

# **Alibaba Cloud Anti-DDoS**

Anti-DDoS Basic Service

Issue: 20200624

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



## Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click <b>Settings &gt; Network &gt; Set network type</b> .
<b>Bold</b>	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	Courier font is used for commands.	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
{ } or {a b}	This format is used for a required value, where only one item can be selected.	switch {active stand}



# Contents

---

<b>Legal disclaimer.....</b>	<b>I</b>
<b>Document conventions.....</b>	<b>I</b>
<b>1 Release notes.....</b>	<b>1</b>
<b>2 Quick Start.....</b>	<b>3</b>
2.1 Quick Start.....	3
<b>3 User Guide.....</b>	<b>6</b>
3.1 Configure a cleaning threshold.....	6
3.2 Cancel traffic cleaning.....	7
3.3 View the duration of a black hole.....	10
3.4 Configure DDoS Protection notification settings.....	11
3.5 View the time when a black hole is enabled for an instance and the reason for enabling the black hole.....	12
3.6 Connect to a server whose IP address is thrown into the black hole.....	13
3.7 Black hole triggering thresholds in Anti-DDoS Basic.....	14
3.8 Anti-DDoS Basic black hole threshold for web hosting.....	17
3.9 Cloud service specification and cleaning trigger value.....	18
3.10 ECS stress test guide.....	18
3.11 Avoid Anti-DDoS Basic false positives by using a whitelist.....	19
3.12 Assets.....	20
<b>4 Agreements.....</b>	<b>21</b>
4.1 Security Credibility.....	21



# 1 Release notes

---

This topic describes new features. It also includes related document updates for Anti-DDoS Basic.

## December 2019

Feature	Description	Release date	Documentation
Console	<p>A new release of the console is available, including the following updates:</p> <ul style="list-style-type: none"><li>• In the left-side navigation pane, <b>Anti-DDoS Basic</b> is changed to <b>Anti-DDoS Services</b>.</li><li>• In the left-side navigation pane, the <b>Basic Protection &gt; Instances</b> path is changed to the <b>Assets</b> node. On the Assets page, the content of <b>DDoS Attack Protection Information</b> is updated.</li><li>• In the left-side navigation pane, the following nodes are added.<ul style="list-style-type: none"><li>- <b>Anti-DDoS Services &gt; Anti-DDoS Pro</b>: directs you to the Anti-DDoS Pro console.</li><li>- <b>Anti-DDoS Services &gt; Anti-DDoS Services Premium</b>: directs you to the Anti-DDoS Premium console.</li><li>- <b>Industry-specific &gt; GameShield</b>: directs you to the GameShield console.</li><li>- <b>How to choose</b>: directs you to a topic named <b>Select an Anti-DDoS service based on the protection scenario</b>.</li></ul></li></ul>	December 18, 2019	<a href="#">Quick Start</a>

Feature	Description	Release date	Documentation
Assets	<p>The previous <b>Basic Protection &gt; Instances</b> page is changed to the <b>Assets</b> page.</p> <p>The Assets page includes the protection status of activated assets under an Alibaba Cloud account. The page provides a quick overview of security risks for your assets from distributed denial of service (DDoS) attacks. On the page, you can also improve the protection capacity for a specified asset . Available assets include Elastic Compute Service (ECS), Server Load Balancer (SLB), and Elastic IP Address (EIP) instances.</p>	December 18, 2019	<a href="#">Assets</a>
Elastic protection	<p>The previous preset protection threshold is changed to an elastic protection threshold. The console no longer shows a score in the <b>Security Credibility</b> field.</p> <p>With elastic protection, Anti-DDoS Basic allows you to assign your asset extra protection capacity over the original basic protection capacity that is provided free of charge. The amount of extra protection capacity Anti-DDoS Basic assigns for an asset changes based on several factors. The factors include the number of resources that an anti-DDoS cluster consumes, available resources, historical attacks that an asset encounters, and security credits for an account.</p>	December 18, 2019	<a href="#">#unique_6</a>

## 2 Quick Start

---

### 2.1 Quick Start

This topic describes how to view protection settings and details for each resource under an Alibaba Cloud account in the Anti-DDoS Basic console. It also provides an overview of protection against DDoS attacks. You can change protection configurations based on your business requirements.

#### Context

Anti-DDoS Basic is enabled by default. It provides a protection capacity of up to 5 Gbit/s for Elastic Compute Service (ECS), Server Load Balancer (SLB), and Elastic IP Address (EIP) instances. The protection against DDoS attacks for the preceding assets that belong to an Alibaba Cloud account is provided free-of-charge.

You must take note of the following items when using Anti-DDoS Basic:

- You can configure an appropriate cleaning threshold based on your business requirements. The throughput of DDoS attacks that an asset encounters may exceed the specified value of a cleaning threshold. In such cases, Anti-DDoS Basic starts cleaning attack traffic to ensure business continuity.
- You must take note of the protection capacity that is used for an instance to protect against DDoS attacks. If the bandwidth of a DDoS attack is no less than the specified cleaning threshold, Anti-DDoS Basic provides traffic cleaning free of charge. The default black hole triggering threshold for an asset changes based on the region that hosts the asset. For more information, see [Default black hole triggering thresholds for Anti-DDoS Basic](#).
- Activate Anti-DDoS Pro based on your business requirements. If the bandwidth of a DDoS attack on an asset exceeds the default black hole triggering threshold for the asset, requests to the asset are forwarded to a [black hole](#). We recommend that you use Anti-DDoS Pro to improve protection capacity. For more information about Anti-DDoS Pro, see [What is Anti-DDoS Pro?](#).

#### Procedure

1. Log on to the [Alibaba Cloud Anti-DDoS Basic console](#).
2. On the top of the **Assets** page, select a region.

3. On the **Assets** page, view **DDoS Attack Protection Information**. The DDoS Attack Protection Information section provides the following links to specific topics.

- Click **Default Basic Protection Threshold** to view default black hole triggering thresholds for different assets that reside in each region.
- Click **Blackholing** to view Alibaba Cloud black hole policies.
- Click **Anti-DDoS Pro** to go to the **Instance List** page of the Anti-DDoS Pro console. You can activate Anti-DDoS Pro based on your business requirements.

**Assets**

**DDoS Attack Protection Information**

When the IP suffer DDoS attack bandwidth than cleaning threshold, alibaba will begin to attack the flow of clean as possible and to protect your business available.

If the attack bandwidth is below the basic protection threshold, you can clean the attack traffic for free. The [Default Basic Protection Threshold](#) varies according to the IP address location.

When you attack bandwidth beyond the elastic protection threshold, Alibaba will attack IP into [Blackholing](#) (Blackholing Disabled At: 4320 Minute(s)) state. We recommend that you use [Anti-DDoS Pro](#) to enhance attack protection. [Learn More](#)

For more information, see [Assets](#).

4. You can change the value of a cleaning threshold based on your business requirements.

a) On the **Assets** page, select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.

- **ECS**: includes a list of IP addresses for ECS instances.
- **SLB**: includes a list of IP addresses for SLB instances.
- **EIP (including NAT)**: includes a list of IP addresses for EIP and NAT instances.



**Note:**

ECS or SLB instances that have Elastic IP addresses associated are sorted into EIP instances.

- **Others:** includes a list of IP addresses for instances that are hosted by other service providers.
- b) In a list of instances, find the target instance, and click the **IP** address of the instance.
- If excessive instances exist, we recommend that you search for the target instance by using the **instance ID**, **instance name**, or **instance IP** as the search condition.

ECS SLB EIP (including NAT) Others			
Instance ID ▾ Please enter 🔍			
<input type="checkbox"/>	IP/Remark	Status 📶	Protection Capacity
<input type="checkbox"/>	139. 36 iZ 7Z	● Normal	2.200G
		Cleaning Trigger Value	
		BPS 1000M   PPS 300.00K	

Open the **Instance Details** page. The Instance Details page shows the peak daily traffic, number of daily data packets, and a list of DDoS attacks for the last seven days.

Instance Details

IP/Remark: 139. 36 iZ 7Z Cleaning Trigger Value: BPS 1000M | PPS: 300K

Cleaning Settings

Traffic Packets

Today 3Day(s) 7Day(s)

- c) On the **Instance Details** page, click **Cleaning Settings**, and select **Manual Setting** or **Default** in the Cleaning Threshold field.

Cleaning Settings

Cleaning threshold: Default Manual setting

Threshold: BPS 1000M | PPS 300000K

The system dynamically adjusts the cleaning threshold value based on ECS's traffic load.

For more information, see [Configure a cleaning threshold](#).

## 3 User Guide

### 3.1 Configure a cleaning threshold

This topic describes how to configure a cleaning threshold in the Anti-DDoS Basic console.

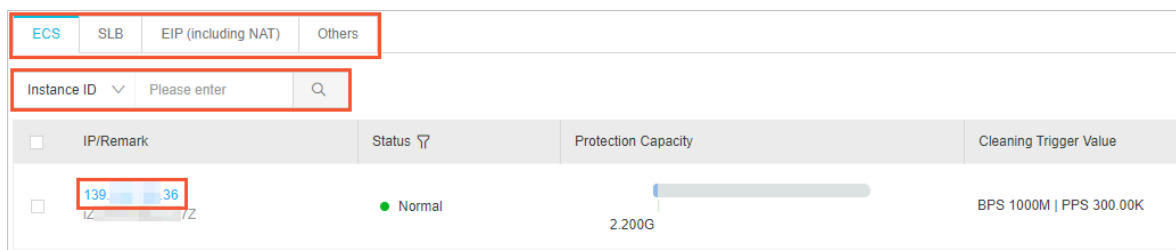
#### Context

Anti-DDoS Basic is applied to protect Alibaba Cloud assets by default. The service is provided free of charge after each asset is activated. The assets include Elastic Compute Service, Server Load Balancer, and Elastic IP Address instances. The maximum throughput of DDoS attacks that an asset encounters may exceed the specified cleaning threshold. In such cases, Anti-DDoS cleans attack traffic and performs other counter measures to ensure business continuity.

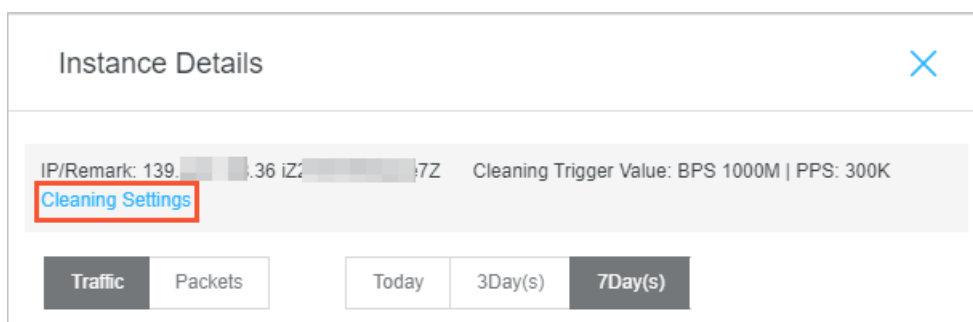
#### Procedure

1. Log on to the [Alibaba Cloud Anti-DDoS Basic console](#).
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
4. In a list of instances, find the target instance and click the **IP** address of the instance.

If excessive instances exist, we recommend that you search for the target instance by using the **instance ID**, **instance name**, or **instance IP** as the search condition.



5. In the **Instances Details** dialog box, click **Cleaning Settings**.

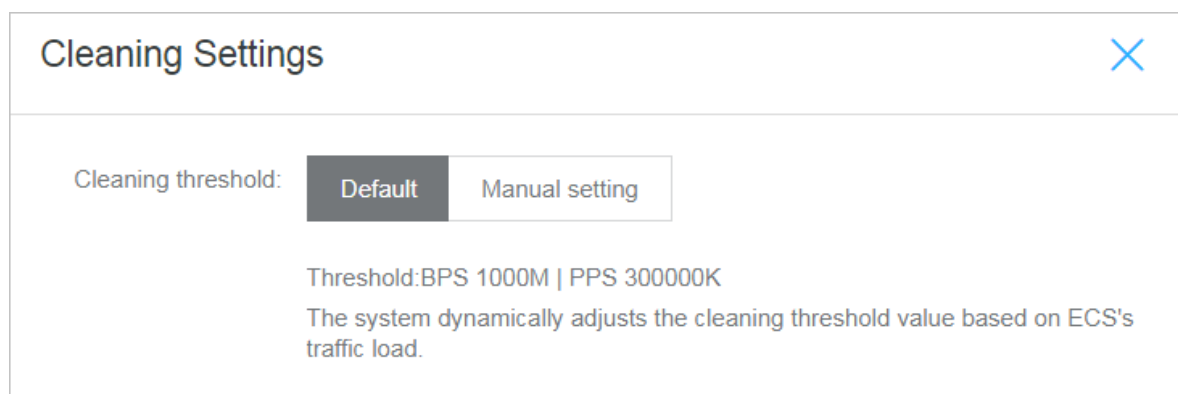


6. In the **Cleaning Settings** dialog box, select **Default** or **Manual Setting** in the Cleaning Threshold field.

- **Default:** Anti-DDoS Basic dynamically adjusts the cleaning threshold based on the traffic load of an asset.
- **Manual setting:** You can select a specific threshold that includes two values. One indicates the minimum throughput and the other indicates the minimum packets per second (PPS).

Recommendations:

- Configure a cleaning threshold of which the value is slightly greater than the maximum bandwidth for actual incoming requests. If the specified value of a threshold is greater than expected, the effect of protection is compromised. If the specified value of a threshold is less than expected, legitimate access may be affected when traffic cleaning is triggered.
- If legitimate access is affected, we recommend that you increase the value of the cleaning threshold.
- During large promotions or activities for a website, we recommend that you increase the specified value of a cleaning threshold.



## Result

The cleaning threshold is configured. When the maximum throughput of incoming requests that a website can serve reaches the specified cleaning threshold, Anti-DDoS Basic launches traffic cleaning.

## 3.2 Cancel traffic cleaning

Anti-DDoS Basic provides default protection against distributed denial of service (DDoS) attacks for Alibaba Cloud instances. Anti-DDoS Basic automatically detects attacks and

cleans excessively high traffic for instances that experience flood attacks. You can cancel traffic cleaning for IP-bound assets that are in an abnormal state such as cleaning.

## Context

Cleaning refers to real-time monitoring that Anti-DDoS Basic performs on incoming data traffic of instances. Based on the monitoring result, Anti-DDoS identifies suspicious traffic such as DDoS attacks. On the premises of business continuity, Anti-DDoS Basic cleans excessively high traffic and redirects suspicious traffic from original routes to a cleaning module. Then, the cleaning module identifies and strips malicious content from suspicious traffic. After the filtering process, legitimate traffic is returned to the original routes and then forwarded to target systems.



### Note:

You can cancel cleaning a maximum of three times a day for each account.

## Procedure

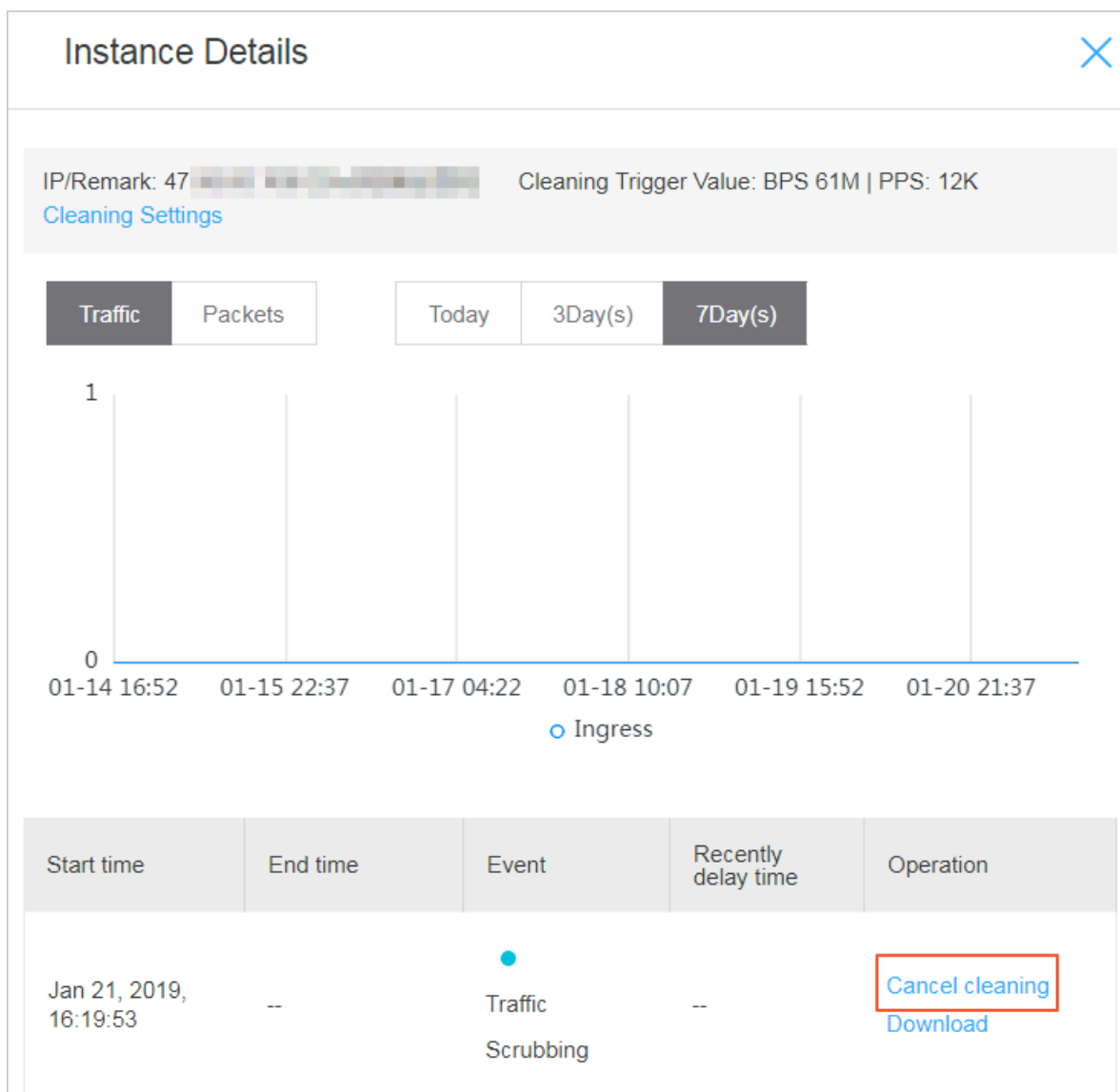
1. Log on to the [Alibaba Cloud Anti-DDoS Basic console](#).
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
4. In a list of instances, find an instance of which the **Status** is **Cleaning**, and click the **IP** of the instance.
5. On the **Instance Details** page, find an entry of which the **Event** is **Traffic Scrubbing** and the **End Time** is empty and click **Cancel cleaning** in the Operation column.



### Note:



If no traffic scrubbing event exists, the **cancel cleaning** operation is unavailable.



## Result

The traffic cleaning operation is canceled.

## What's next

After you cancel traffic cleaning, we recommend that you increase cleaning thresholds in specific scenarios, such as scenarios with a sharp increase in traffic during large activities or promotions. This action avoids triggering traffic cleaning again. For more information, see [Configure a cleaning threshold](#).



### Note:

The maximum cleaning threshold for each instance of a cloud service changes based on the instance type. If the maximum cleaning threshold that you can configure cannot meet

your requirements, we recommend that you upgrade the specified instance type of the cloud service.

### 3.3 View the duration of a black hole

A server may encounter a distributed denial of service (DDoS) attack. After a black hole is triggered due to the attack, access from clients to the public IP address of the server is blocked for a period of time. The access is unblocked after the duration of the black hole expires. The default black hole duration for an asset changes based on the region where the asset resides. You can view the duration of a black hole for an asset in the Anti-DDoS Basic console.

#### Context

The default duration of a black hole is 2.5 hours and you cannot disable the black hole during the period. In practical scenarios, the black hole duration depends on the attack situation and may range from 30 minutes to 24 hours. The duration of a black hole changes based on the following factors:

- The duration of attacks. If attacks continue, the black hole duration is extended.
- The frequency of attacks. If an asset experiences attacks for the first time, the black hole duration automatically decreases. Otherwise, assets that experience frequent attacks have a high probability to encounter continuous attacks. In such cases, the black hole duration is automatically extended.

You can refer to the Anti-DDoS Pro console for more details about the black hole triggering threshold and black hole duration.



#### Note:

- If excessive breaches of the black hole threshold occur on an asset, Alibaba Cloud reserves the right to extend the black hole duration and decrease the black hole threshold for the asset.
- Blackhole filtering is a service that Internet service providers (ISPs) provide for Alibaba Cloud. Specific black hole triggering thresholds are predefined by ISPs. In most cases, the duration of a black hole is greater than or equal to 30 minutes. The duration of each black hole for an account changes based on the security credits of the account.

For more information about black hole policies that Alibaba Cloud provides, see [#unique\\_9](#).

#### Procedure

1. Log on to the [Alibaba Cloud Anti-DDoS Basic console](#).
2. On the top of the **Assets** page, select a region.
3. On the top of the Assets page, view **DDoS Attack Protection Information**.

The duration after **Blackholing Disabled At** in the DDoS Attack Protection Information section refers to the black hole duration for an asset in the specified region.

Assets

DDoS Attack Protection Information

When the IP suffer DDoS attack bandwidth than cleaning threshold, alibaba will begin to attack the flow of clean as possible and to protect your business available.

If the attack bandwidth is below the basic protection threshold, you can clean the attack traffic for free. The [Default Basic Protection Threshold](#) varies according to the IP address location.

When you attack bandwidth beyond the elastic protection threshold, Alibaba will attack IP into [Blackholing](#) state. We recommend that you use [Anti-DDoS Pro](#) to enhance attack protection. [Learn More](#)

Blackholing Disabled At: 150 Minute(s)

## 3.4 Configure DDoS Protection notification settings

Alibaba Cloud provides DDoS Protection notifications. When a server under your account suffers DDoS attacks, triggers traffic scrubbing or the blackhole mechanism, the system sends notifications by specified methods to specified receivers.

### Manage message recipients

To configure the notification methods (Internal Messages, Email, and Text message) and recipients for Security Notice, follow these steps:

1. Log on to the [Message Center console](#).
2. Click **Message Settings** and locate to **Security Notice**.

Message Center	Product overdue payment, suspension, and imminent release notifications ⓘ	Account Contact	<a href="#">Modify</a>	✓
Internal Messages	Product release notifications ⓘ	Account Contact	<a href="#">Modify</a>	✓
All Messages	Product renewal or bill settlement notifications ⓘ	Account Contact	<a href="#">Modify</a>	✓
Unread Messages	Product or system upgrade and product configuration change notifications ⓘ	Account Contact	<a href="#">Modify</a>	✓
Read Messages	New product function launch and function removal notifications ⓘ	Account Contact	<a href="#">Modify</a>	✓
Message Settings	Security notice ⓘ	Account Contact	<a href="#">Modify</a>	✓

3. Click **Modify** and select the message recipient.



**Note:**

To add a new message recipient, click **Add Receiver**.

Modify Contact

Reminder: You can go to Manage Contacts to add or modify the contacts.  
A message will be sent to verify the email address.

Message Type: Product Message - Security notice

	Name	Email	Occupation	Action
<input checked="" type="checkbox"/>	Account Contact	ali****@service.aliyun.com		

+ Add Receiver

\*Note: At least 1 receivers are needed.

Save

Cancel

### 3.5 View the time when a black hole is enabled for an instance and the reason for enabling the black hole

In the Anti-DDoS Pro console, you can view a list of black hole events for all assets that belong to an account. For example, you can view the time point when a black hole is enabled for an asset and a list of IP addresses from which attacks originate.

#### Context

The public IP address of an Elastic Compute Service (ECS) or Server Load Balancer (SLB) instance may experience a large number of distributed denial of service (DDoS) attacks. If the throughput of these attacks exceeds the predefined black hole triggering threshold, all traffic to the public IP address is routed to a black hole. Your businesses are no longer accessible by clients because all exterior traffic is dropped.

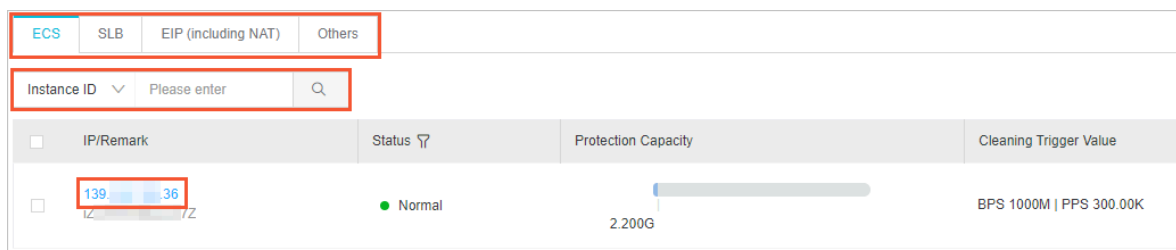
The black hole triggering threshold for an instance changes based on the region where the instance resides. For more information about black holes, see [#unique\\_9](#).

#### Procedure

1. Log on to the [Alibaba Cloud Anti-DDoS Basic console](#).
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.

4. In a list of instances, find the target instance and click the **IP** address of the instance.

If excessive instances exist, we recommend that you search for the target instance by using the **instance ID**, **instance name**, or **instance IP** as the search condition.



5. On the **Instance Details** page, view a list of historical black hole events where the **Event** is **Black Hole** and view the peak traffic for each attack.

The **Start time** and **End time** of a black hole event are displayed.

**Note:**

If no black hole or scrubbing event for an asset exists, no result is displayed in the event list.

6. Optional: In the Operation column of the target event, click **Download**. You can use the downloaded packet file for the attack event as evidence of criminal activity. You can send the evidence to the Internet Crime Reporting Center.

## 3.6 Connect to a server whose IP address is thrown into the black hole

If your server suffers from a heavy traffic attack and its IP address is thrown into the black hole, then all external traffic to the server is discarded. However, you can still access this server from Alibaba Cloud services within the same region as that of this server.

**Note:**

During the black hole period, external access requests sent to this server are blocked.

You can use an Alibaba Cloud ECS instance to connect to your server, even when its IP address is thrown into the black hole.

1. Connect to an Alibaba Cloud ECS instance that can be normally accessed and is within the same region as this server.

**Note:**

This ECS instance must be connectable to the server under black hole status. They must belong to the same VPC environment, and the connection is not blocked by any security group access control rules.

2. Use a tool or command line to connect from the ECS instance to the server under black hole status.

After successfully connecting to the server from the ECS instance, you can transfer files from the server to the ECS instance and modify the configuration files on this server.

## 3.7 Black hole triggering thresholds in Anti-DDoS Basic

The following table lists the default thresholds at which Anti-DDoS automatically triggers black holes in each region. These thresholds are measured in bit/s.



### Note:

- Anti-DDoS can automatically trigger black holes for Elastic Compute Service (ECS), Server Load Balancer (SLB), Elastic IP Address (EIP), and Web Application Firewall (WAF) instances. This feature is available for IPv4 networks in all regions and for IPv6 network only in specific regions. In the following table, a check sign (✓) in the Support IPv6 column indicates that the automatic black hold trigger feature is supported for IPv6 in the region and the thresholds are applicable to both IPv4 and IPv6. A cross sign (×) indicates that the feature is not supported for IPv6 in the region and the thresholds are applicable only to IPv4 networks.
- Practical black hole triggering thresholds for ECS, SLB, and EIP instances change based on the instance type and bandwidth that you purchase. You can refer to the **Assets** page of the Anti-DDoS Basic console for more details. For more information, see [Assets](#).
- In each region, the same threshold to trigger black holes is applied for WAF, SLB, and EIP instances.

Region	Support IPv4	Support IPv6	ECS instances with one vCPU	ECS instances with two vCPUs	ECS instances with more than four vCPUs	SLB, EIP ( includes public IP addresses of NAT gateways ), and WAF instances
China ( Hangzhou)	√	√	500 Mbit/s	1 Gbit/s	5 Gbit/s	5 Gbit/s
China (Shanghai )	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Qingdao)	√	×	500 Mbit/s	1 Gbit/s	5 Gbit/s	5 Gbit/s
China (Beijing)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China ( Zhangjiakou-Beijing Winter Olympics)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Hohhot)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Shenzhen )	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Heyuan)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Chengdu)	√	×	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Hong Kong)	√	√	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Singapore	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Australia ( Sydney)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Malaysia (Kuala Lumpur)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Indonesia ( Jakarta)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Japan (Tokyo)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Germany ( Frankfurt)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s

Region	Support IPv4	Support IPv6	ECS instances with one vCPU	ECS instances with two vCPUs	ECS instances with more than four vCPUs	SLB, EIP ( includes public IP addresses of NAT gateways ), and WAF instances
UK (London)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
US (Silicon Valley)	√	×	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
US (Virginia)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
India (Mumbai)	√	×	500 Mbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s
UAE (Dubai)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s

The default black hole duration is 2.5 hours. During this period, blackholing is enabled and cannot be disabled. The actual black hole duration changes based on the type of attack, ranging from 30 minutes to 24 hours. The black hole duration is based on the following factors:

- The duration of attacks: If attacks continue, the black hole duration is extended. The next black hole duration is set to zero and starts at the time when the last black hole duration is extended.
- The frequency of attacks: If an asset experiences attacks for the first time, the black hole duration automatically decreases. Otherwise, assets that experience frequent attacks have a high probability to encounter continuous attacks. In such cases, the black hole duration is automatically extended.



**Note:**

If excessive breaches of the black hole threshold occur on an asset, Alibaba Cloud reserves the right to extend the black hole duration and decrease the black hole threshold for the asset. You can refer to the Anti-DDoS console for more details about the black hole triggering threshold and black hole duration.



## 3.8 Anti-DDoS Basic black hole threshold for web hosting

The default black hole threshold for web hosting is as follows (unit: bps).

**Note:**

For shared web hosting, the specific black hole threshold cannot be defined as multiple web hosting may share one IP address. Additionally, the actual threshold must be lower than the default threshold value. When a shared web hosting server triggers the black hole, all the other servers that share IP address with this server becomes inaccessible. We strongly recommend that you buy ECS instance if you give utmost importance to the security.

Region	Web hosting threshold
China (Hangzhou)	5 G
China (Qingdao)	5 G
China (Shenzhen)	2 G
China (Beijing)	2 G
China (Shanghai)	2 G
Hong kong	500 M
US West	500 M
Singapore	500 M

The black hole duration is the amount of time the triggered back hole lasts, 2.5 hours by default. The actual black hole duration varies from 30 minutes to 24 hours, depending on attack intensity. Additionally, the following factors are considered:

- Attack Continuity. The black hole duration is extended, if the attack continues.
- Attack Frequency. The black hole duration is shortened automatically when the ECS instance is attacked for the first time, but can be prolonged accordingly, if under frequent attacks.

**Note:**

If an ECS instance triggers too many black holes, Alibaba Cloud Security reserves the right to extend the black hole duration and lower its threshold. You can check the actual duration and threshold information in Alibaba Cloud Anti-DDoS Basic console.

To get more powerful DDoS mitigation capacities, see [Alibaba Cloud Anti-DDoS Pro](#).

## 3.9 Cloud service specification and cleaning trigger value

Alibaba Cloud provides basic DDoS protection capabilities to help mitigate DDoS attacks on cloud products open to the public network. When the network traffic of the public IP address of the cloud product exceeds the specified cleaning threshold, the traffic to this IP is automatically scrubbed to protect your normal service from DDoS attacks.

For more information about traffic scrubbing, see [Traffic scrubbing, black hole, and threshold value](#).

The maximum cleaning threshold supported for each Alibaba cloud service depends on the specifications of the instance. When you create or change an ECS or SLB instance, the system automatically adjusts the maximum cleaning threshold based on the current instance specification.

**Note:**

The actual black hole threshold for each instance IP is calculated based on factors such as maximum cleaning threshold and security credibility score.

- For the specific calculation method of the maximum cleaning threshold of ECS instances, see [Basic DDoS Protection for ECS](#).
- For the specific calculation method of the maximum cleaning threshold of SLB instances, see [Basic DDoS Protection for SLB](#).

## 3.10 ECS stress test guide

Alibaba Cloud Security Anti-DDoS Basic provides defense against DDoS attacks. By default, when the public traffic exceeds 180 MB per second, 30,000 messages per second, or 480 HTTP requests per second on an ECS server, Anti-DDoS Basic automatically starts traffic scrubbing to protect the ECS server.

Therefore, before you start the stress testing on an ECS server, you have to adjust the cleaning trigger value to an appropriate value in the [Alibaba Cloud Anti-DDoS Basic console](#). For more information, view [Set the cleaning trigger value](#).

**Note:**

We recommend that you do not set the increasing pace per minute to exceed 100 times during the stress test.

### 3.11 Avoid Anti-DDoS Basic false positives by using a whitelist

In some situations, you may find that some normal traffic is blocked by Anti-DDoS Basic (such as normal website service access).

#### Context

For example, in an NAT network environment (hosts in the LAN share an Internet IP address for Internet access), some hosts in the LAN infected by a virus or suffering intrusion may attack an ECS server. In this situation, once Alibaba Cloud Security acknowledges the attacks, it blocks the shared Internet IP address of the NAT, resulting to an access failure.

However, you can set a whitelist in the Alibaba Cloud Security Control platform to avoid such false positives.

#### Procedure

1. Log on to the [Alibaba Cloud Security Control console](#).

**Note:**

You can also hover your mouse on the account icon in the upper-right corner of Alibaba Cloud console and click **Security Control** to open it.

2. Go to **Whitelist > Access Whitelist**, click **Add**.
3. Select the Object Type, and enter the Source IP (not the IP belongs to your current Alibaba Cloud account). Then, select object IPs of your current account from the list on the left side (for example, select a public IP of your ECS instance), click the right arrow button to add the selected IPs to the list on the right side, and click **OK**. Thus, the specified source IP is added to the access whitelist of the selected object IPs, and all accesses from the source IP to the object IPs are not restricted by Alibaba Cloud Security Control platform.

**Note:**

To allow accesses from all IPs to the object IP, enter 0.0.0.0 in the **Source IP** field.

After setting the whitelist, all accesses to the target host asset from the source IP in the access whitelist are not restricted by any Alibaba Cloud security controls, even if the access may be risky. Therefore, set the access whitelist carefully.

**Note:**

After the source IP is added to the access whitelist, it takes effect within 10 minutes.

## 3.12 Assets

The Assets page of the Anti-DDoS Basic console shows a list of assets that belong to an Alibaba Cloud account and the protection status of each asset. These assets include ECS, SLB, and EIP instances. The information allows you to obtain an overview of security risks from distributed denial of service (DDoS) attacks for your assets. You can also improve protection for an asset.

### Procedure

1. Log on to the [Alibaba Cloud Anti-DDoS Basic console](#).
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
4. In a list of assets, view the protection status of each asset.

The **Assets** page lists all assets in a region and provides further details about protection against DDoS attacks for each asset. The details include the **status**, **protection capacity**, and **cleaning trigger value**.

- **Status** indicates the security state of an instance. Available states include **Normal**, **Cleaning**, and **Black Hole Activated**.
  - If an instance is in the Cleaning state, you can cancel the cleaning operation. For more information, see [Cancel traffic cleaning](#).
  - If an instance is in the Black Hole Activated state, you can view black hole events. For more information, see [View the time when a black hole is enabled for an instance and the reason for enabling the black hole](#).
- **Protection capacity** indicates the capability of protection against DDoS attacks for an instance. The capacity refers to the maximum throughput of DDoS attacks against which defense can be provided. If the bandwidth that DDoS attacks consume exceeds the protection capacity of an instance, a black hole is triggered and all packets that are routed to the instance is dropped. For more information about how to improve protection capacity for an instance, see Step 5.
- **Cleaning Trigger Value** indicates the minimum throughput that must be reached before traffic cleaning is triggered. The throughput is measured in Mbit/s and packets per second (PPS). For more information, see [Configure a cleaning threshold](#).

5. Improve the protection capacity for a specific asset.

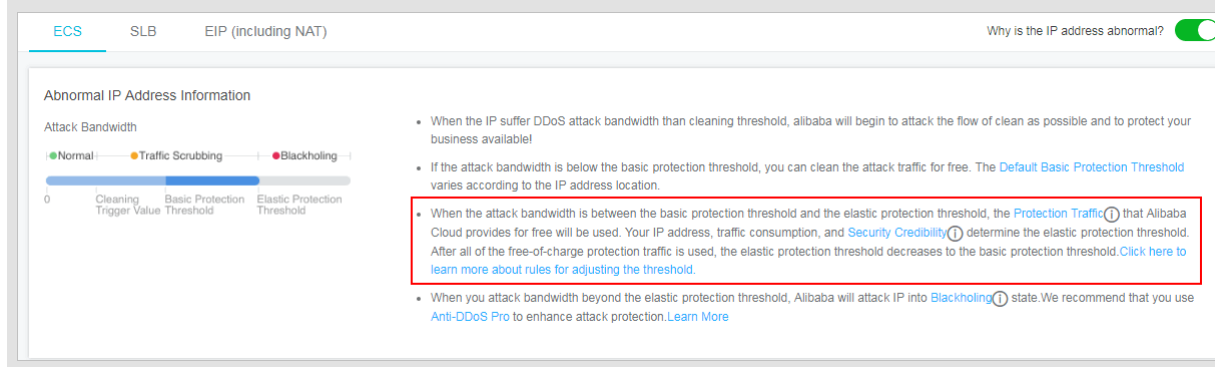
## 4 Agreements

### 4.1 Security Credibility



#### Note:

All Alibaba Cloud users became members of the Security Credibility program by default on July 31, 2018. You can log on to the [Anti-DDoS Basic console](#) to view the details.



#### I. Program introduction

Security Credibility is a program that Alibaba Cloud has developed to improve your user experience during security protection and provide higher security capabilities. Alibaba Cloud provides users in this program with flexible anti-DDoS protection capabilities based on the security credibility of the user.

Currently, you can join Security Credibility for free.

#### II. Program benefits

- **A higher black hole threshold.** The black hole threshold is adjusted flexibly based on your credit score. For most users, the adjusted black hole threshold is no smaller than the default threshold. This lowers the probability that your servers fall into a black hole.
- **Open credibility evaluation criteria.** The members of this program can improve their credibility based on the credibility evaluation criteria to obtain more protection capabilities.

#### III. Security protection mechanism

- The anti-DDoS protection capability of a user is adjusted based on the security credit score of the user. Most users can obtain additional anti-DDoS protection capability for free.

- The security credit score is the basis for calculating the black hole threshold. If the attack traffic volume is below this threshold, Alibaba Cloud protects your ECS and SLB instances against the attacks at zero cost. If your servers fall into black holes frequently, the black hole threshold is lowered to the default value. If the attack traffic volume exceeds the current threshold, your servers fall into a black hole to block all IP addresses.
- Attacks affect the next credibility evaluation.
- The security protection capabilities that you can obtain from the program are provided by a resource pool shared by all members of the program. In standard cases, Alibaba Cloud provides you with security protection capabilities based on your credit score. However, if the members of the program encounter attacks or other malicious events together and the resources in the shared resource pool run out, your security protection capabilities may be reduced.
- For users with frequent black holing, Alibaba Cloud reserves the right to increase the black hole duration and lower the black hole threshold. You can go to the console to view the black hole threshold and duration.
- If the attack traffic volume exceeds the traffic covered by the additional protection capabilities provided by the program, you must purchase Anti-DDoS Pro to obtain higher protection capabilities. Otherwise, services running on your ECS and SLB instances may be interrupted due to DDoS attacks.
- Make sure to keep your security credit score and related information confidential.

#### IV. Terms of service

1 You understand and acknowledge that you shall not use the security protection capabilities that you obtain as a member of the Security Credibility program to perform any of the following activities:

1.1 Provide either paid or free security protection services to others.

1.2 Illegal activities or activities that do not comply with the service purposes or procedures according to the information published on [www.alibabacloud.com](http://www.alibabacloud.com) or the assessment of Alibaba Cloud.

1.3 Upload, download, or disseminate any of the following information, or help others in such activities:

1.3.1 Political propaganda and/or news information in violation of China's regulations;

1.3.2 Information related to China's state secrets and/or state security;

- 1.3.3 Information related to superstition, obscenity, or solicitation to commit a crime;
- 1.3.4 Information related to illegal Internet publishing activities, such as lottery prizes, gambling games, private servers, and plug-ins;
- 1.3.5 Information that violates China's national policies, or ethnic or religious policies.
- 1.3.6 Information that adversely impacts Internet security.
- 1.3.7 Information about activities that infringe on the legitimate interest of others and/or other activities that disrupt social order, threaten public security, or violate public morals.
- 1.3.8 Other content in violation of laws, regulations, departmental rules, or China's national policies.
- 1.4 You shall not modify, translate, edit, lease, sublicense, transmit, or transfer over networks any software or services provided by Alibaba Cloud, or obtain the source code of the software provided by Alibaba Cloud through reverse engineering, decompilation, or other methods;
- 1.5 You shall not conduct any behavior that undermines or attempts to undermine network security, including but not limited to phishing, hacking, network fraud, suspected involvement in the spreading of viruses/trojans/malicious code to websites or cyberspace , and suspected involvement in attacks on other websites and servers by using virtual servers, such as scanning, sniffing, ARP spoofing, and DDoS;
- 1.6 You shall not change or attempt to change the system configurations provided by Alibaba Cloud or undermine network security.
- 1.7 You shall not use the services provided by Alibaba Cloud to conduct any activities that impair the legitimate interests of Alibaba Cloud, Alibaba Cloud affiliated companies or any company or website within the Alibaba Group, including but not limited to Alibaba, Taobao , Alipay, Alimama and Ant Financial (hereinafter collectively referred to as Alibaba Group). The behaviors that impair the legitimate interests of Alibaba Group and websites include but are not limited to violations of any agreement or terms, management norms, trading rules, or other norms published by Alibaba Group, and behaviors that damage or attempt to damage the fair-trade environment or normal trade order of Alibaba Group.</cf>
- 1.8 You shall not conduct any other activities in violation of laws, regulations, or the terms of Security Credibility.
- 1.9 You understand that Alibaba Cloud agrees that you can join this program on the premise of your commitment to obey the preceding terms. If you violate any of the

preceding terms, Alibaba Cloud reserves the right to stop providing you the services or capabilities related to this program and remove you from this program with prior notice.

2 You understand and agree that Alibaba Cloud has the right to terminate this program at any time based on Alibaba Cloud business plans, the program operations status, or other factors, without being liable to the related consequences. Alibaba Cloud will inform you of the program termination in advance. After the program is terminated, all services or capabilities that you obtain from this program will be disabled.

3 You understand and agree that you have read the security protection mechanism and the terms of Security Credibility and understand the results of joining this program. You have decided to join this program of your own free will, and shall be liable for the corresponding results.

4 Both Alibaba Cloud and you shall keep your decision about whether to join this program confidential, unless the information has become public, or Alibaba Cloud has to reveal the information as otherwise appointed with you, as required by laws and regulations, or as demanded, ordered, or executed by related authorities. You shall keep confidential your security credit score, the corresponding black hole threshold, and related credibility information. If this information is leaked, attackers may launch targeted attacks on your system.

**5 Alibaba Cloud may optimize or change the security protection mechanism of this program periodically or at random times. Alibaba Cloud will inform you of the changes in advance, and then provide you with the latest versions of services or provide you with services or capabilities based on the latest mechanism. If you do not agree to use the latest mechanism, you can apply to exit the program and terminate the use of services provided by Alibaba Cloud.**

**6 You understand and agree that the security protection capabilities that you can obtain from the program are provided by a resource pool shared by all members of the program. In standard cases, Alibaba Cloud provides you with security protection capabilities based on your credit score. However, if the members of the program encounter attacks or other malicious events together and the resources in the shared resource pool run out, your security protection capabilities may be reduced. The adjusted capabilities will not be lower than the default protection capabilities.**

**7 Disclaimers and limitation of liability: The security protection that Alibaba Cloud provides for you, a member of the program, is a technical measure. You understand**



**and agree that this technical measure taken by Alibaba Cloud based on the program is regarded as flawless security protection. If Alibaba Cloud does not deliberately undermine your system security or make mistakes in the program, Alibaba Cloud shall not be liable for the protection results.**

**8 If your websites encounter viruses, intrusions, attacks (including but not limited to DDoS attacks), or other activities that threaten the network security, and these activities are not covered by this program, the websites or website services may become unavailable to users for a certain period of time. This situation will be hereinafter referred to as service unavailability. You understand and agree that the preceding service unavailability does not indicate breach of the contract by Alibaba Cloud. If the service unavailability undermines the interests of Alibaba Cloud or adversely impacts the communications between Alibaba Cloud and the Internet, between Alibaba Cloud and specific networks or servers, and between Alibaba Cloud servers, Alibaba Cloud has the right to pause or terminate providing security protection services to you based on the Security Credibility program mechanism, without being liable to the results. Alibaba Cloud will inform you of the suspension or termination of protection beforehand.**

9 The related rules, norms, and procedures that have been published on [www.aliyun.com](http://www.aliyun.com) constitute a part of the terms of services herein. Alibaba Cloud has the right to modify these rules, norms, or procedures at any time, and require you to comply with the latest rules, norms, and procedures.