# Alibaba Cloud gameshield

## Best Practices

Issue: 20190905

# Legal disclaimer

**Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.**

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

# Generic conventions

Table -1: Style conventions

| Style | Description | Example |
| --- | --- | --- |
|  | This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. |  Danger:<br>Resetting will result in the loss of user configuration data. |
|  | This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. |  Warning:<br>Restarting will cause business interruption. About 10 minutes are required to restore business. |
|  | This indicates warning information, supplementary instructions, and other content that the user must understand. |  Notice:<br>Take the necessary precautions to save exported data containing sensitive information. |
| | This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user. |  Note:<br>You can use Ctrl + A to select all files. |
| > | Multi-level menu cascade. | Settings > Network > Set network type |
| Bold | It is used for buttons, menus , page names, and other UI elements. | Click OK. |
| `Courier font` | It is used for commands. | Run the `cd /d C:/windows` command to enter the Windows system folder. |
| *Italics* | It is used for parameters and variables. | `bae log list --instanceid` *Instance_ID* |
| [] or [a\|b] | It indicates that it is a optional value, and only one item can be selected. | `ipconfig` *[-all\|-t]* |

| Style | Description | Example |
| --- | --- | --- |
| {} or {a\|b} | It indicates that it is a required value, and only one item can be selected. | `swich {stand \| slave}` |

# Contents

# 1 Best practice for achieving fast data transmission

This topic describes how to design a fast transmission plan with GameShield to satisfy your business requirements.

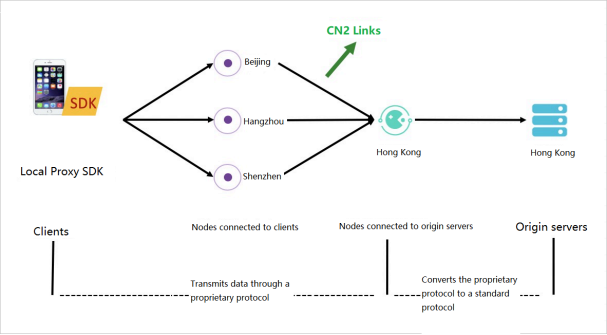
## Background

GameShield provides nodes in some regions and allows the nodes to establish connections to origin servers and clients to achieve fast data transmission. For example, if your origin server is located in the China (Shenzhen) region, GameShield can establish connections starting from China (Beijing) to China (Shenzhen) for your gamers in northern China. In this way, these gamers can enjoy fast access to your origin server.

However, the routing algorithm of GameShield focuses on defending against attacks. It only selects the fastest transmission link from a client to the connected node instead of the entire transmission link.

If you need fast data transmission, we recommend that you design a transmission plan based on your own business requirements.

## Plan description




- Nodes in all supported regions can establish connections to clients. These nodes can be used only for your gaming service.
- GameShield selects a node in a region to establish the optimal connection to the origin.
- Two nodes within the border are connected over the Alibaba Cloud network while cross-border transmission between two nodes is through the CN2 network.
- Although fast transmission plans do not affect the capability of GameShield against DDoS attacks and HTTP flood attacks, some users may experience poorer services while GameShield is in defense mode.

### Supported regions

Currently nodes are available in the following regions:

- Regions where nodes can connect to clients: China (Hangzhou), China (Beijing), and China (Shenzhen) in what regions BGP is deployed, Wuhan where only China Telecom provides transmission links, and Shijiazhuang where only China Unicom provides transmission links.
- Regions where nodes can connect to origin servers:
  - Regions in Mainland China: China (Hangzhou), China (Shanghai), China (Beijing), and China (Shenzhen) in what regions BGP is deployed.
  - Regions outside Mainland China: China (Hong Kong) and Singapore in what regions BGP is deployed.

### Procedure

1. When initializing SDK, you need to obtain endpoints that are used for accessing nodes from clients based on different `GroupName` values, but the same origin IP address and port.

   The core interface is `YunCeng . getProxyTc pByDomain ( Token , GroupName , Dip , Dport )` with multiple `GroupName` values input. With this interface, you can obtain the following endpoints:

   ```
   Link 1 from China ( Hangzhou ) to China ( Hong Kong ): https :// yxd . example . com : 54723
   Link 2 from China ( Shenzhen ) to China ( Hong Kong ): https :// yxd . example . com : 45712
   Link 3 from China ( Beijing ) to China ( Hong Kong ): https :// yxd . example . com : 56371
   Link 4 from a region where Alibaba Cloud Anti - DDoS Pro is activated to China ( Hong Kong ) with filing not required or other traditiona l transmissi on links : https :// gf . example . com
   ```

   **Note:**
   The process of obtaining an endpoint is equivalent to that of domain name resolution, which does not affect your business.

2. You can call the SpeedTest interface of the business SDK to test the delay of multiple transmission links over which clients can access origin servers. Then, you can compare the test results. For example, you can use `https :// yxd .`

`example . com : 17281 / speedtest` to complete a test. The result is shown as follows:

```
{
 " baiduPingD  elay ": " 533 ",
 " domainName ": " https :// yxd . example . com : 51567 ",
 " domainName  Delays ": [{
   " delay ":  1990 ,
   " url ": " https :// yxd . example . com : 51567 "
 }, {
   " delay ":  2174 ,
   " url ": " https :// yxd . example . com : 37869 "
 }, {
   " delay ":  2369 ,
   " url ": " https :// yxd . example . com : 38465 "
 }, {
   " delay ":  3196 ,
   " url ": " https :// yxd . example . com : 42877 "
 }],
 {
   " delay ": 23196 ,
   " url ": " https :// gf . example . com "
 }],
 " ipAddress ": " 113 . 210 . 179 . 96 ",
 " netWorkTyp  e ": " 4G ",
 " operator ": "",
 " phoneModel ": " VKY - L29 ",
 " systemVers  ion ": " 9 "
}
```

You can upload the result to Log Service for comparison and analysis.

3. From the result, use the endpoint (https://yxd.example.com:51567) with the shortest delay (1990) to access your business.

You can also perform other tests based on your business requirements. For example,

- enable or disable a transmission link,
- specify a link for a group of gamers, and
- allow gamers to select transmission links.
- You can cache these test results to accelerate the startup of applications.

# 2 Best practice for dealing with HTTPS business

This topic describes how to use GameShield to deal with HTTPS business.

## Background

It requires several complex steps to deal with HTTPS business by using GameShield. You need to take some steps to tackle HTTPS compatibility issues, such as certificate verification, cookie insertion, and Server Name Indication (SNI).

This topic provides you a solution in the scenario where you want to use GameShield to deal with HTTPS business.

## Solution

To solve the compatibility issue of certificate verification, GameShield introduces a domain name (www-yxd.test.com) that resolves to 127.0.0.1. In comparison to dealing with TCP business, you need to use domain names and take a stitching step for domain name resolution.

Step 1. https://www.test.com

Step 2. https://127.0.0.1:28291 (Certificate verification may fail.)

Step 3. https://www-yxd.test.com:28291 (GameShield introduces a domain name that resolves to 127.0.0.1. You must configure the server to listen to the domain name.)

The procedure for TCP business is also provided for comparison.

Step 1. tcp://1.1.1.1:8001

Step 2. tcp://127.0.0.1:21781

To use this solution, you must configure the server to listen to the domain name that is introduced (www-yxd.test.com).

However, this solution has the following problems:

GameShield is designed to eliminate the need for DNS and avoid business unavailability caused by DNS hijacking. However, domain name resolution is introduced in this solution, which increases the risk of hijacking. Test results show that DNS servers of some Internet service providers (ISPs) do not respond to the resolution from a domain name to 127.0.0.1, thereby affecting business.

### Use a custom DNS server

To solve the potential problem of the domain name that resolves to 127.0.0.1, you can check whether your network protocols support resolution by custom DNS servers. If yes, we recommend that you use a custom server to resolve the domain name (www-yxd.test.com) instead of a DNS server provided by an ISP. In this way, you can avoid DNS spoofing and hijacking.

For example, with the DNS interface in the OkHttp library, you can resolve the domain name used by GameShield through a custom DNS server.

In comparison to resolving the domain name to 127.0.0.1 by using a DNS server of an ISP, resolution by a custom DNS server is implemented based on a DNS interface. In this way, it helps prevent DNS hijacking. Resolution by a custom server is easy to implement and requires minimum code modification. It is well suited for many scenarios, such as HTTPS certificate verification, cookie insertion, and SNI.

This practice also applies to the scenario where the Retrofit and OkHttp libraries are used. After you have configured OkHttpClient, use it as the argument for `Retrofit . Builder :: client ( OkHttpClie nt )`.

As for other libraries, you can search for solutions on the Alibaba Cloud website.

# 3 Best practice for obtaining the real IP address of a client

This topic describes how to obtain the real IP address of a client after GameShield is activated for your business.

## Background

GameShield adopts full network address translation (NAT). After receiving a request from a client, GameShield replaces the IP address of the client with the IP address of GameShield. This topic provides you a solution in the scenario where you want to obtain the real IP address of the client.

## Principle

GameShield transfers the IP address of a client through the Option field of TCP and thus provides a module called TCP Option Adapter (TOA). The TOA module is only applicable to GameShield. To obtain the real IP address of the client, you need to integrate the TOA module with your origin servers. You can integrate the TOA module in the kernel, applications, or code. Select the easiest method based on your business requirements.

## Integration methods

Table 3-1: Architectures for different scenarios

| Scenario | Supported architecture | Unsupported architecture |
| --- | --- | --- |
| Obtain the real IP address of a client when the client uses TCP for transmission | · GameShield -> Alibaba Cloud servers or servers that are not provided by Alibaba Cloud<br>· GameShield -> Alibaba Cloud Layer-4 Server Load Balancer (SLB) -> Alibaba Cloud servers | GameShield -> Layer-4 server-side load balancers that are not provided by Alibaba Cloud -> servers |

| Scenario | Supported architecture | Unsupported architecture |
| --- | --- | --- |
| Obtain the real IP address of a client when the client uses HTTP/HTTPS for transmission | · GameShield -> Alibaba Cloud servers or servers that are not provided by Alibaba Cloud<br>· GameShield -> Alibaba Cloud Layer-4 SLB -> Alibaba Cloud servers | · GameShield -> Alibaba Cloud Layer-7 SLB ( including WAF/Anti-DDoS Pro) -> Alibaba Cloud servers<br>· GameShield -> Layer-4 or Layer-7 server-side load balancers that are not provided by Alibaba Cloud -> servers |

 Note:

GameShield is based on Layer-4 server-side load balancers. It does not manage HTTPS certificates, and cannot read data from HTTPS data streams. The real IP address of a client is not obtained from the X-Forwarded-For (XFF) HTTP header field. Instead, it is obtained by using the TOA module of the server.

Table 3-2: Support for operating systems (OSs)

| Module | Linux | Windows |
| --- | --- | --- |
| TOA module in the kernel (Code modification is not required.) | Partially supported | Not supported |
| Hook-TOA module in applications (Code modification is not required.) | Supported | Partially supported |
| TOA module in code (Code modification is required.) | Supported | Supported |

Description

- Linux

  If your origin servers are running CentOS and GameShield supports your kernel version, we recommend that you install the TOA module in the kernel.

  If your kernel version is not supported, integrate the Hook-TOA module in applications.

  If the Hook-TOA module in applications is not applicable, modify code to integrate the TOA module.

- Windows

  Some Windows applications support integration with the Hook-TOA module. We recommend that you integrate the Hook-TOA module in the applications.

  If you cannot integrate the Hook-TOA module, modify code to integrate the TOA module.

### Integrate the TOA module in the kernel

> **Note:**
> We recommend that you use CentOS 7.2 because it is the most stable OS. If your origin servers are not running CentOS 7.2 and switching the OS does not affect your business, we recommend that you switch to CentOS 7.2. This helps you gain the real client IP address in an easier way.

To install the TOA module in a Linux kernel, perform the following steps:

1. Verify that the kernel version is supported and the kernel has all required modules. GameShield supports the Linux kernel version of 2.6.32-642.13.1. You need to check whether the TOA module supports your kernel version.

   If you need to install a required kernel module, run the corresponding command.

   ```
   modprobe   nf_conntra  ck_ipv4
   modprobe   nf_defrag_  ipv4
   modprobe   xt_state
   modprobe   nf_conntra  ck
   modprobe   iptable_fi  lter
   modprobe   ip_tables
   ```

2. Run the vi /etc/sysctl.conf command to edit the sysctl.conf file and include the following options in the file.

   ```
   vi  / etc / sysctl . conf
   net . ipv4 . tcp_fin_ti  meout  =  10
   net . ipv4 . tcp_tw_rec  ycle =  1
   ```

```
net . ipv4 . tcp_tw_reu  se  =  1
net . ipv4 . tcp_keepal  ive_time  =  15
net . ipv4 . tcp_max_tw  _buckets  =  1048576
net . nf_conntra  ck_max = 655360
```

**Note:**

The last option in this configuration text does not exist. You must add this option.

3. Run the following command to allow the changes to take affect.

```
sysctl  - p
```

4. Run the following command to install the module.

```
 insmod     XXXX . ko  ( Replace  XXXX  with  a  module  name
.)
```

You can run the following commands to perform other operations on the module.

- Check whether the module is installed.

```
 lsmod  |  grep  toa
```

- Delete the module.

```
  rmmod  ali_flex_t  oa
```

- View the module information.

```
modinfo   ali_flex_t  oa . ko
```

- View the operating status of the module.

```
cat  / proc / aliflex / toa
```

### Integrate the Hook-TOA module in applications

Perform the following steps to integrate the Hook-TOA module:

1. Run the *install . sh* command to install services related to toa-server.
2. Include the *preload . so* parameter in the command to start the server. If the server name is nginx, run the following command to start the server.

```
LD_PRELOAD =./ preload . so  ./ nginx
```

**Note:**

You must find the entry point of your program and include the parameter in the preceding command to start the service.

### Integrate the TOA module in code

**For more information, see the instructions in the TOA archive. You can also consult the GameShield service team for more details.**