Alibaba Cloud gameshield

Quick Start

Issue: 20190118

MORE THAN JUST CLOUD | Alibaba Cloud

Legal disclaimer

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

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

al property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

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

Contents

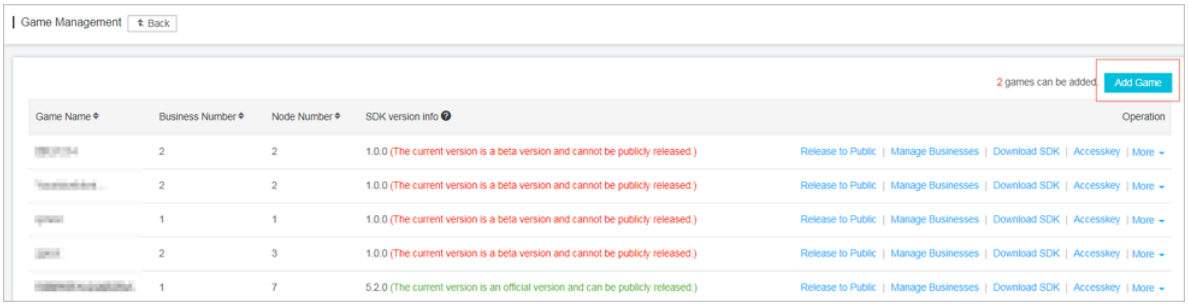
Legal disclaimer.....I
Generic conventions..... I
1 Step 1: Create a Game..... 1
2 Step 2: Create a Business..... 2
3 Step 3: Configure Forwarding Rules.....4
4 Step 4: Configure Business Group..... 6
5 Step 5: Complete Access.....8
6 SDK integration..... 9
6.1 Get SDK..... 9
6.2 Integration summary.....10
6.3 Key Points of SDK Access..... 11
7 CNAME Access.....14
7.1 CNAME access method.....14

1 Step 1: Create a Game

Context

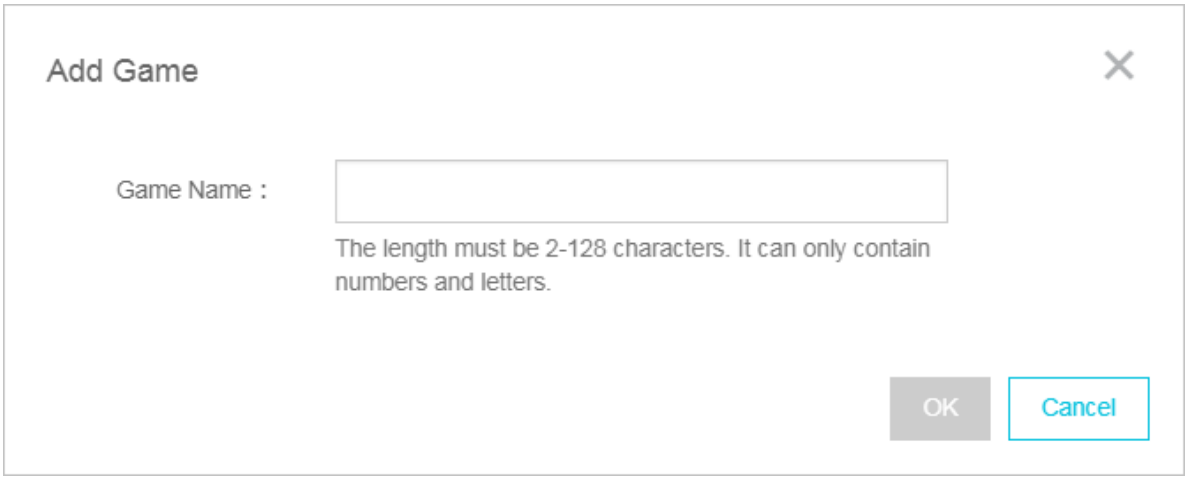
Procedure

1. Log on to the Alibaba Cloud Security Game Shield Management console, go to **Business Management**, click **Manage** to open the *Game Management* page.
2. Click **Add Game** in the upper right corner.



3. Enter the game name and click **OK**.

> **Note:**
> The game name is up to 24 characters and only supports English letters, numbers, or Chinese characters.

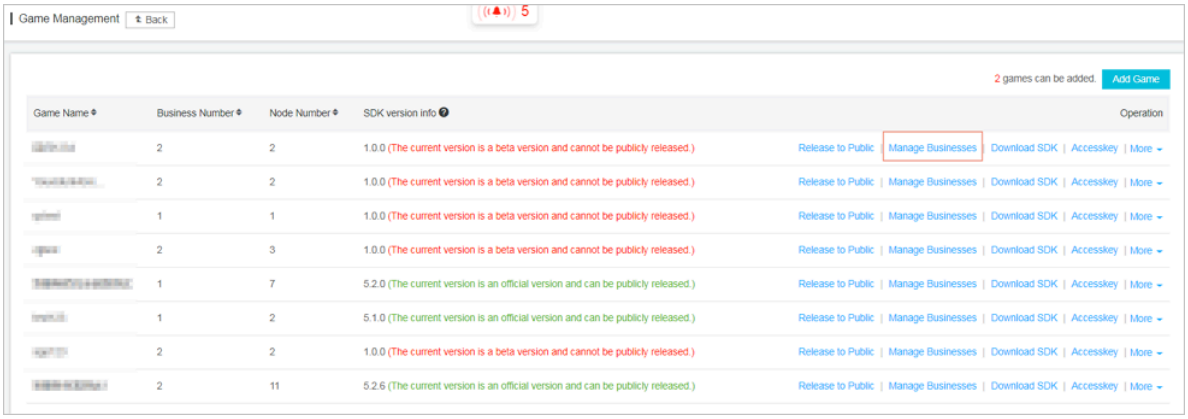


2 Step 2: Create a Business

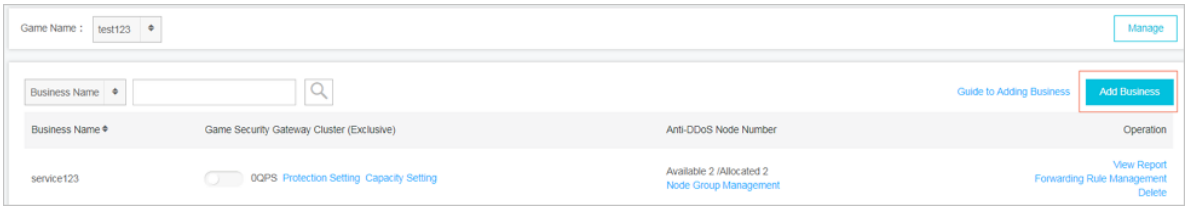
Context

Procedure

1. Log on to the Alibaba Cloud Security Game Shield Management console, go to **Business Management**, click **Manage** to open the *Game Management* page.
2. Select the game that you created, and click **View Business**.

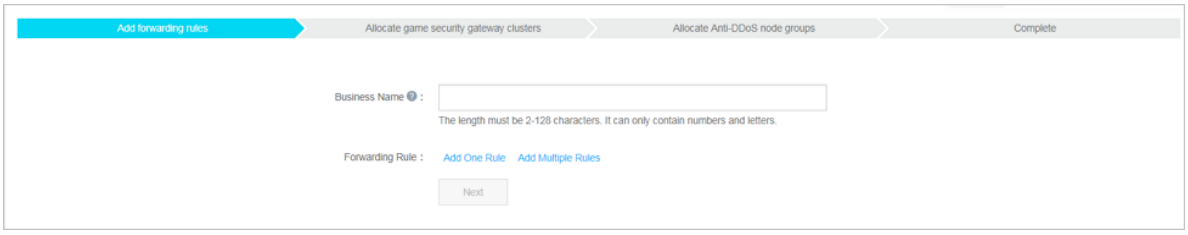


3. Click **Add Business**.

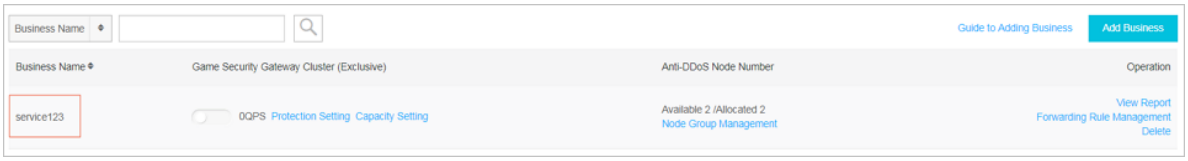


4. Fill in the business name and click **Next**.

> **Note:**
> You can click **Next** until the business is created. Forwarding rules and business grouping can be configured after the business creation.



Complete the business creation.

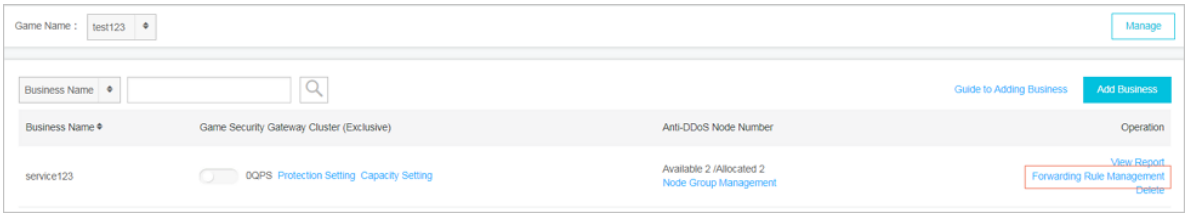

Business Name
Guide to Adding Business
Add Business
Business Name
Game Security Gateway Cluster (Exclusive)
Anti-DDoS Node Number
Operation
service123
0QPS Protection Setting Capacity Setting
Available 2 /Allocated 2
Node Group Management
View Report
Forwarding Rule Management
Delete

3 Step 3: Configure Forwarding Rules

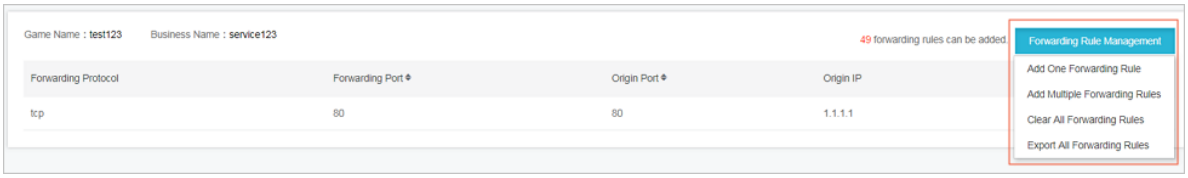
Context

Procedure

1. Log on to the Alibaba Cloud Security Game Shield Management console, go to **Business Management**, and select **Game Name**.
2. Locate to the business that you added, and click **Forwarding Rule Management**.



3. Click **Rule Management** and select **Add a rule**.



4. In the **Add Rule** dialog box, fill in the forwarding rule, and click **OK**.

Note:

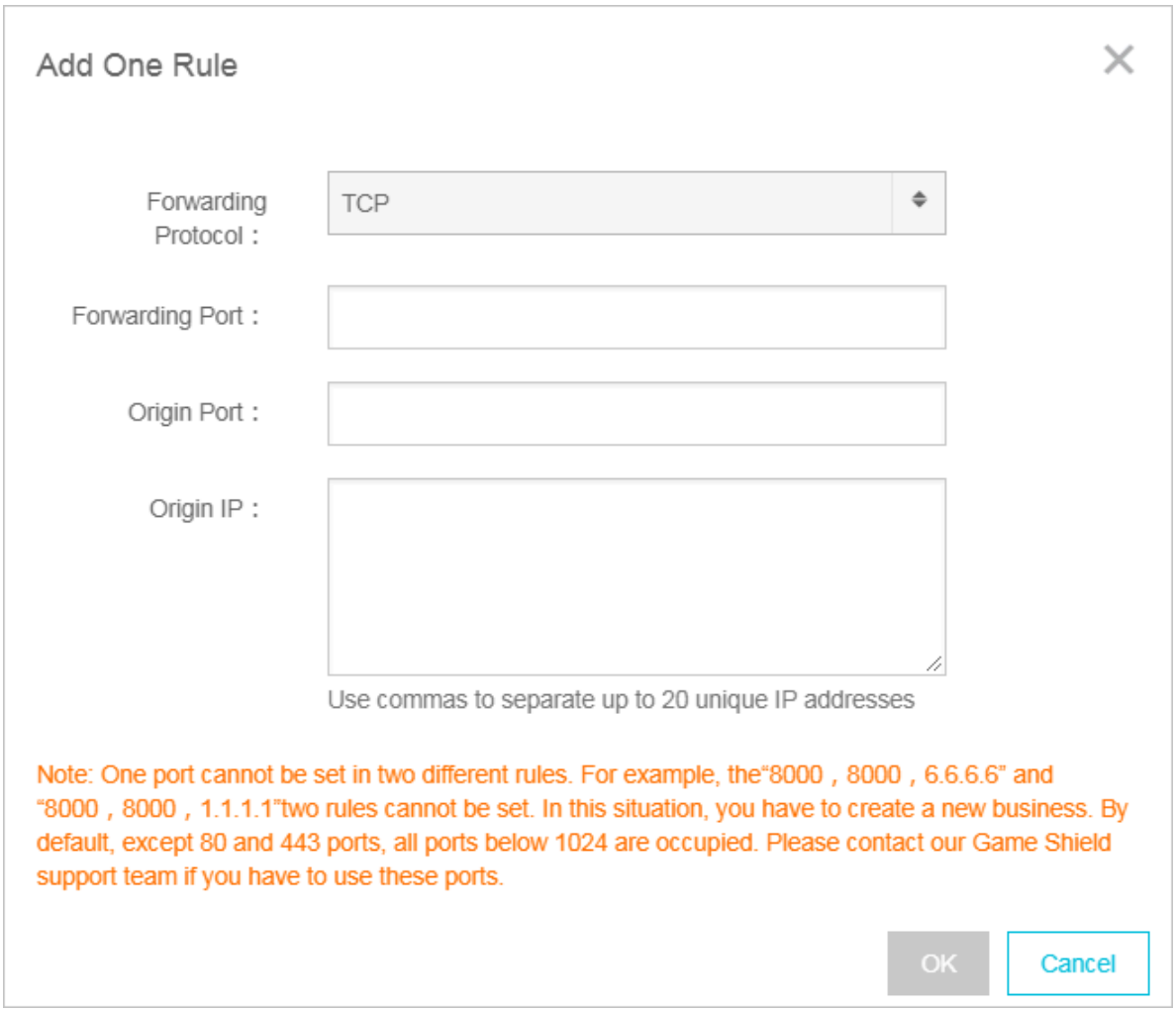
If a port corresponds to multiple origin site IPs, the IPs can be entered to the **Origin IPs** field, separated by commas (up to 20 IPs). After multiple origins are configured, load balancing is achieved automatically through polling.

Note:

Multiple rules for a same port are not allowed, for example, “8000, 8000, 6.6.6.6” and “8000, 8000, 1.1.1.1” cannot appear simultaneously. Under such circumstance, you must create a new business.

Note:

Ports below 1024, except port 80 and port 433, are system reserved ports. If you want to add such ports, please contact the Game Shield team.

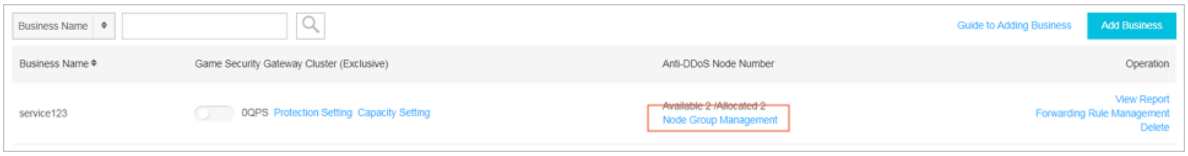

Add One Rule
Forwarding Protocol :
TCP
Forwarding Port :
Origin Port :
Origin IP :
Use commas to separate up to 20 unique IP addresses
Note: One port cannot be set in two different rules. For example, the“8000，8000，6.6.6.6” and “8000，8000，1.1.1.1”two rules cannot be set. In this situation, you have to create a new business. By default, except 80 and 443 ports, all ports below 1024 are occupied. Please contact our Game Shield support team if you have to use these ports.
OK
Cancel

4 Step 4: Configure Business Group

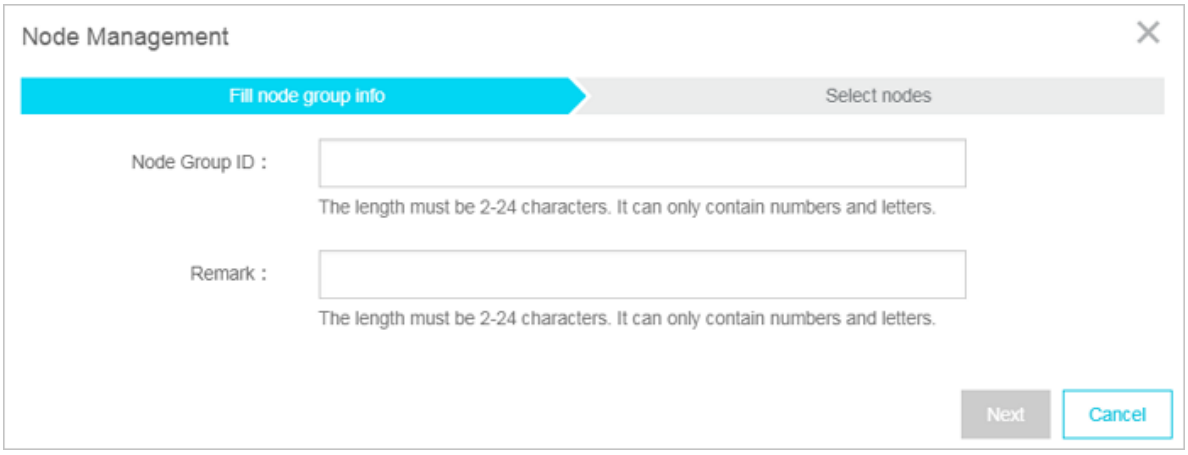
Context

Procedure

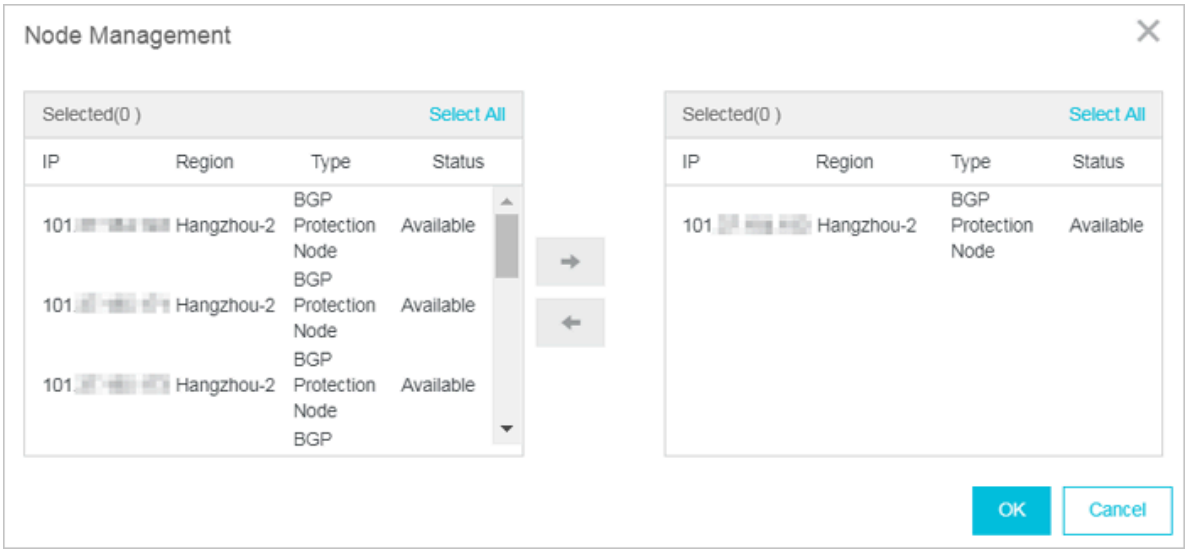
1. Log on to the Alibaba Cloud Security Game Shield Management console, go to **Business Management**, and select **Game Name**.
2. Locate to the added business, click **Node Group Management** to open the **Node Group Management** page.



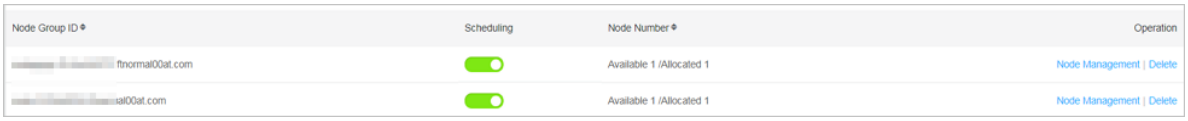
3. Click **Add Node Group**.
4. Fill in the node group identity and remark fields.



5. Select corresponding protection nodes to add to the node group.



6. Click **OK** to complete the node group configuration.



After the node group configuration completes, the node group identity information (for example, default.xxxxx.ftnormal00al.com) is the scheduling CNAME of the node group.

5 Step 5: Complete Access

Game Shield offers two access methods:

- CNAME access
- SDK access (recommended)

CNAME Access

The group name obtained in step four is a scheduling CNAME. You can complete the access of Game Shield by resolving the service domain name to this CNAME address.

Note:

1. When large DDoS attacks cause intra-group IP switchover, the CNAME scheduling time is usually over 10 minutes, and is uncontrollable due to the influence of the carrier's DNS cache.

SDK Access

SDK scheduling occurs at the second-level and has the functions of link detection and smart scheduling.

For SDK access guide, see the corresponding SDK access documents.

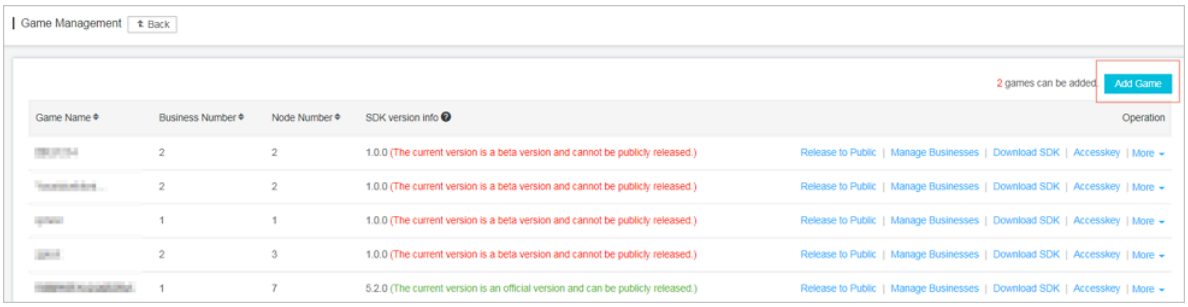
6 SDK integration

6.1 Get SDK

Context

Procedure

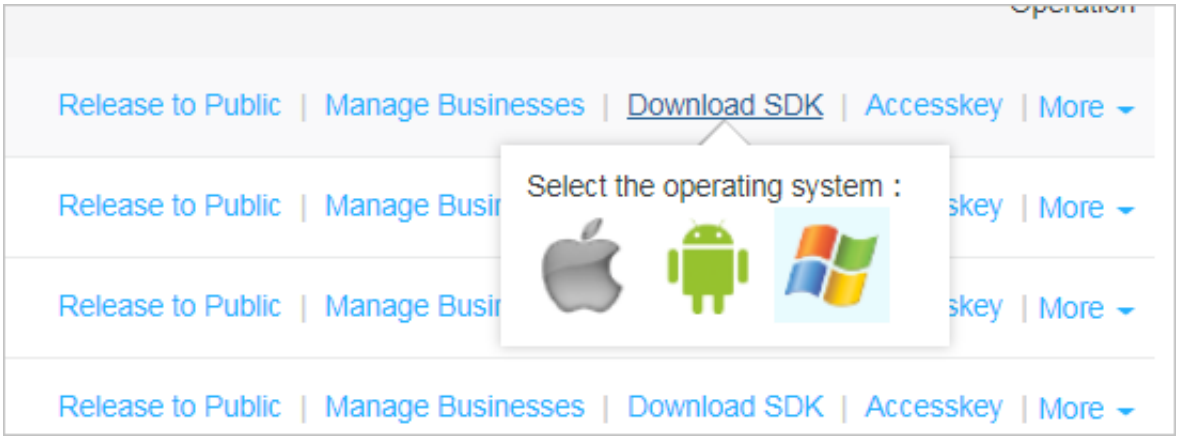
1. Log on to the Alibaba Cloud Security Game Shield Management console, go to **Business Management**, click **Manage** to open the *Game Management* page.



2. Locate a game that has been added, click **Download SDK**, select the applicable operating system, and download the SDK package.

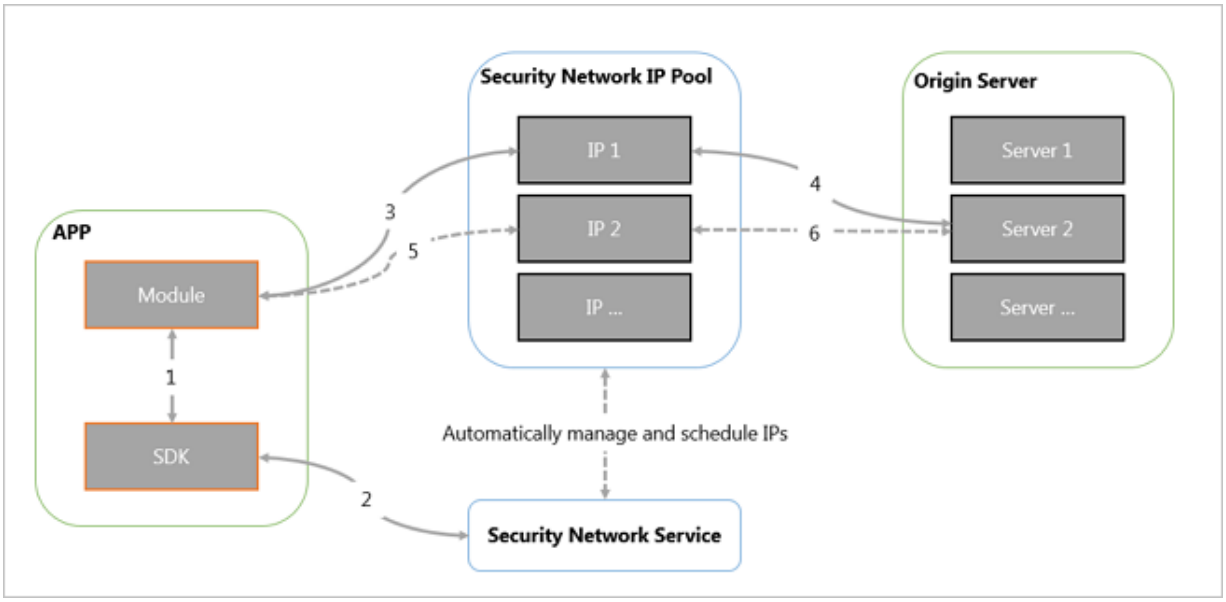
Note:

- The default testable version provided is the SDK1.0.0. This version can be debugged, but does not provide high-strength encryption.
- The official version can be obtained by contacting the Game Shield team after the SDK is activated. Each user gets a customized encrypted version.
- The Game Shield SDK after version 5.2.5 is docked through *SDK encrypted tunnel*, which can solve protocol stimulation-based connection flood attacks.



6.2 Integration summary

1. Typical access scenario



2. Integration process

For how to integrate with the program, see the help manual in the corresponding SDK package, which differs for different versions.

3. Appendix

Return value definition

Return value	Definition
0	Success
1000-1999	Network communication error

Return value	Definition
2000-2999	Appkey and initialization error
3000-3999	Game Shield console error
4000-4999	Data exchange with Game Shield console error
9000-9999	SDK error

If the problem persists, please contact **Technical Support**.

6.3 Key Points of SDK Access

Key Points of SDK Access.

1. Obtain the Game Shield node IP and port

The client must call the SDK's initialization interface as early as possible. We recommend putting it at the head of all service logic.

The changes in the process before accessing the original server are as follows:

- Original: The client obtains the server IP and port -> connects the server
- New: The client calls the SDK to get the Game Shield IP and port -> connects the Game Shield IP and port -> the server

The IP and port returned by Game Shield must be fully used. The IP and port instances returned by Game Shield are as follows:

- Normal mode: 116.211.171.31 10009
- Link encryption mode: 127.0.0.1 56382 (*How to be immune to connection flood attacks*)

Normal mode returns public IP addresses and fixed ports (with the same forwarding rule configuration), while link encryption mode returns local addresses and random ports.

2. Optimization of the logic for the client to reconnect after losing connection

When the client times out in the heartbeat or connection, it usually needs to immediately enter the reconnection logic. We suggest that the time-out period be 3 to 5 seconds (referring to the time for issuing cards in a game), and prompt the user of connection failure when reconnection exceeds 3 to 5 times or when the reconnection time exceeds 60 seconds. This may weaken the user's perception of reconnection.

The logic of communications between the client and the server must be that a data request is first initiated by the client before the server responds, otherwise it is blocked by the Game Security Gateway cluster of Game Shield as an null connection attack.

3. Server-side optimization and transformation

The user's online status must be determined to set the aging time (usually 15 to 30 seconds).

The user's re-login must be processed such that the new login user kicks out the old logged-in user (the reconnection may be faster than the aging time).

To obtain the real client IP, see *Obtain real client IP*.

4. IPV6 support

Game Shield supports the IPv6 environment. During the iOS audit, Game Shield automatically determines the network environment to enable the IPv6 dispatching and forwarding environment.

5. Downgrade when the Game Shield service is unavailable

The client must downgrade when Game Shield calls the SDK and returns a non-zero code. The usual practice is to hard code the Anti-anti-DDoS node of Game Shield as the backup logic, and use the Anti-DDoS Pro service as the backup service when the Game Shield service is unavailable.

Whether Game Shield is enabled or not, a switch must be set on the server side to control the flow of data.

6. Suggestions for user grouping and Game Shield node grouping

We recommend that your server also implement stratified governance on your clients. Different users correspond to different Game Shield groups. The general logic is as follows:

- New players are those whose registration time is less than 10 days
- Old players are those whose registration time is below 10 days, whose game time is below or equal to 10 hours, or who have played below 30 games
- VIP players are those whose game time is over 10 hours, who play over 30 games, or who have spent over 100 rmb in the game

The preceding logic is for reference only. You can modify it according to your service situation. We recommend that you update the logic of user grouping regularly.

The service can assign custom users to a designated Game Shield group and has the logic for manually dispatching malicious users once they are detected.

7. Check before officially taking the client online

The following must be checked to ensure the protective effect of Game Shield after access:

1. Game Shield's on-off switch.
2. Scheduling logic and scheduling time of nodes in Game Shield groups after the nodes are put into the black hole routing status (contact the Game Shield team to simulate attacks).
3. Scheduling logic for when the Game Shield SDK fails to obtain the node (contact the Game Shield team to simulate attacks).
4. Manual scheduling function of Game Shield. (Non-mandatory, and this can be implemented through smart scheduling of Game Shield)
5. Game Shield SDK's compatibility after integration (provide APK and IOS packages to the Game Shield team for stability and compatibility test).

7 CNAME Access

7.1 CNAME access method

This article introduces the CNAME access method of Game Shield.

CNAME Access Description

Advantages: easy and fast access, and smart resolution and automatic scheduling ability of black hole routing.

Disadvantages: slow switching, and direct exposure of the Game Shield node.

Note:
The CNAME access is recommended only when access to the SDK is unavailable. Only with access through the SDK can you enjoy the full protection benefits of Game Shield.

How do you configure CNAME access?

The name of the node group is the CNAME where the Game Shield access uses.

What is CNAME smart scheduling logic?

Default line: The BGP line has a higher priority than a single line. If there is a BGP line, only the BGP line is revealed (up to 2 IPs are revealed). If there is no BGP line, a single line is returned (up to 6 IPs are revealed).

China Telecom line: A China Telecom line gets allocation priority. If there is no China Telecom line , no allocation is made (up to 2 IPs are revealed).

China Unicom line: A China Unicom line gets allocation priority. If there is no China Unicom line, no allocation is made (up to 2 IPs are revealed).

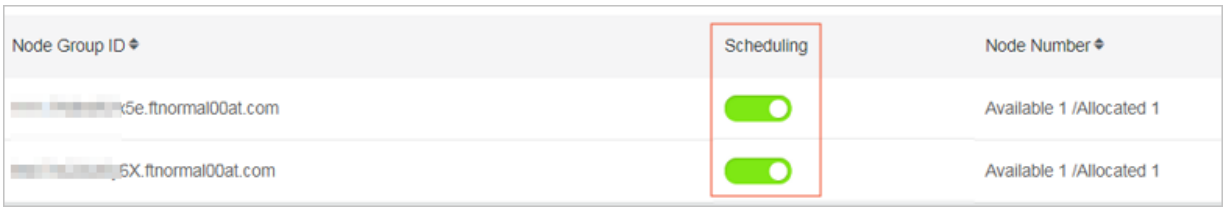
China Mobile line: A China Mobile line gets allocation priority. If there is no China Mobile line, no allocation is made (up to 2 IPs are revealed).

Note:

- After some nodes are routed to black holes: Automatically remove the nodes in black holes and automatically adjust DNS resolution according to the preceding logic.
- After all nodes are routed to black holes: The resolution state is equivalent to that when all nodes survive.

How do you verify the effectiveness of smart resolution?

You can use *https: // www. 17ce.com/* to verify the smart resolution result of CNAME.

Is smart resolution automatically enabled for old users?

Only the node groups created after March 21 have the smart resolution function automatically enabled. The older groups must undergo events, such as enabling scheduling, disabling scheduling, adding nodes, deleting nodes, and black hole attacks, to trigger their own DNS resolution logic.