through a connection group, which reduces the repetitive work involved in managing individual connections.

1. Log in to the GAAP console, enter the **Connection Group Management** page, and click **Create**.

2. In the pop-up window, enter the connection group information.



- Project: the project to which the connection group belongs, which can be changed.
- Connection Group Name: it can contain up to 30 characters.

- IP Version: select IPv4 or IPv6 as needed. Currently, IPv6 is supported only for access nodes in the Chinese mainland.
- Access Node: select one or multiple nodes in the client region or the region closest to the client.

> Note:
> - A premium BGP network is available in Hong Kong (China). If you need it, submit a ticket to contact us.
> - A non-BGP node network is available in the Chinese mainland. If you need it, submit a ticket to contact us.

- Origin Server Region: select a node in the destination server region or the region closest to the destination server.

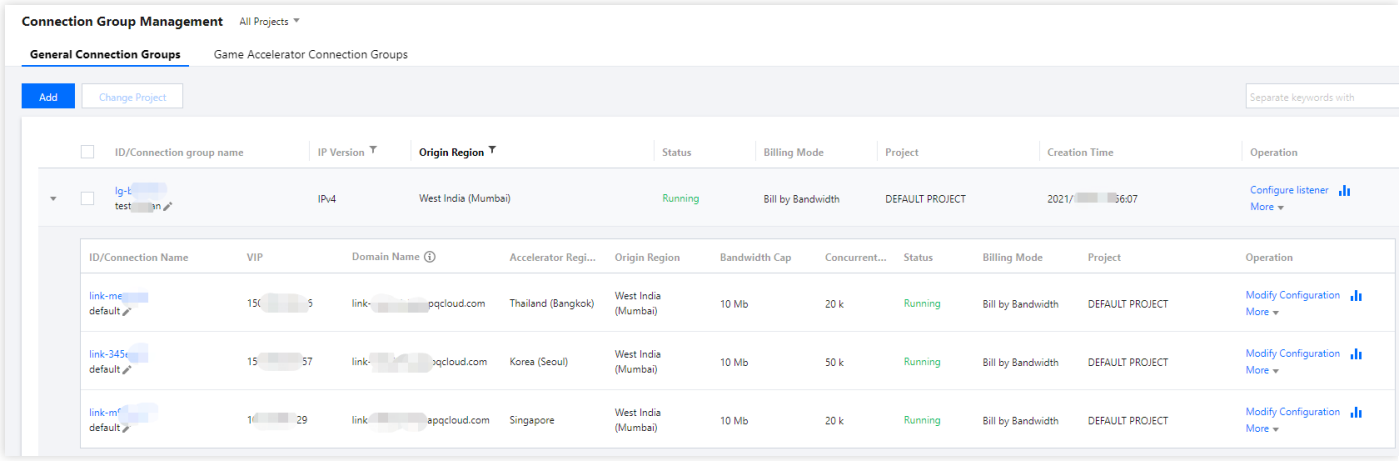
> Note:
> No direct connection can be established between Taiwan (China) and the Chinese mainland.

- Connection Specification: select the bandwidth cap and maximum number of concurrent connections for each connection.
- Bandwidth Cap: the upper limit of the connection's bandwidth is 10,000 Mbps (or 1,000 Mbps for certain connections).
- Maximum Concurrent Connections: the maximum number of concurrent connections supported by a connection is 1 million (or 300,000 for certain connections).

> Note:
> A connection group can contain up to 20 connections.

- Tag: you can optionally set tags to categorize connections for management.
- Fees: the corresponding connection fees and bandwidth fees will be displayed below according to the bandwidth and concurrency you select.
  a. Connection fees: billed by day until the connection is deleted. Note that connection fees will still be charged for one day even if the connection is deleted less than one day after creation.
  b. Bandwidth fees: billed by the daily outbound/inbound bandwidth peak.

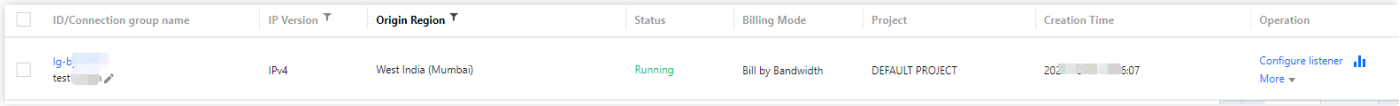
3. Click **OK**.
4. On the Connection Group Management page, view the connection group list information. You can manage different connections in a connection group based on your actual needs and monitor their real-time running status.



- ID/Connection Group Name: ID and name (customizable) of the connection group.
- VIP: IP address accessed by the client.
- Domain Name: domain name accessed by the client, which is assigned by the system and automatically bound to the VIP.
- Status: only the acceleration connections in the **Running** status can work normally.

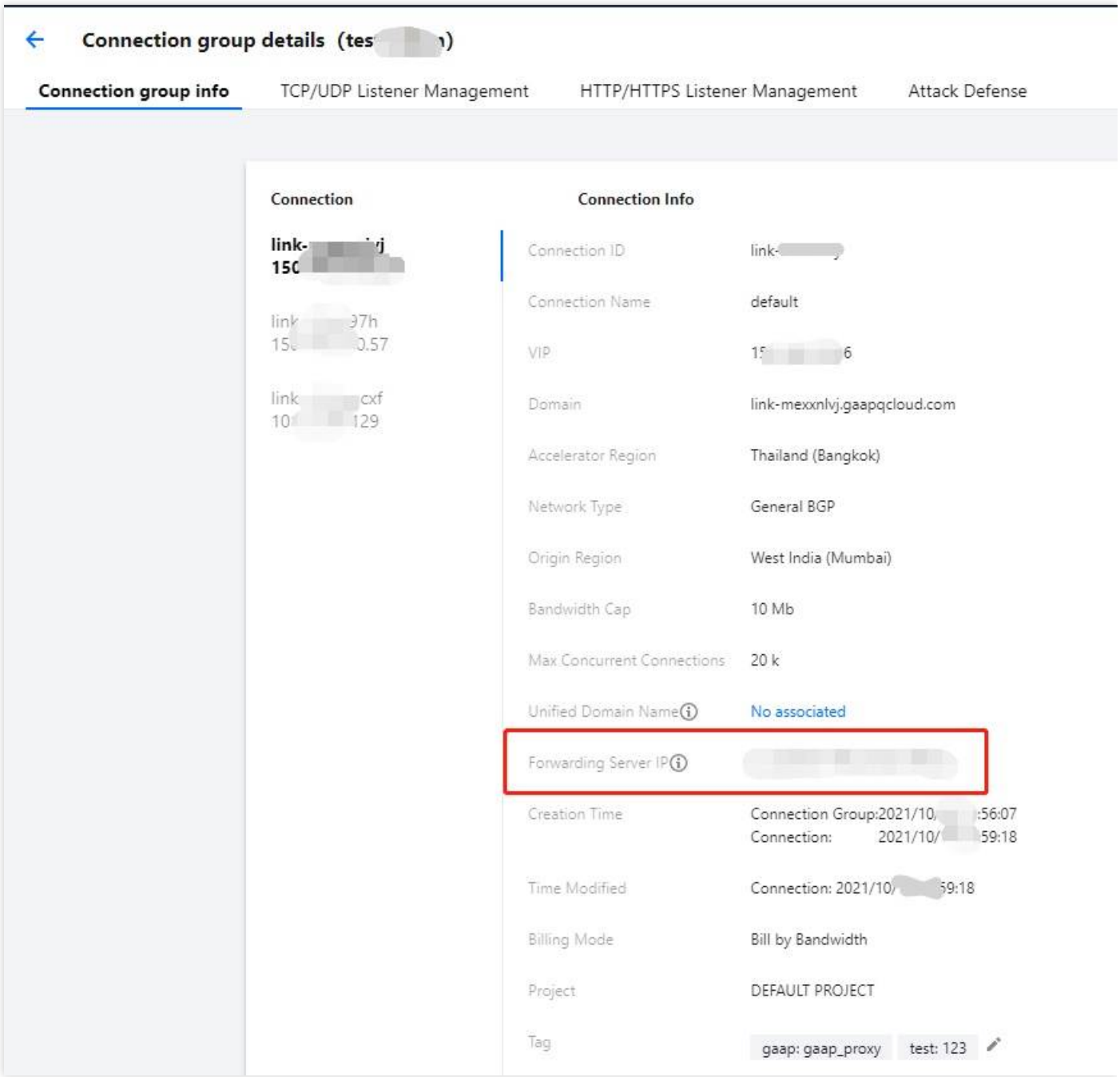
Viewing Connection Group Information

1. Log in to the GAAP console, enter the **Connection Group Management** page, and click the **ID/Connection Name** of the specified connection group.



2. On the **Connection Group Info** tab, you can view the details of each connection. **Forwarding server IP** refers to the IP of the forwarding node at the end of the acceleration connection, which is responsible for forwarding the data of the connection to the origin server over the public network. If you want multiple connections to use the same domain name, click **Unified Domain Name** to redirect to the Unified Domain Name page for configuration. A

unified domain name can be configured separately for different connections in the same connection group.



TCP/UDP Listener Management

Creating TCP/UDP listener

For directions, see TCP/UDP Listener Management.

Setting TCP/UDP listener

For directions, see TCP/UDP Listener Management.

HTTP/HTTPS Listener Management

Creating HTTP/HTTPS listener

For directions, see HTTP/HTTPS Listener Management.

Setting HTTP/HTTPS listener

For directions, see HTTP/HTTPS Listener Management.

Security Protection

For more information, see HTTP/HTTPS Listener Management.

Statistics

Last updated：2022-06-20 15:18:55

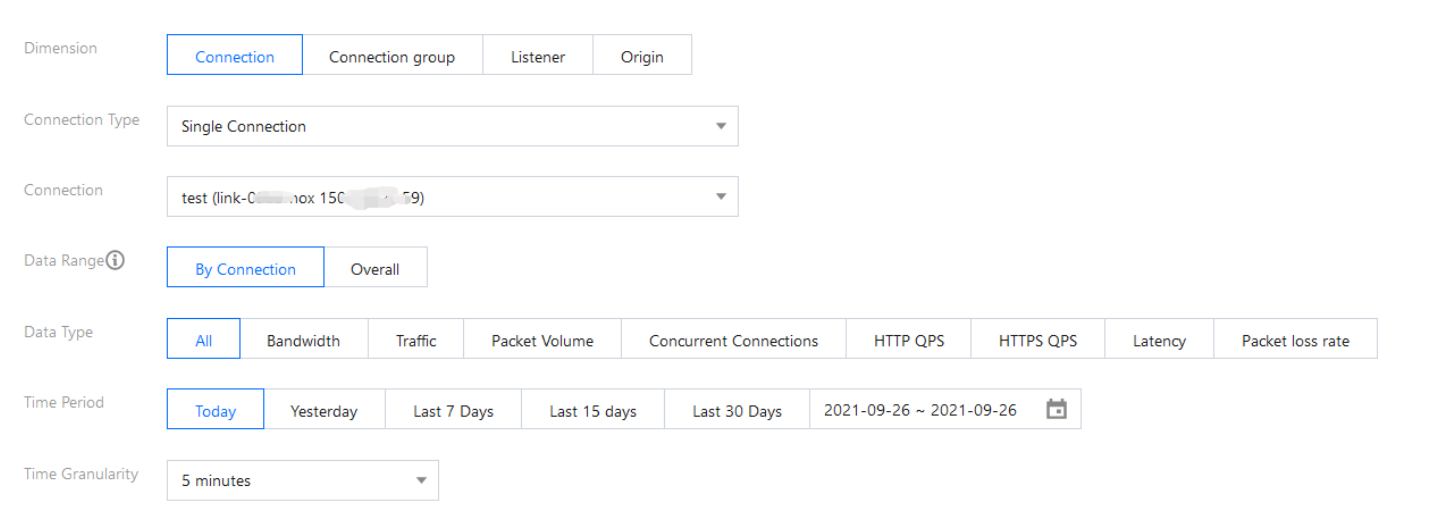
Log in to the GAAP console. Enter the **Statistics** page.

This page provides the following dimensions: Connection, connection group, listener, origin server, and domain name.

Connection

You can view the connection statistics, as shown below:

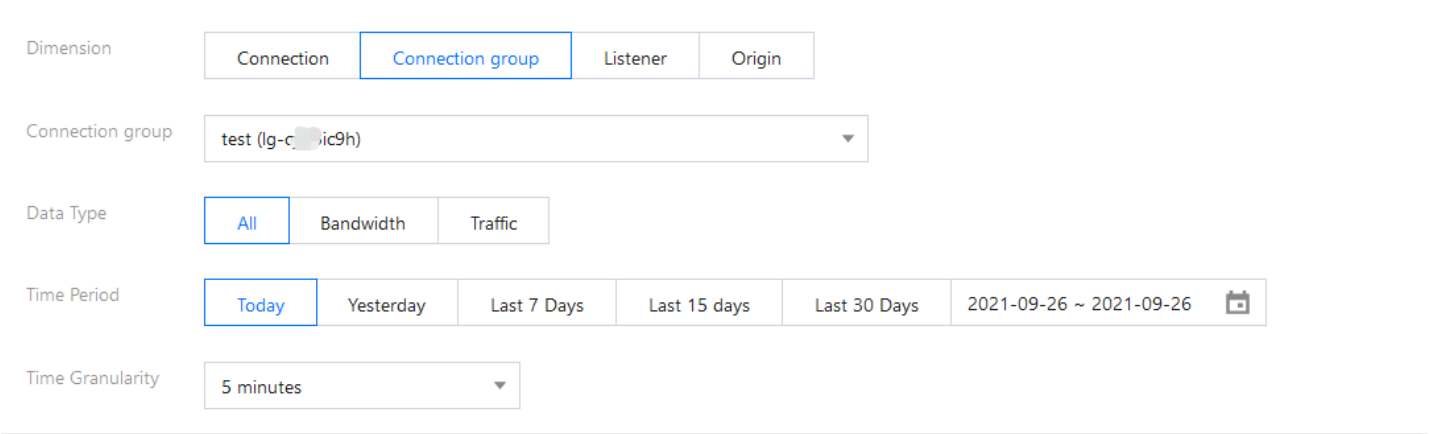
- **Connection Type**: It defaults to single connection. You can also select a connection group that has been created before.
- **Connection**: Select a connection of the **Access Management** or of the connection group.
- **Data Type**: Select one or all data types (bandwidth, traffic, packet volume, concurrent connections, HTTP QPS, HTTPS QPS, latency, and packet loss rate).
- **Time Period**: Select a time period.
- **Time Granularity**: Select a time granularity. Supported options: 1 minute, 5 minutes, 1 hour, and 1 day.
  [The maximum query time is 1 day if you select a 1-minute granularity, 3 days for a 5-minute granularity, 15 days for a 1-hour granularity and 186 days for a 1-day granularity.]



Connection Group

You can view the connection group statistics, as shown below:

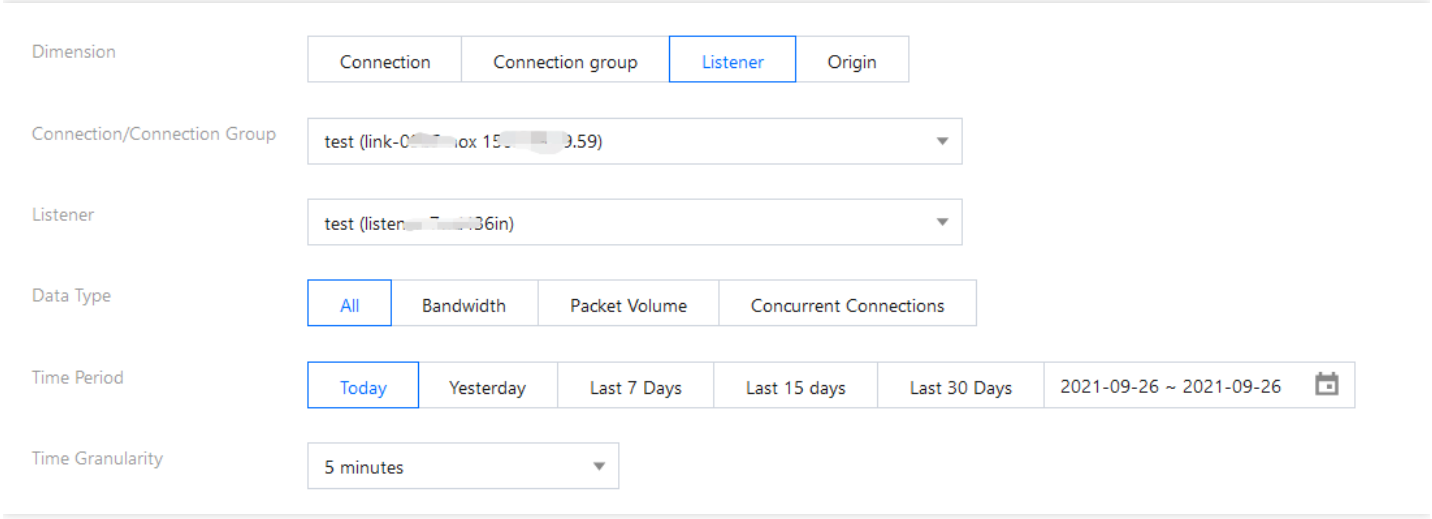
- **Connection Group**: Select one or more connection groups.
- **Data Type**: Select one or all data types (bandwidth and traffic).
- **Time Period**: Select a time period.
- **Time Granularity**: Select a time granularity. Supported options: 1 minute, 5 minutes, 1 hour, and 1 day.
  [The maximum query time is 1 day if you select a 1-minute granularity, 3 days for a 5-minute granularity, 15 days for a 1-hour granularity and 186 days for a 1-day granularity.]



Listener

You can view the listener statistics, as shown below:

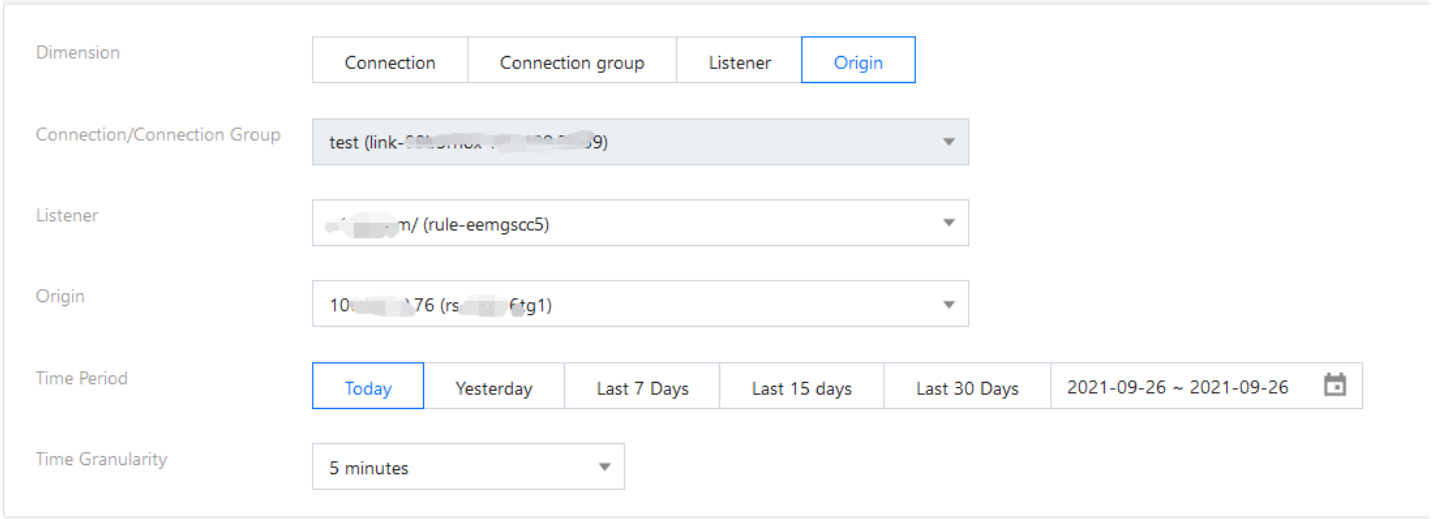
- **Connection/Connection Group**: Select a connection or connection group for the listener.
- **Listener**: Select a listener.
- **Data Type**: Select one or all data types (bandwidth, packet volume, concurrent connections).
- **Time Period**: Select a time period.
- **Time Granularity**: Select a time granularity. Supported options: 1 minute, 5 minutes, 1 hour, and 1 day.
  [The maximum query time is 1 day if you select a 1-minute granularity, 3 days for a 5-minute granularity, 15 days for a 1-hour granularity and 186 days for a 1-day granularity.]



Origin Server

You can view the statistics of the bound origin server when it is healthy.

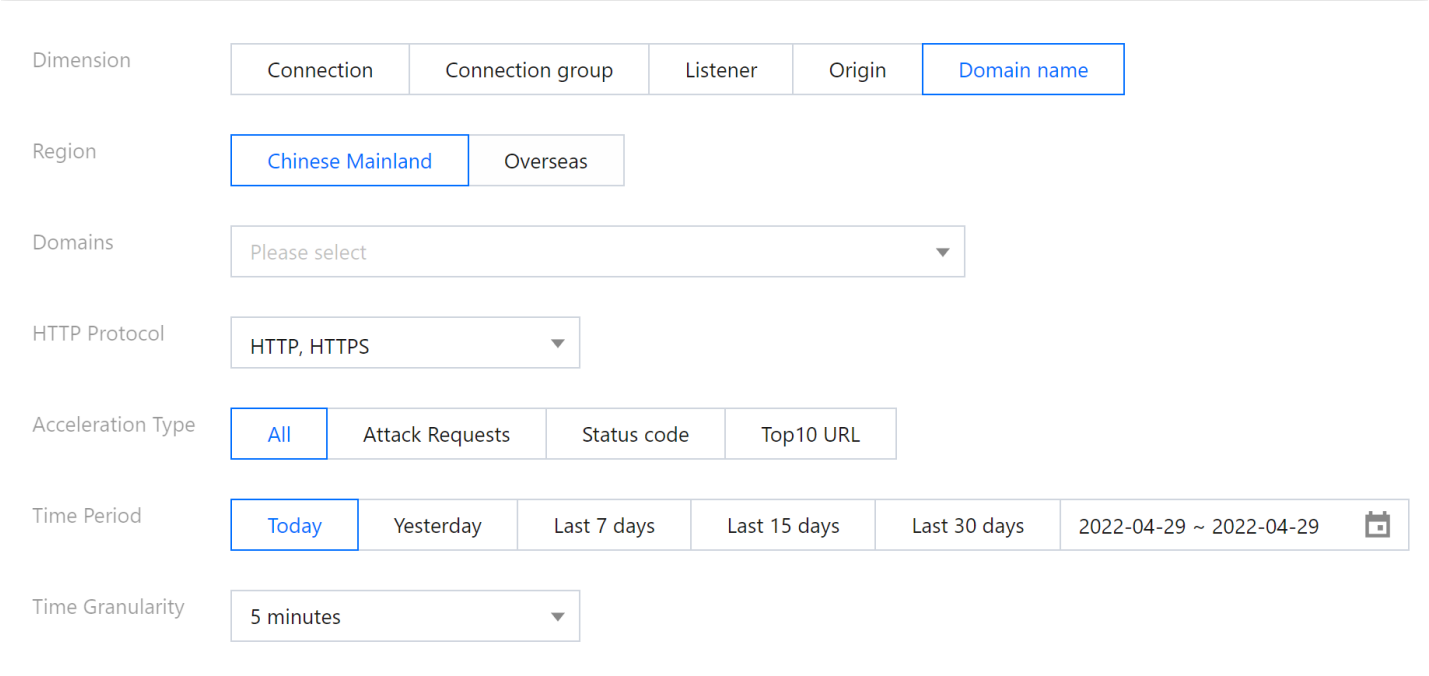
- **Connection/Connection Group**: Select a connection or connection group for the origin server.
- **Listener**: Select a listener for the origin server.
- **Origin**: Select an origin server.
- **Time Period**: Select a time period.
- **Time Granularity**: Select a time granularity. Supported options: 1 minute and 5 minutes.
  [The maximum query time is 1 day if you select a 1-minute granularity, and 31 days for a 5-minute granularity.]



Domain Name

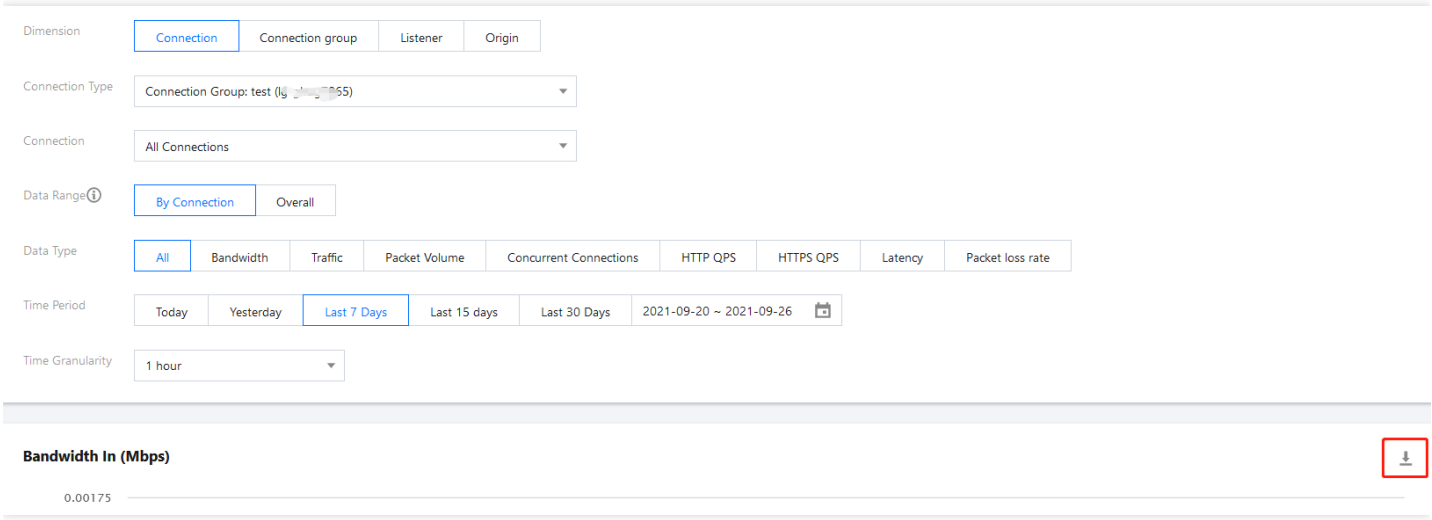
You can view the statistics of the domain names in the HTTP/HTTPS listener configuration, as shown below:

- **Region**: Select Chinese mainland or Outside the Chinese mainland.
- **Domains**: Select one or multiple domain names.
- **HTTP Protocol**: Select one or all HTTP protocols.
- **Data Type**: Select one or all data types (requests, status code and top 10 URLs).
- **Time Period**: Select a time period.
- **Time Granularity**: Select a time granularity. Supported options: 1 minute, 5 minutes, 1 hour, and 1 day.
  [The maximum query time is 1 day if you select a 1-minute granularity, 3 days for a 5-minute granularity, 15 days for a 1-hour granularity and 186 days for a 1-day granularity.]



Exporting Data

Enter the **Statistics** page, and click the download icon to export data.



Configuring an Alarm Policy

Enter the Statistics page, and click **Configure Alarm** in the top right corner to configure an alarm policy. For more details, see Access Cloud Monitoring.

Configuring Permissions

Last updated：2021-12-14 13:00:48

A root account or other accounts with AdministratorAccess permissions can assign collaborator accounts with GAAP read-write or read-only access permission by configuring access management permissions.

There are two ways the user can authorize the collaborator account: by binding a policy with a user, or by binding a user with a policy. For more information, see Cloud Access Management (CAM).

Preparation

1. Log in to the Tencent Cloud Console with a root account or an account with AdministratorAccess permissions.
2. In the top navigation, select **Cloud Products** > **Manage and Audit** > **Cloud Access Management** to open the CAM console.

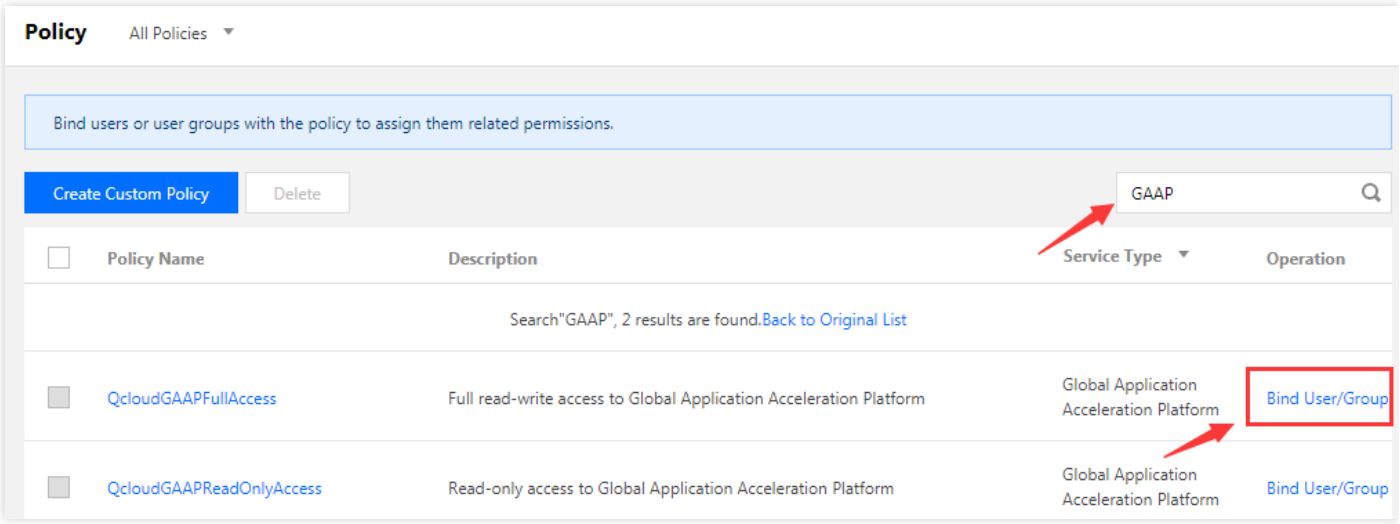
> You can also open the CAM console by selecting **Your Account Name** > **Access Management** in the upper-right corner of the console.

Directions

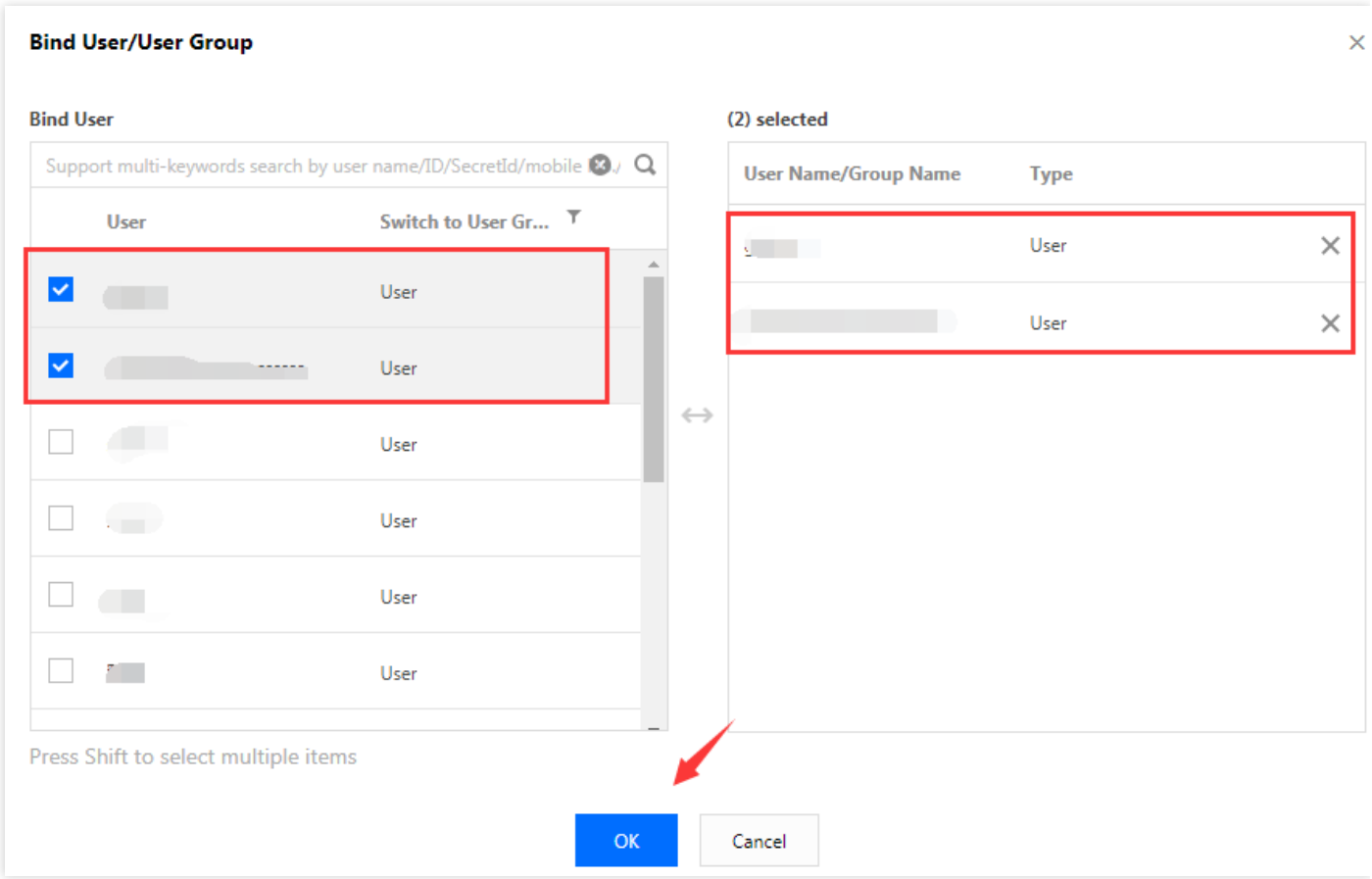
Bind a User with a Policy

1. In the left sidebar, click **Policy** to enter the management page.

2. In the search bar, enter **GAAP**. 2 results are found. Select Policy Permissions, and click **Bind User/Group**.



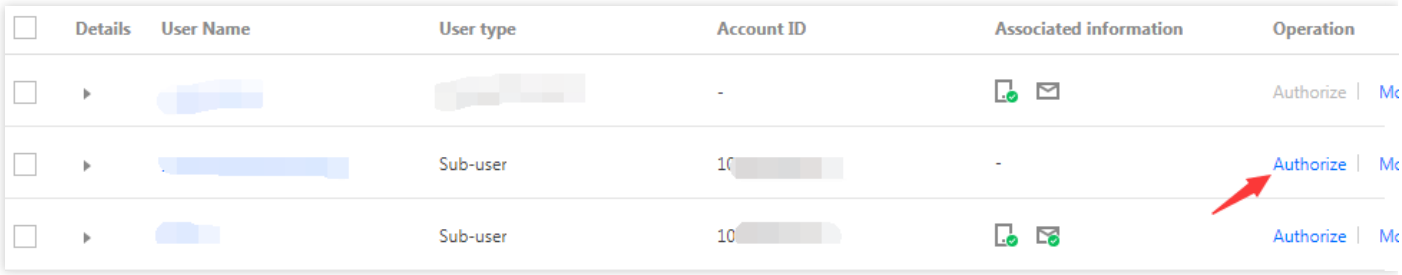
3. Select the user to be authorized, and click **OK**. The user is authorized.



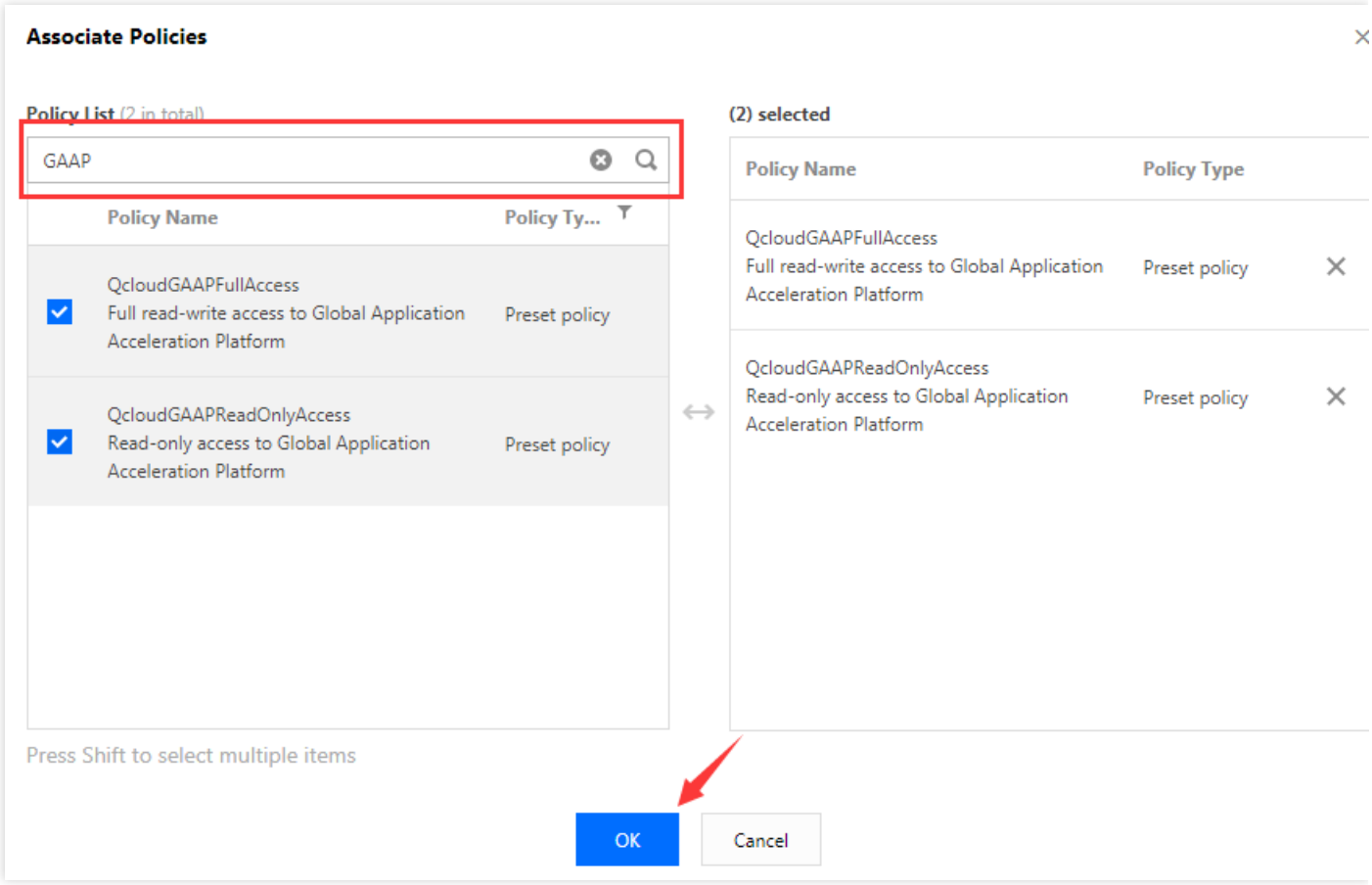
Bind a Policy with a User

1. In the left sidebar, click **User** > **User List** to enter the management page.

2. Find the line in the list that contains the user to be authorized. In the operation column, click **Authorize**.

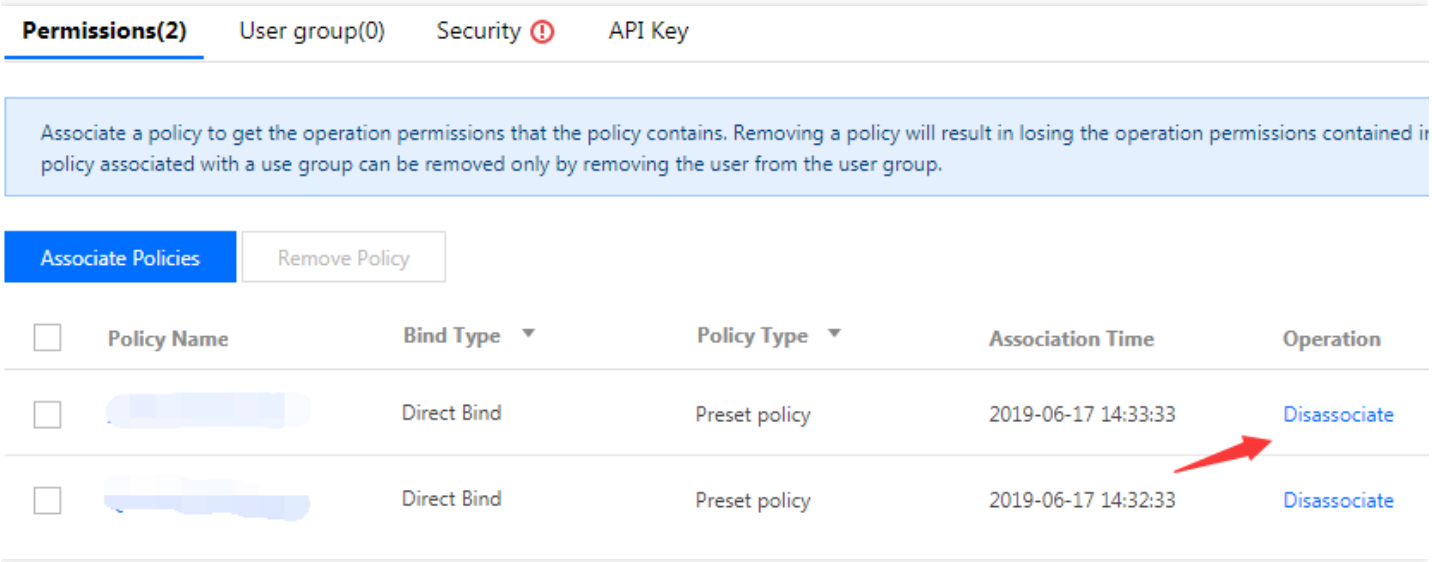


3. Search for **GAAP** in the association list. Select the policy to be authorized and click **OK**. The user is authorized.



Check and Remove Permissions

Authorized users can check and remove permissions by clicking the user names in the User List.



Access Tencent Cloud Observability Platform

Last updated：2023-05-09 18:45:56

Scenarios

To create a better user experience, alarm rules can be configured in Tencent Cloud Observability Platform. An alarm is triggered immediately when the alarm condition configured for the acceleration connection is reached.

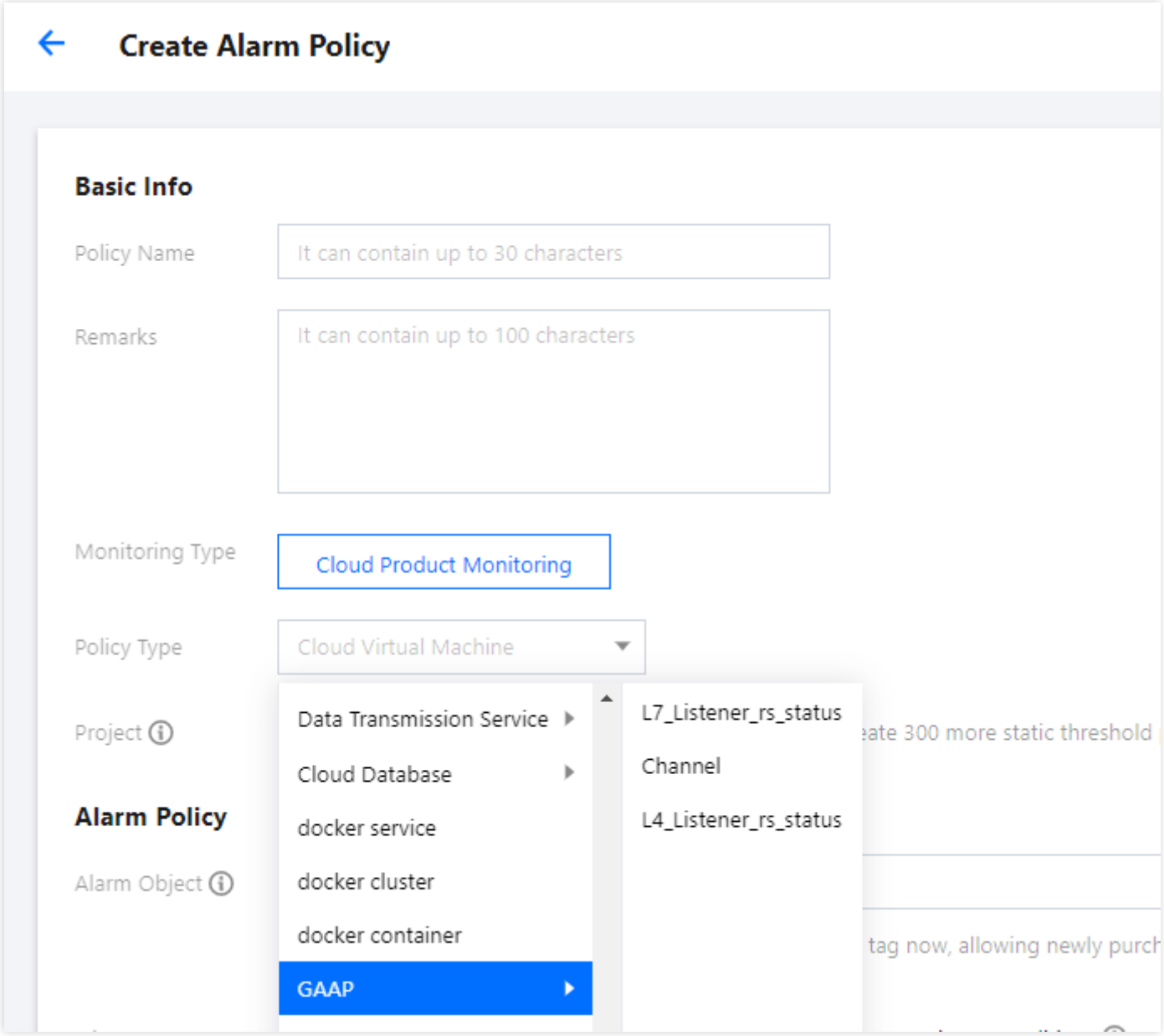
Directions

Log in to the Tencent Cloud Observability Platform Console before taking the following procedures.

Connection monitoring

1. Click **Alarm Policy** on the left sidebar. Click **Create** to enter the **Create Alarm Policy** page.

2. For **Policy Type**, select **GAAP** > **Channel**.

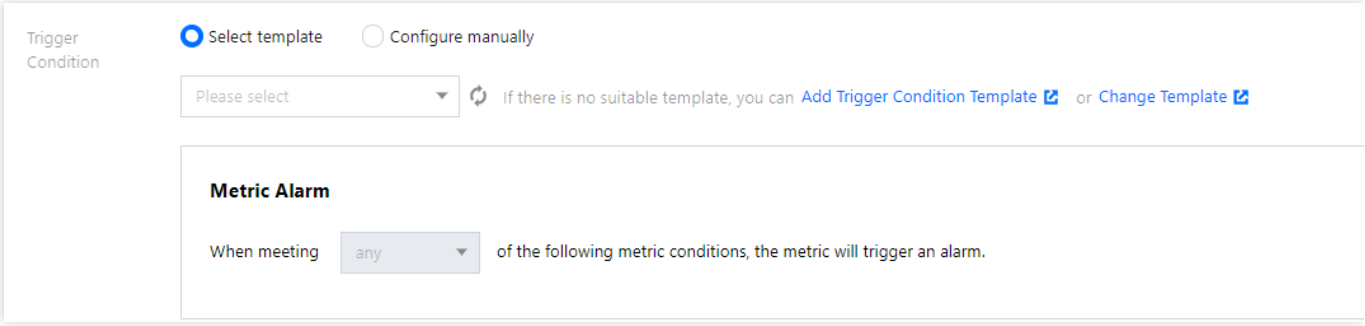


3. In the **Alarm Policy** section, add channels as needed for **Policy Object**.

   You can choose **Select template** or **Configure manually** for **Trigger Condition**.

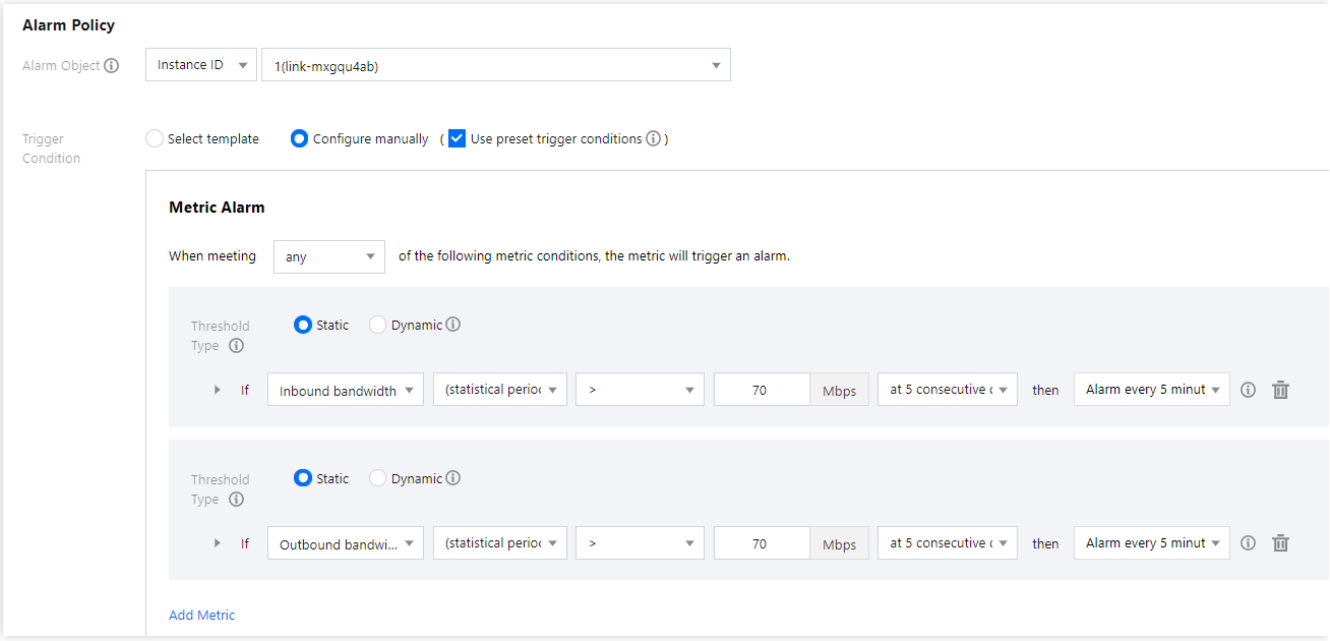
   If you choose **Select template**, you can use the alarm policies that has been configured before. If there are no templates, you can create and configure a new template as follows. The template will be saved to the console for subsequent use.

i. Click **Add Trigger Condition Template** to enter the template configuration page.



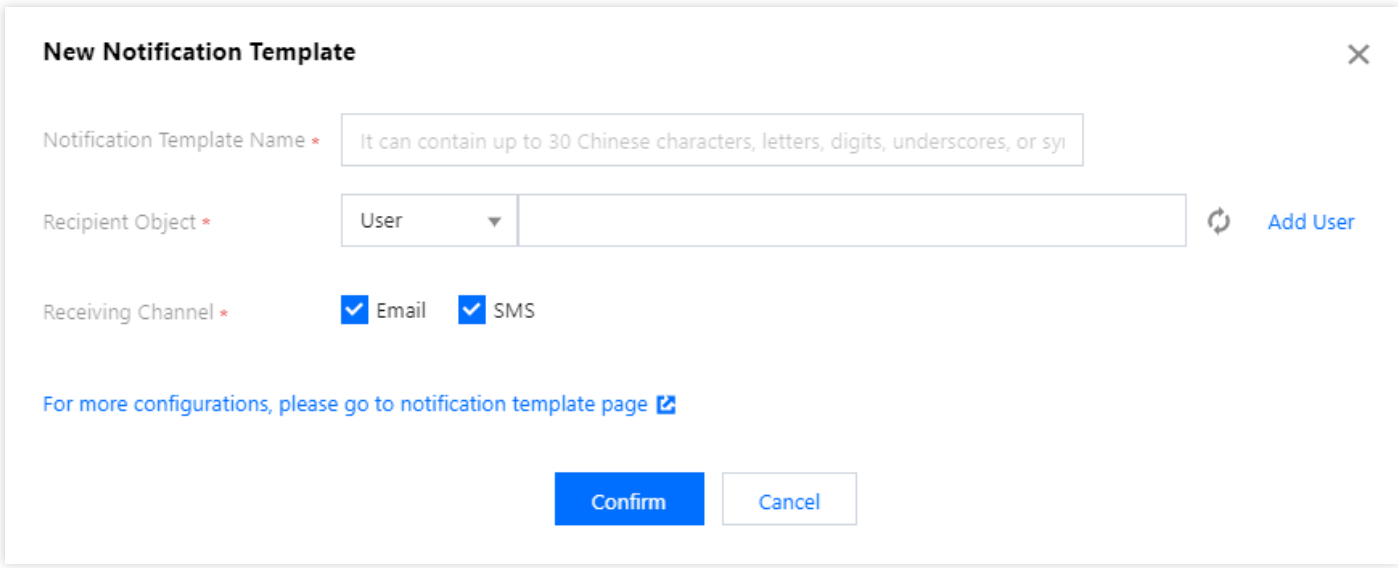
ii. Click **Create**. In the pop-up window, configure the following trigger conditions:

- **Template Name**: Enter a template name.
- **Remarks**: Enter template remarks.
- **Policy Type**: Select a monitoring service, such as **GAAP** > **Channel**.
- Use preset trigger conditions: Select this option to enable preset trigger conditions for the corresponding monitored product.
- Trigger condition: includes indicator alarm and event alarm. You can click **Add** to set multiple alarms. If you choose **Configure manually**, you can add multiple alarm trigger conditions as needed.

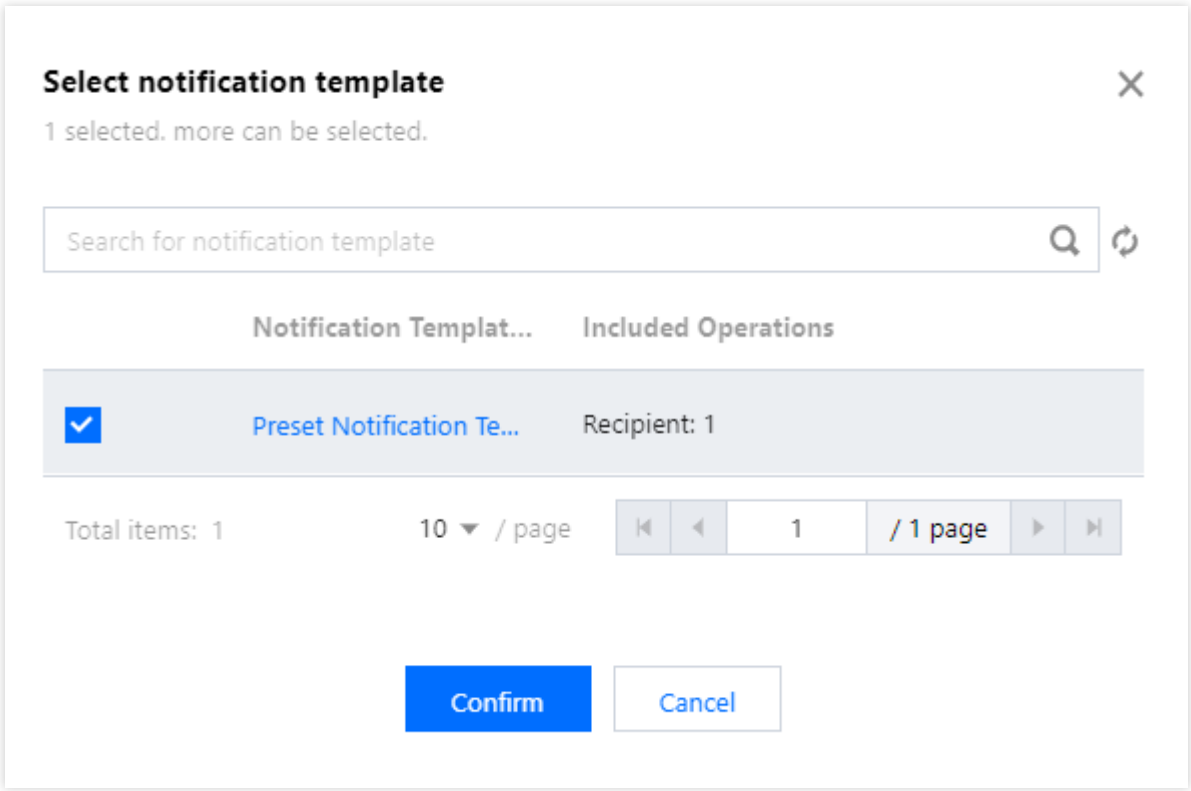


4. In the **Configure Alarm Notification** section, click **Create Template**, create a template name and select a recipient object and channel.

> Note：
> The recipient object needs to be bound with a channel. Otherwise, you will not receive an alarm notification.



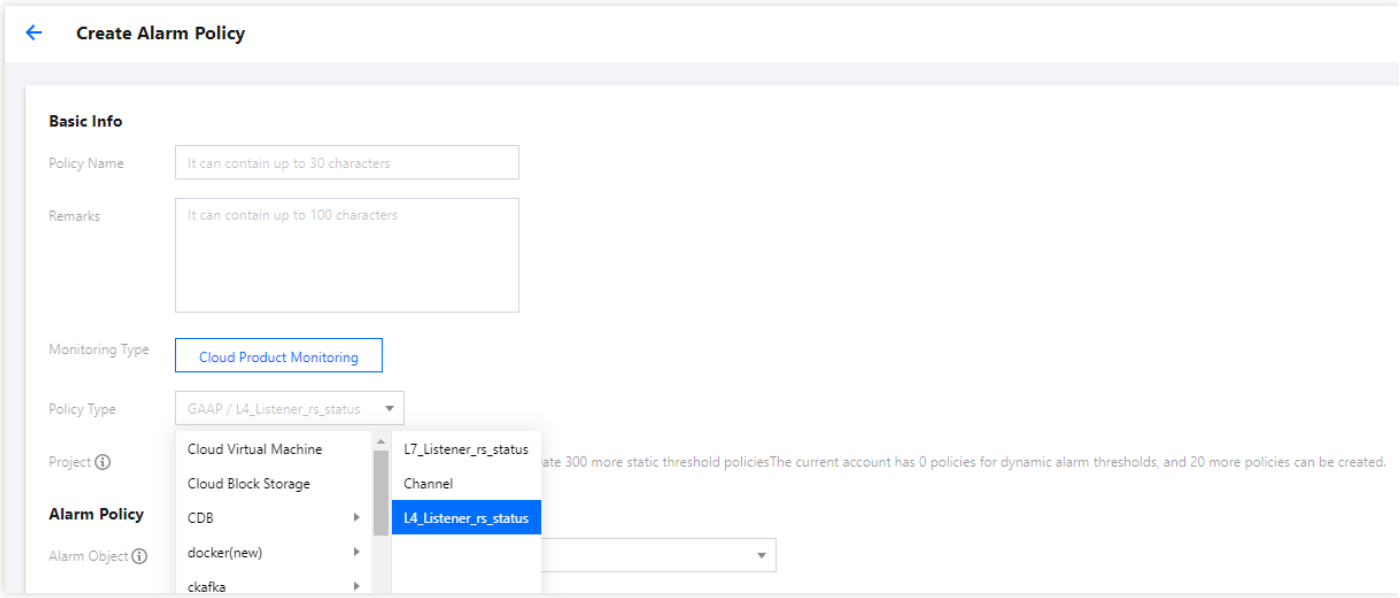
Click **Select template** to choose a template you need.



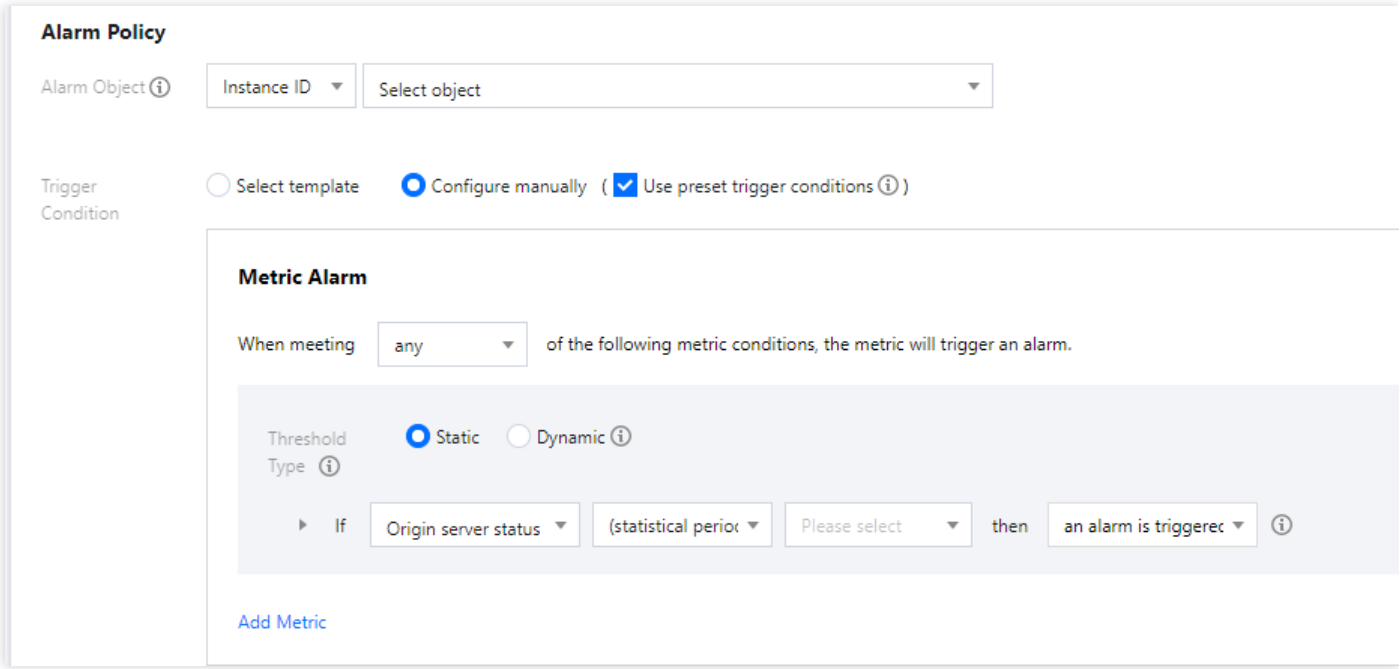
Listener monitoring

1. Select **Alarm Policy** on the left sidebar. Click **Create** to enter the **Create Alarm Policy** page.

2. For **Policy Type**, select **GAAP** > **L4 Listener Origin Server Status/L7 Listener Origin Server Status**.

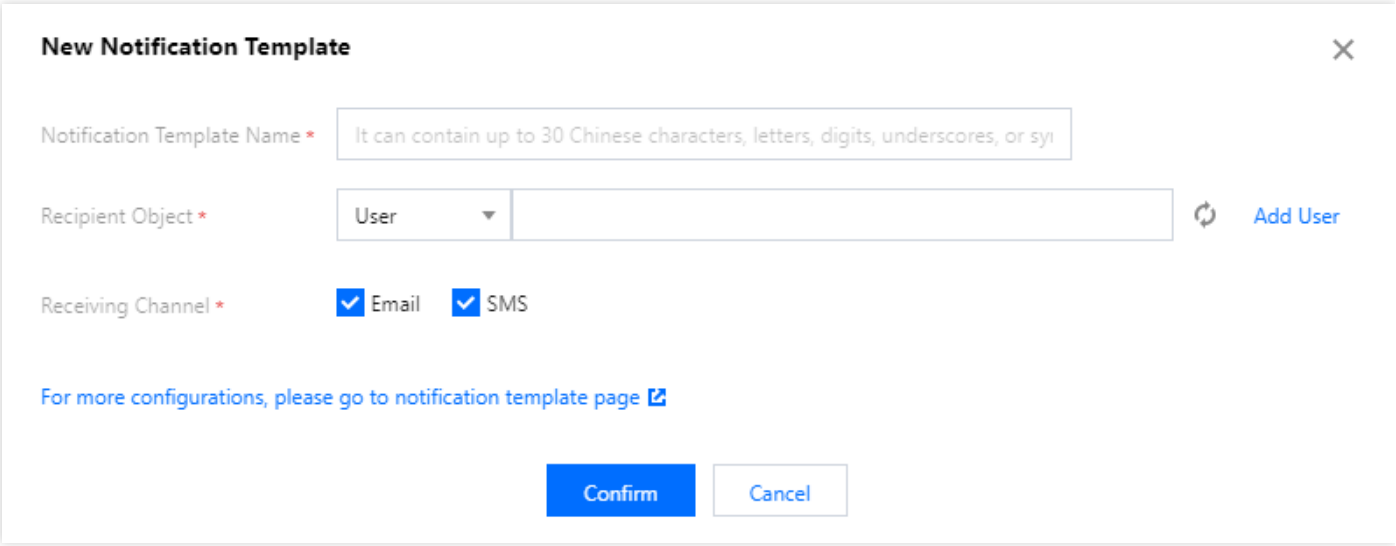


3. In the **Alarm Policy** section, select an object for **Policy Object**, and choose **Select template** or **Configure manually** for **Trigger Condition**. If you choose **Configure manually**, you can set a trigger condition to notify you that an origin server is found exceptional.

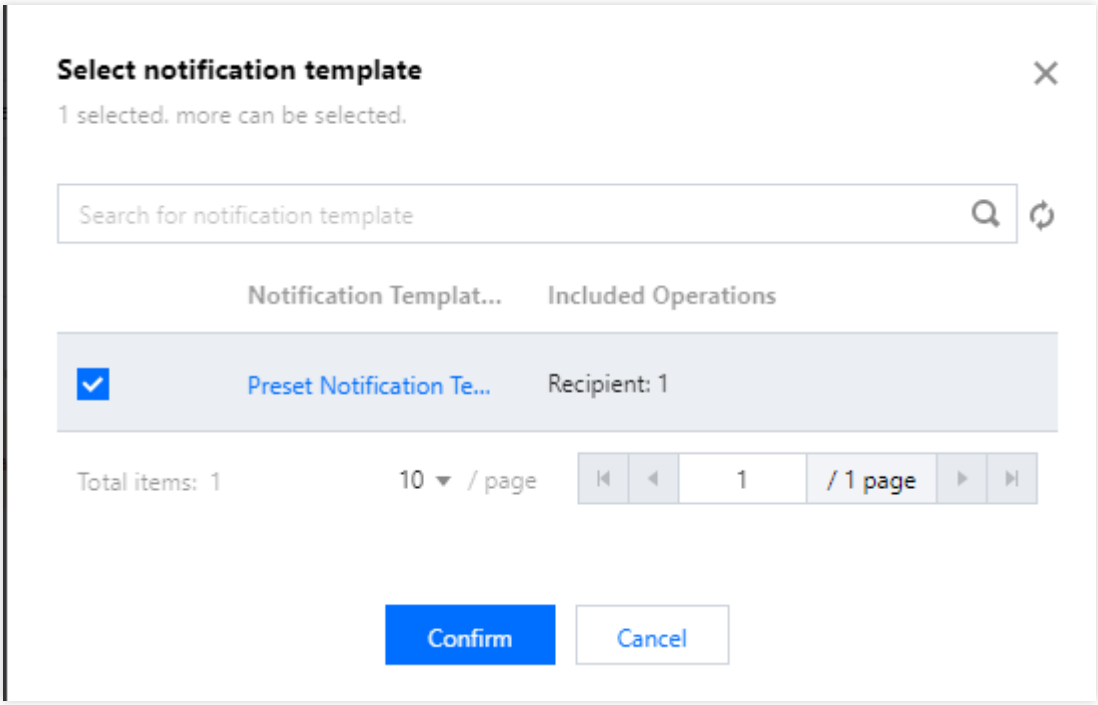


4. In the **Configure Alarm Notification** section, click **Create Template**, create a template name and select a recipient object and channel.

> Note：
> The recipient object needs to be bound with a channel. Otherwise, you will not receive an alarm notification.



Click **Select template** to choose a template you need.

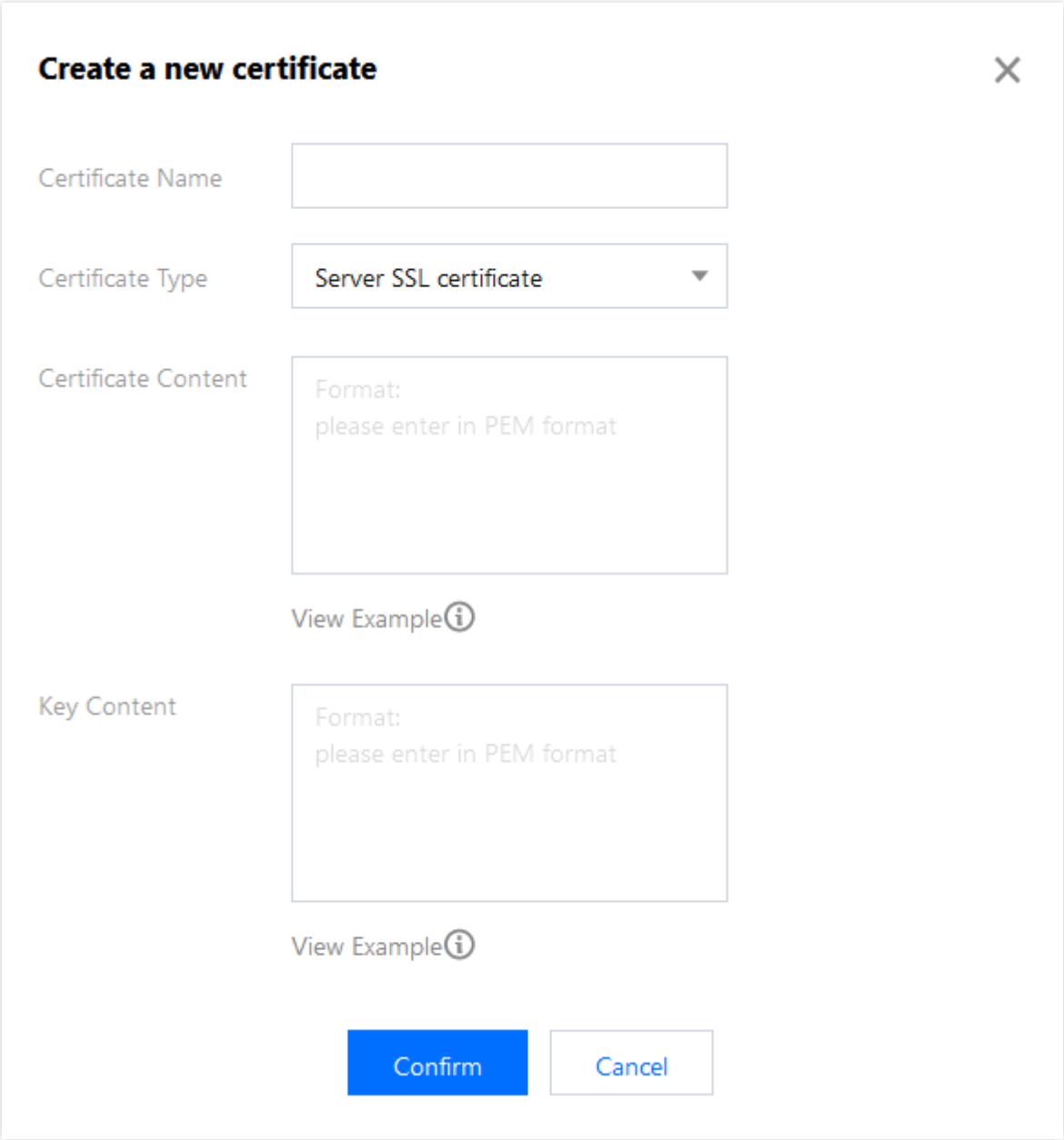


Certificate Management

Last updated：2021-12-14 13:00:48

Adding a Certificate

1. Log in to the GAAP console, enter the **Certificate Management** page and click **Add**.
2. Enter the certificate information.



- **Certificate Name**: user-defined name of the certificate.

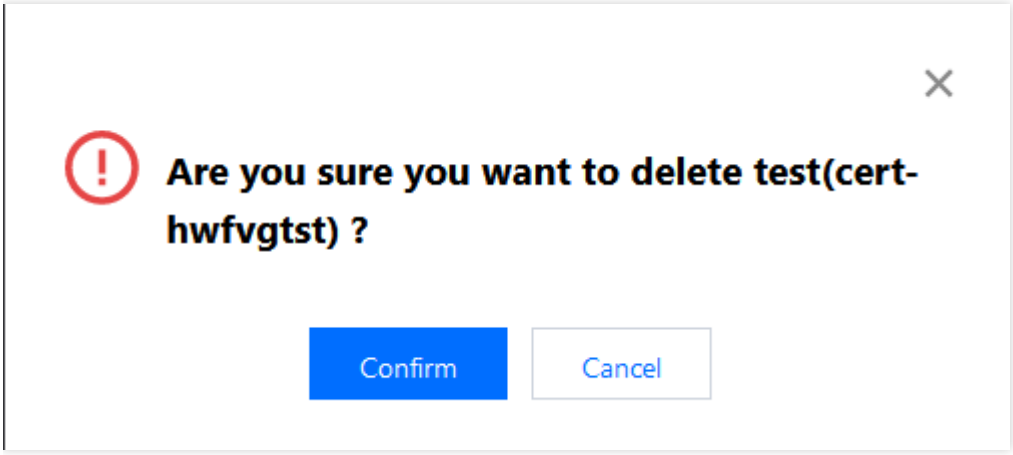
- **Certificate Type**: supports basic authentication configurations, client CA certificate, server SSL certificate, origin CA certificate, and connection SSL certificate, of which a key is required for server SSL certificates and connection SSL certificates, and can be purchased in Tencent Cloud's **SSL Certificate Management**.
- **Certificate Content**: supports certificate content in PEM format.
- **Key Content**: supports key content in PEM format.

Certificate Details

Enter the **Certificate Management** page, and click **ID/Name** or **Details** of a certificate you want to check.

Deleting a Certificate

Enter the **Certificate Management** page and click **Delete** of a certificate you want to remove. Then click **OK** on the pop-up window.



Obtaining Real Client IP
Obtaining Real Client IP Through TOA (TCP Only)
Basic Principles

Last updated：2022-07-13 15:44:03

When an acceleration connection forwards the data packet, SNAT and DNAT will be performed on the packet; that is, the source and destination addresses of the data packet will be modified. The packet source address seen by the origin server will be the forwarding IP address of the acceleration connection, rather than the real client IP. To pass the client IP to the server, the acceleration connection will include the client IP and port in the custom `tcp option` field when forwarding the packet, as shown below:

```
#define TCPOPT_ADDR 200
#define TCPOLEN_ADDR 8 /* |opcode|size|ip+port| = 1 + 1 + 6 */
/*
* insert client ip in tcp option.
* must be 4 bytes alignment.
*/
struct ip_vs_tcpo_addr{
__u8 opcode;
__u8 opsize;
__u16 port;
__u32 addr;
};
```

After the Linux kernel has received the ACK packet of three-way handshake while listening the socket, its status is changed from SYN_REVC to TCP_ESTABLISHED. In this case, the kernel calls the `tcp_v4_syn_recv_sock` function. The Hook function `tcp_v4_syn_recv_sock_toa` calls the original `tcp_v4_syn_recv_sock` function, then extracts `TOA OPTION` from the `TCP OPTION` by calling the `get_toa_data` function, and saves it in the `sk_user_data` field. After the above call is completed, the kernel calls `inet_getname_toa hook inet_getname` to obtain the source IP and port. It first calls the original `inet_getname` , and check whether the `sk_user_data` field is empty. If the real IP and port can be extracted from this field, then replace the returned values of `inet_getname` with these two values.
The server program calls `getpeername` in the user mode, and the client's original IP and port are returned.

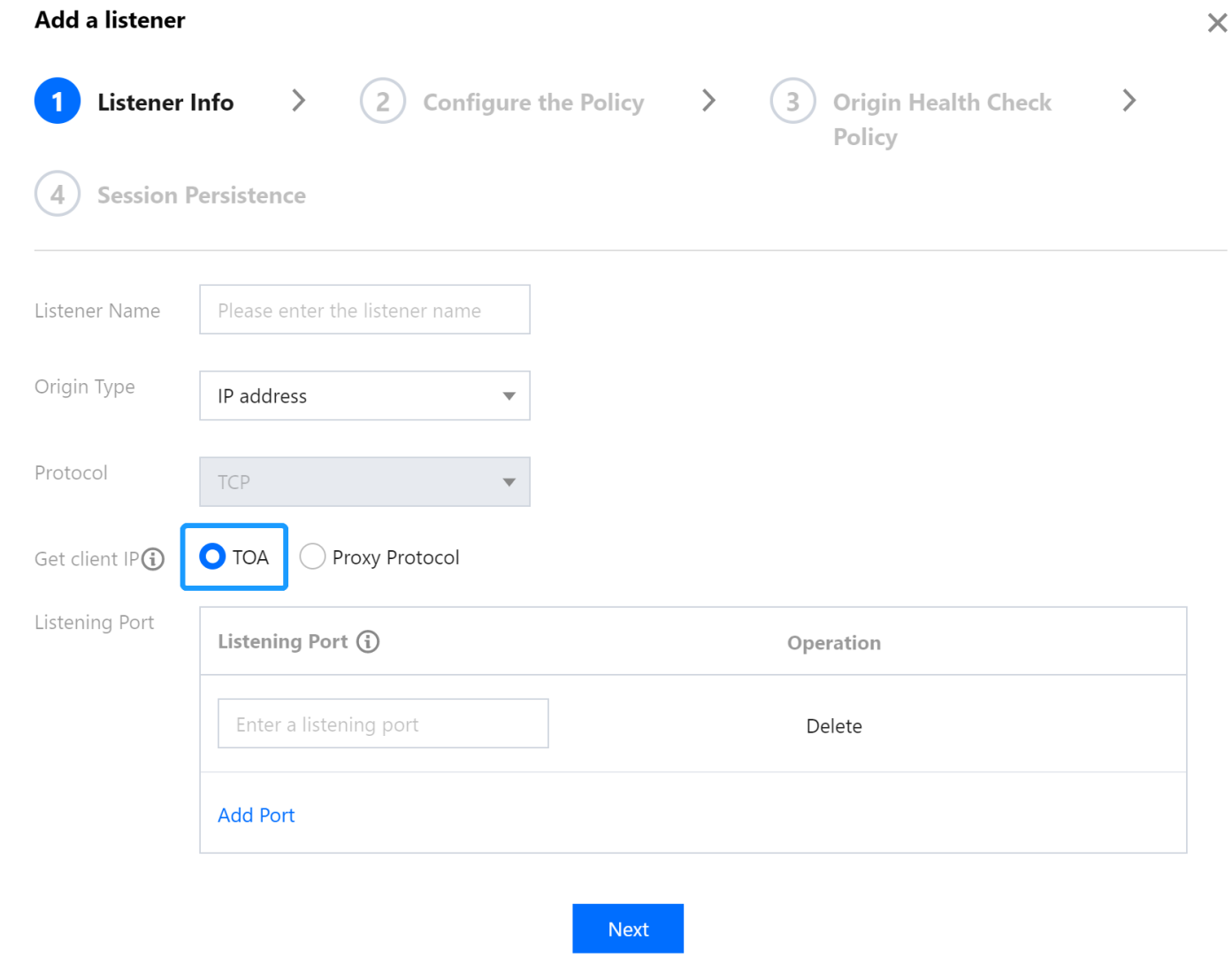
Invoking Linux Backend Version
Step 1: Create TCP Listener and Enable TOA

Last updated：2022-06-20 10:49:51

Note：
If there are problems with backend adaptation, please submit a ticket for assistance.

Only layer-4 TCP allows TOA to obtain the real client IP. Please enable TOA in the acceleration connection as follows:

Log in to the GAAP console. Select **Access Management** > **TCP/UDP Listener Management**. Click **Create** to add a TCP listener and select TOA, and then complete configurations required to create the listener and connection.



Step 2: Load TOA on Backend Server

Last updated：2022-07-13 15:22:55

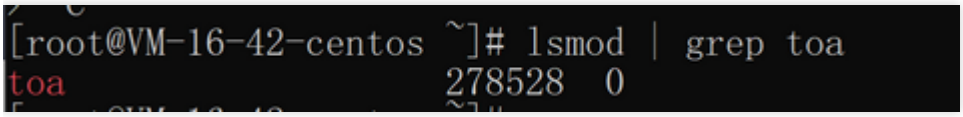
Method 1: Download source code and load the module

1. Download and decompress the TOA package corresponding to the version of Linux OS on Tencent Cloud.
   - **arm64**
     - kernel-4.18.0.rar
   - **centos**
     - CentOS 6.5 64.rar
     - CentOS 7.2 64.rar
     - CentOS 7.3 64.rar
     - CentOS 7.4 64.rar
     - CentOS 7.5 64.rar
     - CentOS 7.6 64.rar
     - CentOS 7.7 64.rar
     - CentOS 7.8 64.rar
     - CentOS 7.9 64.rar
     - CentOS 8.0 64.rar
     - CentOS 8.2 64.rar
   - **debian**
     - Debian 10.2 64.rar
     - Debian 8.2 64.rar
     - Debian 9.0 64.rar
   - **suse linux**
     - SUSE Linux Enterprise Server 12 SP3 64.rar
   - **ubuntu**
     - Ubuntu Server 14.04.1 LTS 64.rar
     - Ubuntu Server 16.04.1 LTS 64.rar
     - Ubuntu Server 18.04.1 LTS 64.rar
     - Ubuntu Server 20.04.1 LTS 64.rar
2. After decompression is completed, run the `cd` command to access the decompressed folder and run the module loading command:

```
insmod toa.ko
```

3. Run the following command to check whether the loading is successful:

```
lsmod | grep toa
```



4. After it is loaded, load the `toa.ko` file in the startup script (the `toa.ko` file needs to be reloaded if the server is restarted).

```
echo "insmod xxxxx /toa.ko" >> /etc/rc.local
```

5. (Optional) To disable TOA temporarily, run the command `rmmod path/module name` .

```
rmmod toa.ko
```

6. (Optional) If TOA is no longer needed, run the following command to uninstall it.

```
rmmod toa
```

7. (Optional) Run the following command to check whether the module is uninstalled. If you see the message "TOA unloaded", the uninstallation is successful.

```
dmesg -T
```

Method 2: Compile and load the module

If there is no installation package provided for your OS version, you can download the source package of the Linux general version and then compile it to obtain an installation package. The following is the example for CentOS.

1. Obtain the source package.

```
wget "https://thunder-pro-mainland-1258348367.cos.ap-guangzhou.myqcloud.com/gaap-toa.rar"
```

2. Install the build environment.

```
yum install gcc
yum install make
yum install kernel-headers kernel-devel -y
```

3. Decompress the source package.

```
tar zxf gaap-toa.rar
```

4. Enter the TOA directory.

```
cd toa
```

5. Compile make.

```
make
```

6. Move and load the module.

```
mv toa.ko /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko
insmod /lib/modules/`uname
¬-r`/kernel/net/netfilter/ipvs/toa.ko
```

7. Check whether the module is loaded successfully.

```
lsmod | grep toa
```

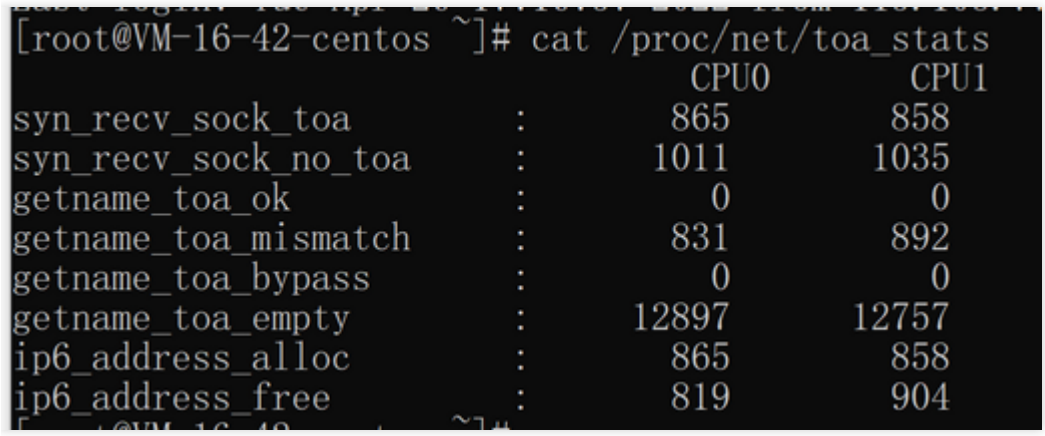
Step 3: View TOA Metric Status (Optional)

Last updated：2022-06-17 18:49:37

To ensure execution stability, this kernel module allows you to monitor status. After inserting the `toa.ko` kernel module, you can monitor the TOA working status in either of the following ways.

Run the following command to check the TOA metrics.

```
cat /proc/net/toa_stats
```



The monitoring metrics are described as follows:

Metric	Description
syn_recv_sock_toa	Number of sockets that carry TOA information
syn_recv_sock_no_toa	Number of sockets that do not carry TOA information
getname_toa_ok	This count increases when you call `getsockopt` and get the source IP successfully or when you call `accept` to receive client requests.
getname_toa_mismatch	This count increases when you call `getsockopt` and get the source IP that does not match the required type. For example, a client connection contains an IPv4 source IP address whereas you get an IPv6 address, the count will increase.
getname_toa_empty	This count increases when the `getsockopt` function is called in a client file descriptor that does not contain TOA.
ip6_address_alloc	It allocates space to store the information when the TOA kernel gets the source IP and source port saved in the TCP data packet.

Metric	Description
ip6_address_free	When the connection is released, TOA will release the memory previously used to save the source IP and source port. If all connections are closed, the total count of `ip6_address_alloc` for each CPU should be equal to the count of this metric.

Viewing Real Client IP

Last updated：2022-06-17 18:49:37

Method 1: Check the client IP in nginx logs (log path: /var/log/nginx/access.log)

Method 2: Check the client IP using tcpdump in Wireshark.

1. Run the following command on the backend server to capture the ENI.

```
sudo tcpdump -i eth0 -w dump.pcap
```

`-i` specifies an ENI to capture.

`-w` specifies a location for saving results.

2. After the client accesses the test URL, press Ctrl + C to stop capturing.

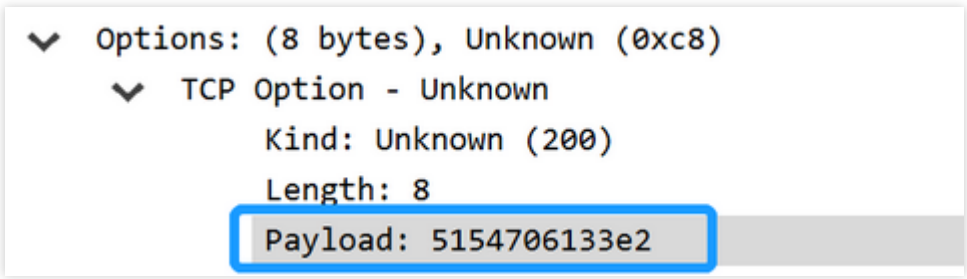
```
[root@VM-16-42-centos ~]# sudo tcpdump -i eth0 -w dump.pcap
dropped privs to tcpdump
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C361 packets captured
362 packets received by filter
0 packets dropped by kernel
```

3. Download the dump.pcap file to your local PC using the `sz` command or any other method.

```
sz dump.pcap
```

4. Open the downloaded file dump.pcap in Wireshark and check the real client IP in `TCP Option`.

The `Payload` field is in hexadecimal format. The last 4 bytes stands for the real client IP.



Common Problems

Last updated：2022-06-17 18:49:37

A signature error occurred "module verification failed: signature and/or required key missing - tainting kernel"

- Module signature verification is a kernel feature, which needs to be enabled through the Linux kernel compilation.
- Solution 1: When compiling the kernel, add `CONFIG_MODULE_SIG=n` .
- Solution 2: Sign the kernel module with the certificate, as shown below:
  /usr/src/linux-4.9.61/scripts/sign-file sha512/usr/src/linux-4.9.61/certs/signing_key.pem /usr/src/linux-4.9.61/certs/signing_key.x509 toa.ko

The /lib/modules directory is missing during compilation

- This error is often associated with the following situations:
- The kernel package is not installed.
- When the directory is modified, you need to correct it by yourself.
- When the kernel does not have the build directory, you need to manually create a soft link to the exact version of the kernel header.
  cd /lib/modules/4.9.0-13-amd64 && ln -s /usr/src/linux-headers-4.9.0-13-amd64 build

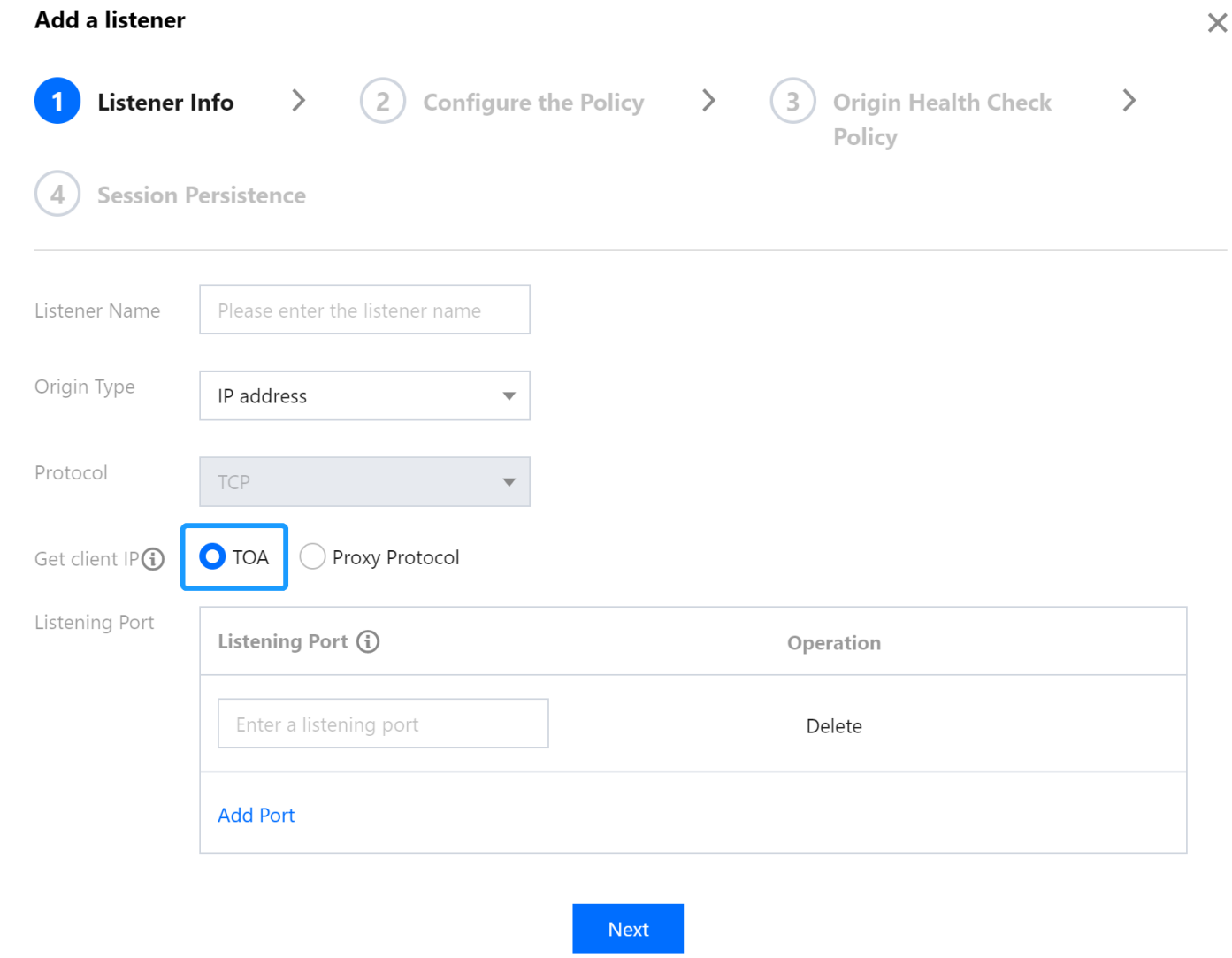
Invoking Windows Backend Version
Step 1: Create TCP Listener and Enable TOA

Last updated：2022-06-20 10:54:39

Note：
If there are problems with backend adaptation, please submit a ticket for assistance.

Only layer-4 TCP allows TOA to obtain the real client IP. Please enable TOA in the acceleration connection as follows:

Log in to the GAAP console. Select **Access Management** > **TCP/UDP Listener Management**. Click **Create** to add a TCP listener and select TOA, and then complete configurations required to create the listener and connection.



Step 2: Load TOA on Backend Server

Last updated：2022-06-17 18:49:37

Downloading the File

Click here to download the file.

General Version

File Description

File	Description
WinPcap_4_1_3.exe	WinPcap driver, see WinPcap Documentation for details
lib_toa.lib	TOA static library
toa_fetcher.h	Header file that the static library relies on
pcap.h	Header file that the static library relies on

Preparing the environment

1. Double-click WinPcap_4_1_3.exe to install the WinPcap driver (no restart is required).
2. Add lib_toa.lib to the .lib library path of the project.
3. Add toa_fetcher.h and pcap.h to the header file of the project.

Go Version

File Description

File	Description
WinPcap_4_1_3.exe	WinPcap driver, see WinPcap Documentation for details
toa_win.exe	TOA program for Windows server
toa_win.conf	Config file of TOA program for Windows server
program_auto_up.bat	bat script for Windows server

File	Description
demo.go	A sample program written in Go language, used to access TOA services

Deployment steps

1. Modify the toa_win.conf file as instructed below:

Parameter	Required	Description
ToaWinPort	Yes	The service port of toa_win.exe, used to communicate with TOA client, default is 9999.
NetworkCardIP	Yes	This is used to identify the IP address of the network interface, for example, 10.75.132.39. This is the NIC that communicates with the client.
ServerListenIP	Yes	The IP address of the server, for example, 10.75.132.39. It is used to filter TCP flows.
ServerListenPortList	No	The port list of the server. It is used to filter TCP flows. A maximum of 3 ports can be added. **Either ServerListenPortList or PortRange must be configured.**
PortRange	No	The port range of the server. It is used to filter TCP flows. A maximum of 3 port ranges can be added. **Either ServerListenPortList or PortRange must be configured.**
CacheSeconds	No	The length of the cache time, unit in seconds. The default is 15 seconds.

Note：
The configuration file must be placed in the same directory as toa_win.exe.

```
#ToaWinPort
9999
#NetworkCardIP
172.19.0.9
#ServerListenIP
172.19.0.9
#ServerListenPortList
9102;5555;6666
#PortRange
6666-7777;7777-8888
#CacheSeconds
15
```

2. Modifying program_auto_up.bat.

   Modify the path to the directory where the program is located. Add the script to the scheduled task, and execute on it periodically. The script is used to monitor the toa_win.exe program and automatically activate the program when it exits.

```
@echo off
set Program="toa_win.exe"
tasklist -v | findstr %Program% > NUL
if ErrorLevel 1 (
    echo "process not exists" >> auto_up_log.txt
    echo %date%+ %time% >> auto_up_log.txt
    C:
    cd C:\xxxx\
    toa_win.exe
)else (
    echo "process exists"
)
```

3. Run the toa_win.exe program. The log is saved to toa_win.log in the same directory. Now, you can get the real IP address from TOA services through UDP communication. For details, see How to Use.

Step 3: Obtain Real Client IP

Last updated：2022-06-17 19:46:53

General Version

Data structure and function description

- **class ToaFetcher**
  A subject class used to manage the acquisition and release of TOA.
- **InitUpToaFetcher**

1. Function description
   This function is used to initialize TOA fetcher.

```
bool InitUpToaFetcher(char *ncard_ip_str, char *svr_ip_str, u_short svr_port[],
u_short svr_port_num, u_short cache_secs=TIMER_CACHE_SECS)
```

2. Input parameters description
   - ncard_ip_str: This is used to identify the IP address string of the network interface, for example, 10.75.132.39. This is the NIC that communicates with the client.
   - svr_ip_str: The IP address string of the server, such as 10.75.132.39, used to filter TCP flows.
   - svr_port: The port list of the server, used to filter TCP flows. Up to three ports can be added. Either `svr_port` or `port_range_ptr` must be configured.
   - svr_port_num: The number of server ports.
   - port_range_ptr: The array of server port range pointers, where the elements are pointers pointing to a string. A port range string is in the format of 10001-10005, and up to three ranges can be added. This parameter is used to filter TCP flows. Either `svr_port` or `port_range_ptr` must be configured.
   - port_range_num: The number of port ranges of the server.
   - cache_secs: The length of cache in seconds. The default value is 15 seconds. For more information, see `toa_fetcher.h: TIMER_CACHE_SECS` . The TOA will no longer be saved after the cache expires.
3. Returned value
   - TRUE: Successfully created an additional thread to obtain TOA
   - FALSE: Failed to create an additional thread to obtain TOA

- **FetchToaValue**

1. Function description

   This function is used to get the TOA value. After the tcp-syn packet interacts, TOA can be obtained after 1 ms. Normally, a three-way handshake takes more than 1 ms.

```
bool FetchToaValue(u_long fake_client_ip_addr, u_short fake_client_port, u_long &real_client_ip_addr, u_short &real_client_port)
```

2. Input parameters description

   - fake_client_ip_addr: The fake IP address of the client stored in network byte order and can be obtained from the opposite address returned by the `accept` function of the server.
   - fake_client_port: The fake port number of the client stored in network byte order and can be obtained from the opposite address returned by the `accept` function of the server.
   - real_client_ip_addr: The real IP address of the client stored in network byte order and can be obtained from TOA.
   - real_client_port: The real port number of the client stored in network byte order and can be obtained from TOA.

3. Returned value

   - TRUE: TOA obtained successfully.
   - FALSE: Failed to obtain TOA. Normally, the reason is TOA has been cleared because the cache expires.

- **StopToaFetcher**

1. Function description

   This function is used to stop TOA fetcher.

```
void StopToaFetcher()
```

2. Input parameters description

-

3. Returned value

-

- **GetFetcherStatus**

1. Function description

   This function is used to obtain the Fetcher status.

```
int GetFetcherStatus()
```

2. Input parameters description

-

3. Returned value

0: initial status. An instance will be in this status after it is created. During fetcher initialization, this status will remain unchanged. If an error occurs, -1 will be returned. If the execution succeeds, 1 will be returned.

-1: an exception occurs.

1: normal operation.

- **FetchThreadHandler**

1. Function description

   This function is used to obtain the TOA additional thread handler.

```
HANDLE FetchThreadHandler()
```

2. Input parameters description

-

3. Returned value

The TOA additional thread handler. When ToaFetcher instance is terminated, this handler will be closed.

- **FetchErrorInfo**

1. Function description

   This function is used to obtain the error code.

```
bool FetchErrorInfo(int* err_code_ptr, char* err_msg_ptr)
```

2. Input parameters description

   - err_code_ptr: An integer-type pointer to the error code, used to return the error code.

- err_msg_ptr: A character-type pointer to a string buffer. It contains at least 50 bytes of data and is used to return the error message.

3. Returned value

- TRUE: Obtained successfully.
- FALSE: Failed to obtain.

Error codes

Error Code	Error Message	Description
0	Ok	Normal
-1001	Exceed max server port number	The maximum number of ports is exceeded. Please check `InitUpToaFetcher: svr_port_num`.
-1002	Invalid IP address	Invalid IPv4 address
-1003	No suitable network interface	No suitable network interface found
-1004	System Error: find dev error	System error: no `dev` can be found. Please contact the lib developer.
-1005	System Error: start timer error	System error: an error occurs when starting the timer. Please contact the lib developer.
-1006	System Error: compile filter error	System error: an error occurs when compiling the filter rule. Please contact the lib developer.
-1007	System Error: set filter error	System error: an error occurs when configuring the filter rule. Please contact the lib developer.
-1008	System Error: open pcap error	System error: an error occurs when opening `dev`. Please contact the lib developer.
-1009	System Error: start pcap error	System error: an error occurs when starting the listener. Please contact the lib developer.
-1010	System Error: begin thread error	System error: an error occurs when starting the thread. Please contact the lib developer.
-1999	Unknown error	Unknown error. Please contact the lib developer.

Example

- **Initialize ToaFetcher:**

```
char ncard_ip_str[] = "1.1.1.1";
char svr_ip_str[] = "1.1.1.1";
char port_range[3][100] = {"10001-10005", "20001-20005", "30001-30005"};
char* port_range_ptr[3] = {port_range[0], port_range[1], port_range[2]};
u_short svr_port_list[3] = {1111, 2222, 3333};
ToaFetcher inst = ToaFetcher();
inst.InitUpToaFetcher((char*)ncard_ip_str, (char*)svr_ip_str, svr_port_list, 3
);
```

- **Obtain TOA:**

```
void GetToa(SOCKADDR_IN client_addr, ToaFetcher * toa_fetcher_ptr)
{
u_long fake_client_ip_addr = 0;
u_short fake_client_port = 0;
u_long real_client_ip_addr = 0;
u_short real_client_port = 0;
memcpy(&fake_client_ip_addr, &client_addr.sin_addr, 4);
memcpy(&fake_client_port, &client_addr.sin_port, 2);
bool ret = toa_fetcher_ptr->FetchToaValue(fake_client_ip_addr, fake_client_port
, real_client_ip_addr, real_client_port);
if(ret == FALSE){
printf("No toa found\n");
}else{
//fpp: Custom print function
fpp("real_client_ip_addr", &real_client_ip_addr, 4);
  fpp("real_client_port", &real_client_port, 2);
}
}
```

Go Version

TOA obtaining program obtains the real IP address from toa_win.exe through UDP communication.

Protocol format

- **Request:** `| ID (4Bytes) | FakeIPAddress (4Bytes) | FakePort (2Bytes) |`

The fields are described as follows:

- ID: The unique ID of the request and will be returned as it is in the response. It contains 4 bytes of data.
- FakeIPAddrss: The fake IP address of the client stored in the network byte order and can be obtained from the opposite address returned by the `accept` function of the server. It contains 4 bytes of data.
- FakePort: The fake port number of the client stored in the network byte order and can be obtained from the opposite address returned by the `accept` function of the server. It contains 2 bytes of data.
- **Response:** `| ID (4Bytes) | Code (1Byte) | RealIPAddress (4Bytes) | RealPort (2Bytes) |`

The fields are described as follows:

- ID: The unique ID of the request and is the same as that in the request. It contains 4 bytes of data.
- Code: It contains 1 byte of data. 0: real IP and port obtained successfully. 1: failed to obtain.
- RealIPAddress: If `Code` is 0, it indicates the real client IP address. It contains 4 bytes of data in network byte order.
- RealPort: If `Code` is 0, it indicates the real client port. It contains 2 bytes of data in network byte order.

Example

For more information, see demo.go. You can develop a TOA obtaining client on your own, or use the `queryToa` function in demo.go to obtain TOA.

1. **Function description**

```
func queryToa(serverAddr string, fakeIp string, fakePort uint16)(int32, string, uint16)
```

2. **Input parameters description**

- serverAddr: The string-type service communication address of toa_win.exe in the format of 127.0.0.1:9999.
- fakeIp: the string-type fake IP address in the format of 1.2.3.4.
- fakePort: The uint16-type fake port in the format of 8899.

3. **Returned value**

- The first returned value: It is in int32 type and used to indicate the error code.
  - 0: Obtained successfully
  - -1: Failed to get TOA. This may happen if `fakeIP` or `fakePort` is incorrect or the cache has expired.
  - -2: Failed due to a network communication exception.
- The second returned value: It is in string type and will return the real IP if TOA is obtained successfully, otherwise an empty string is returned.
- The third returned value: It is in uint16 type and will return the real port if TOA is obtained successfully, otherwise 0 is returned.

Obtaining Real Client IP Through Proxy Protocol (TCP Only)
Basic Principles

Last updated：2022-06-17 18:49:37

Proxy Protocol facilitates the transmission of client information (such as protocol stack, source IP, destination IP, source port, and destination port, etc.) by adding a header to the TCP, which is ideal for cases where network condition is complex and client IPs are required. During this process, the proxy inserts a data packet containing the original connection quadruple information into the connection after the three-way handshake.

To obtain client IPs using the Proxy Protocol method, you need to configure and enable it in the console first. It can only be configured for listeners with TCP. After the acceleration service is connected with the origin server, the Proxy Protocol text will be inserted into the first-transmitted `payload` packet.

Directions

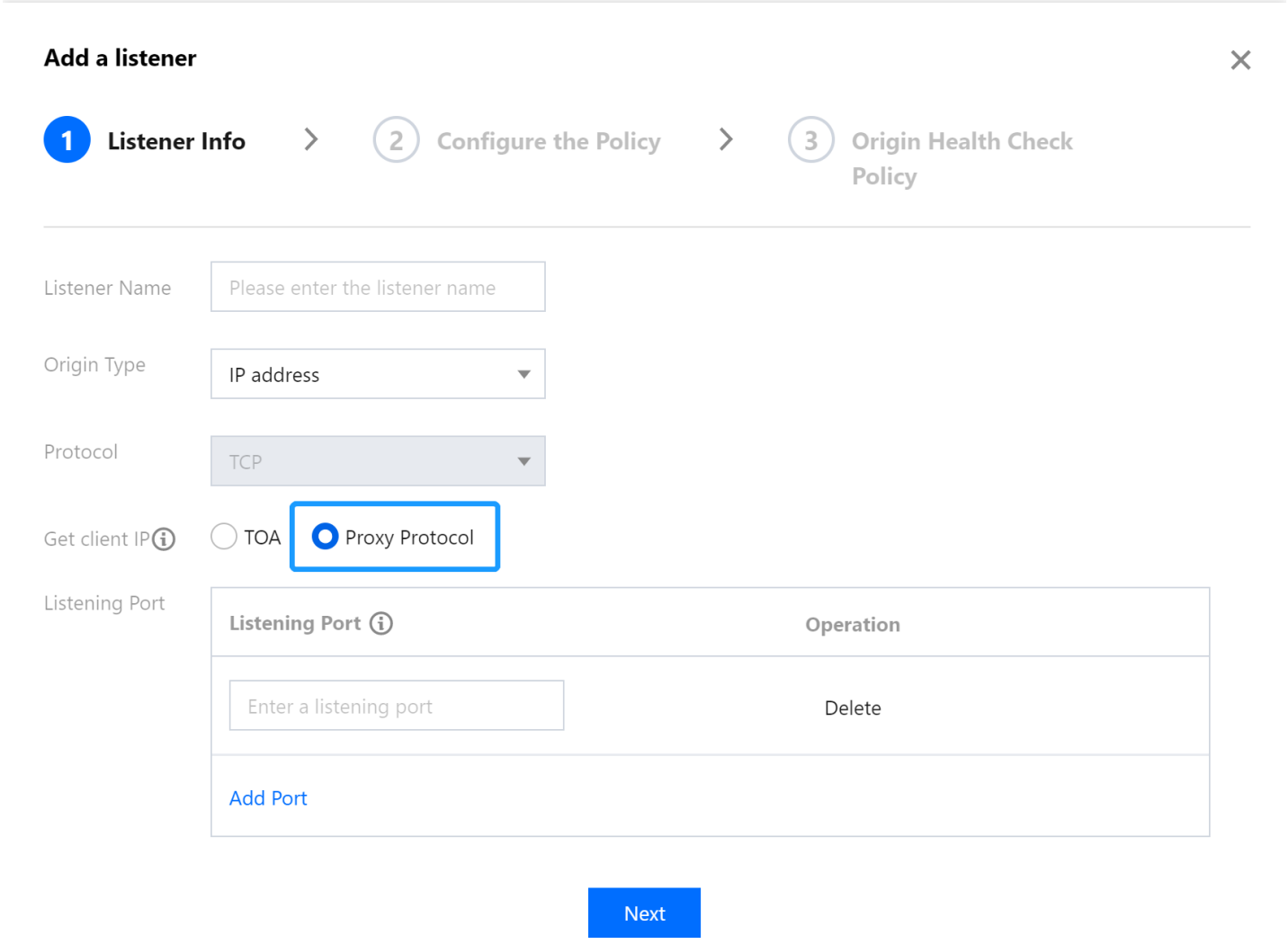
Last updated：2022-06-20 10:33:27

Note：
If there are problems with backend adaptation you cannot fix, please submit a ticket for assistance.

Step 1: Create a TCP Listener and Enable Proxy Protocol

Only layer-4 TCP allows Proxy Protocol to obtain the client real IP. Please enable Proxy Protocol in the acceleration connection as follows:

Log in to the GAAP console. Select **Access Management** > **TCP/UDP Listener Management**. Click **Create** to add a TCP listener and select TOA, and then complete configurations required to create the listener and connection.



Step 2: Adapt Proxy Protocol on the Backend Server

Both Nginx and HaProxy support Proxy Protocol.

For example, to configure Proxy Protocol in Nginx, you only need to add the parameter `proxy_protocol` to listen directive in a server block as follows:

```
http {
#...
server {
listen 80 proxy_protocol;
listen 443 ssl proxy_protocol;
#...
```

```
}
}
```

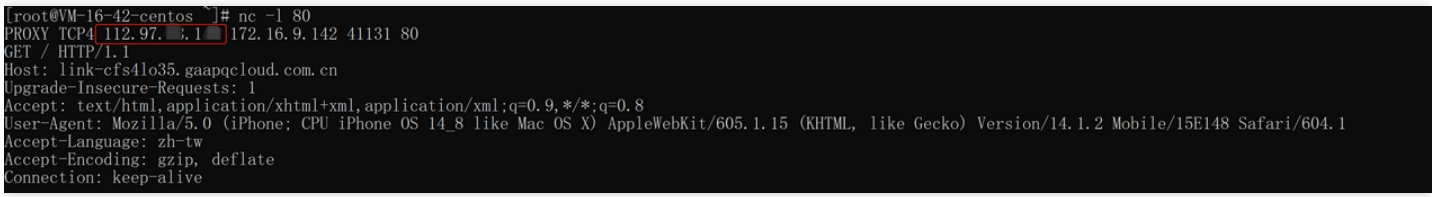
For programs that do not support Proxy Protocol, after the TCP connection is set up, you need to parse the Proxy Protocol text string as follows to obtain the client IP:

```
PROXY TCP4 1.1.1.2 2.2.2.2 12345 80\r\n
```

Step 3: View the Client IP

You can directly check the client IP in nginx logs. The log path is "/var/log/nginx/access.log".

You can also get the client IP with the command `nc -l port` .



Obtaining Real Client IP Through HTTP Header (HTTP/HTTPS)

Basic Principles

Last updated：2022-06-17 18:49:37

Using the HTTP/HTTPS listener, the origin server can directly get the real client IP from the `X-Real-IP` or `X-Forwarded-For` field in the HTTP request header. This feature is enabled by default.

It can also be customized as instructed in HTTP/HTTPS Listener Management. If there is an intermediate linkage such as CLB or self-built Nginx between the origin server and the program, you need to configure it by yourself to prevent the field from being overwritten by the intermediate linkage.

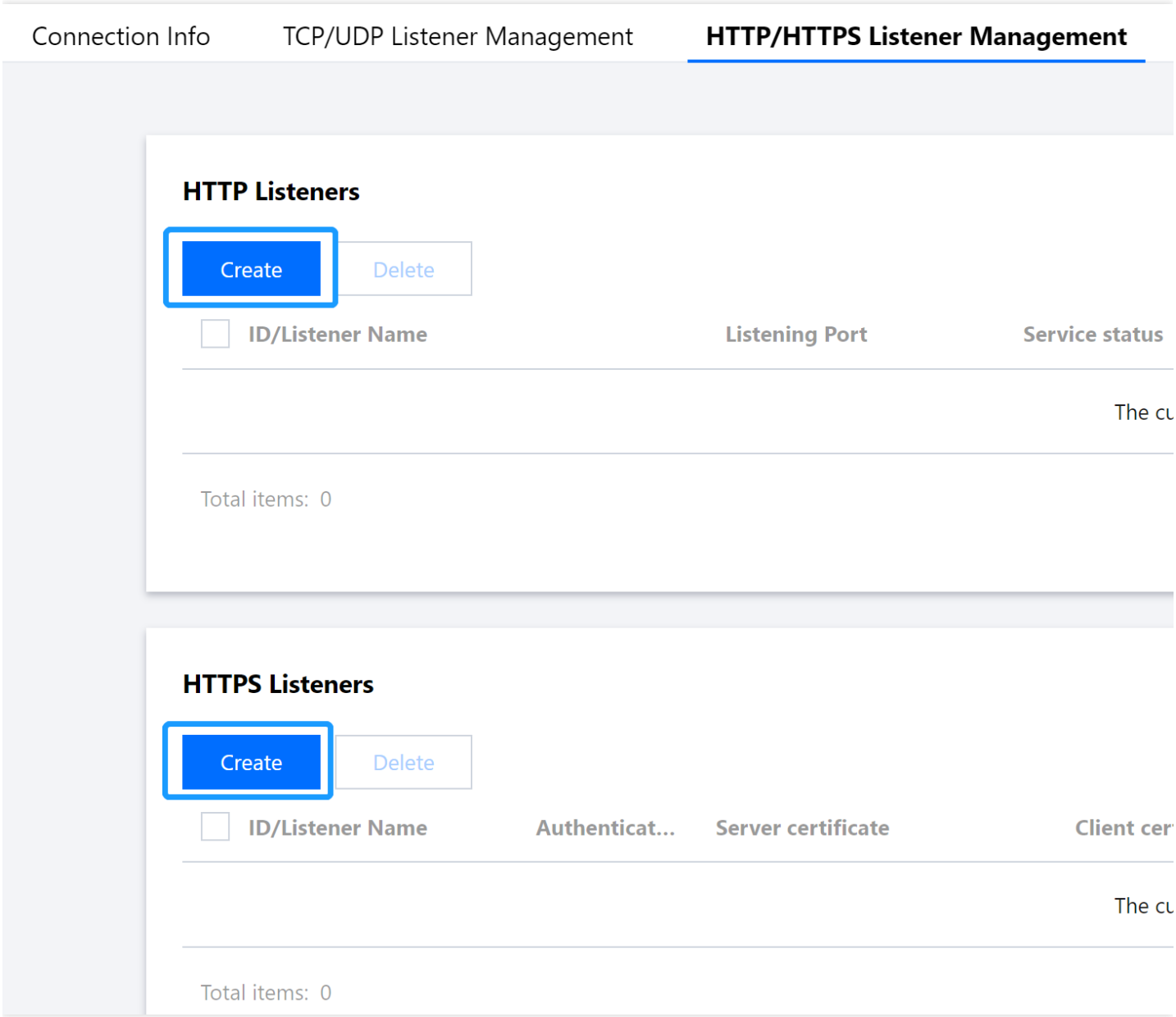
Directions

Last updated：2022-06-20 10:43:56

Note：
If there are problems with backend adaptation you cannot fix, please submit a ticket for assistance.

Step 1: Create an HTTP/HTTPS Listener

Log in to the GAAP console. Select **Access Management** > **HTTP/HTTPS Listener Management**. Click **Create** to add an HTTP/HTTPS listener, and then complete configurations required to create the listener and connection.



Step 2: Adapt the Backend Server

The following sections describe the X-Forwarded-For configuration schemes for Nginx, IIS 7, and Apache servers.

- IIS 7 configuration scheme
- Apache configuration scheme
- Nginx configuration scheme

IIS 7 configuration scheme

1. Download and install the F5XForwardedFor plugin module, copy `F5XFFHttpModule.dll` and `F5XFFHttpModule.ini` in the `x86\Release` or `x64\Release` directory based on your server operating system version to a certain directory (such as `C:\F5XForwardedFor` in this document), and make sure that the IIS process has read permission to this directory.
2. Select **IIS Server** and double-click **Modules**.

3. Click **Configure Native Modules**.

4. In the pop-up window, click **Register**.

5. Add the downloaded DLL files.

6. After adding the files, check them and click **OK**.

7. Add the above two DLL files in "ISAPI and CGI Restrictions" and set the restrictions to "Allow".

8. Restart the IIS server for the configuration to take effect.

Apache configuration scheme

1. Install the Apache "mod_rpaf" module using the following commands:

```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

2. Modify the Apache configuration file `/etc/httpd/conf/httpd.conf` by adding the following to the end of the file:

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
```

```
RPAFproxy_ips IP address //The IP address is the forwarding IP of the connectio
n
RPAFheader X-Forwarded-For
```

3. After adding the above content, restart Apache.

```
/usr/sbin/apachectl restart
```

Nginx configuration scheme

1. You can use `http_realip_module` to get the real client IP when Nginx is used as the server. However, this module is not installed in Nginx by default, and you need to recompile Nginx to add `--with-http_realip_module`. The code is as follows:

```
wget http://nginx.org/download/nginx-1.14.0.tar.gz
tar zxvf nginx-1.14.0.tar.gz
cd nginx-1.14.0
./configure --user=www --group=www --with-http_stub_status_module --without-htt
p-cache --with-http_ssl_module --with-http_realip_module
make
make install
```

2. Modify the `nginx.conf` file.

```
vi /etc/nginx/nginx.conf
Modify the configuration fields in red as follows:

fastcgi connect_timeout 300;
fastcgi send_timeout 300;
fastcgi read_timeout 300;
fastcgi buffer_size 64k;
fastcgi buffers 4 64k;
fastcgi busy_buffers_size 128k;
fastcgi temp_file_write_size 128k;

set_real_ip_from IP address; //The IP address is the forwarding IP of the conne
ction
real_ip_header X-Forwarded-For;
```

3. Restart Nginx.

```
service nginx restart
```

Country/Region Mapping

Last updated：2023-06-30 11:49:57

Due to different territory sizes of countries around the world, and considering data display and coverage of acceleration nodes, we have merged adjacent countries/regions into larger geographical zones, and split those with larger territories. When using the "globally unified domain name" feature and selecting regions to be covered by global acceleration nodes, refer to the following mapping between countries and regions to configure zones to be covered by global acceleration nodes.

Continent	Geographical Zone	Country/Region	Province/State
Asia	East Asia	Chinese mainland - East China	Shandong, Jiangsu, Anhui, Zhejiang, Jiangxi, Fujian, Shanghai
		Chinese mainland - South China	Guangdong, Guangxi, Hainan
		Chinese mainland - North China	Hubei, Hunan, Henan
		Chinese mainland - North China	Beijing, Tianjin, Hebei, Shanxi, Inner Mongolia
		Chinese mainland - Southwest China	Ningxia, Xinjiang, Qinghai, Shaanxi, Ganxu
		Chinese mainland - Southwest China	Sichuan, Yunnan, Guizhou, Tibet, Chongqing
		Chinese mainland - East China	Liaoning, Jilin, Heilongjiang
		Mongolia	
		North Korea	
		South Korea	
		Japan	
	Southeast Asia	Brunei	
		Macao (China)	

	Cambodia	
	East Timor	
	Indonesia	
	Laos	
	Malaysia	
	Myanmar	
	Philippines	
	Hong Kong (China)	
	Singapore	
	Taiwan (China)	
	Thailand	
	Vietnam	
South Asia	Bangladesh	
	Bhutan	
	India	
	Maldives	
	Nepal	
	Pakistan	
	Sri Lanka	
Central Asia	Kazakhstan	
	Kyrgyzstan	
	Tajikistan	
	Turkmenistan	
	Uzbekistan	
Western Asia	Afghanistan	

		Iraq	
		Iran	
		Syria	
		Jordan	
		Lebanon	
		Israel	
		Palestine	
		Saudi Arabia	
		Bahrain	
		Qatar	
		Kuwait	
		United Arab Emirates	
		Oman	
		Yemen	
		Georgia	
		Armenia	
		Azerbaijan	
		Türkiye	
		Cyprus	
Europe	Northern Europe	Finland	
		Sweden	
		Norway	
		Iceland	
		Denmark	
		Faroe Islands	

Eastern Europe	Estonia	
	Latvia	
	Lithuania	
	Belarus	
	Ukraine	
	Moldova	
Central Europe	Poland	
	Czech	
	Slovakia	
	Hungary	
	Germany	
	Austria	
	Switzerland	
	Liechtenstein	
Western Europe	United Kingdom	
	Ireland	
	Netherlands	
	Belgium	
	Luxembourg	
	France	
	Monaco	
Southern Europe	Romania	
	Bulgaria	
	Serbia	
	Macedonia	

		Albania	
		Greece	
		Slovenia	
		Croatia	
		Bosnia and Herzegovina	
		Italy	
		Vatican	
		San Marino	
		Malta	
		Spain	
		Portugal	
		Andorra	
Africa	North Africa	Egypt	
		Libya	
		Sudan	
		Tunisia	
		Algeria	
		Morocco	
		Madeira Island	
	Eastern Africa	Ethiopia	
		Eritrea	
		Somalia	
		Djibouti	
		Kenya	
		Tanzania	

		Uganda	
		Rwanda	
		Burundi	
		Seychelles	
	Central Africa	Chad	
		Central Africa	
		Cameroon	
		Equatorial Guinea	
		Gabon	
		Republic of the Congo	
		Democratic Republic of the Congo	
		Sao Tome and Principe	
	Western Africa	Mauritania	
		Senegal	
		Gambia	
		Mali	
		Burkina Faso	
		Guinea	
		Guinea-Bissau	
		Cape Verde	
		Sierra Leone	
		Liberia	
		Ivory Coast	

		Ghana	
		Togo	
		Nigeria	
		Benin	
		Niger	
	Southern Africa	Zambia	
		Angola	
		Zimbabwe	
		Malawi	
		Mozambique	
		Botswana	
		Namibia	
		South Africa	
		Swaziland	
		Lesotho	
		Madagascar	
		Comoros	
		Mauritius	
		Reunion	
Oceania	Oceania	Australia	
		New Zealand	
		Papua New Guinea	
		Solomon Islands	
		Vanuatu	
		Micronesia	

		Marshall Islands	
		Palau	
		Nauru	
		Kiribati	
		Tuvalu	
		Samoa	
		Fiji	
		Tonga	
		Cook Islands	
		Guam	
		New Caledonia	
		Wallis and Futuna	
		Niue	
		Tokelau	
		American Samoa	
		Northern Mariana	
North America	North America	Canada	
		Eastern US	Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, Connecticut, New York, Pennsylvania, New Jersey, Delaware, Maryland, Washington, D.C, Virginia, West Virginia, North Carolina, South Carolina, Georgia, Florida, Kentucky, Tennessee, Mississippi, Alabama
		Western US	Idaho, Montana, Wyoming, Nevada, Utah, Colorado, Arizona, New Mexico, Alaska, Washington, Oregon, California, Hawaii
		Central US	Wisconsin, Michigan, Illinois, Indiana, Ohio, Missouri, North Dakota, South Dakota, Nebraska, Kansas, Minnesota, Iowa, Oklahoma, Texas, Arkansas, Louisiana

		Mexico	
		Greenland	
	Central America	Guatemala	
		Belize	
		El Salvador	
		Honduras	
		Nicaragua	
		Costa Rica	
		Panama	
	Caribbean	Bahamas	
		Cuba	
		Jamaica	
		Haiti	
		Dominican	
		Antigua and Barbuda	
		Saint Kitts and Nevis	
		Dominica	
		Saint Lucia	
		Saint Vincent and the Grenadines	
		Grenada	
		Barbados	
		Trinidad and Tobago	
		Puerto Rico	

		British Virgin Islands	
		U.S. Virgin Islands	
		Anguilla	
		Montserrat	
		Guadeloupe	
		Martinique	
		Dutch Caribbean	
		Aruba	
		Turks and Caicos Islands	
		Cayman Islands	
		Bermuda	
South America	Northern South America	Colombia	
		Venezuela	
		Guyana	
		French Guiana	
		Suriname	
	Midwestern South America	Ecuador	
		Peru	
		Bolivia	
	Eastern South America	Brazil	
	Southern South America	Chile	
		Argentina	
		Uruguay	

		Paraguay	