ALIBABA CLOUD

Alibaba Cloud

Anti-DDoS

Pricing

Document Version: 20200930

Alibaba Cloud

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

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

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

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

Table of Contents

1.Billing methods of Anti-DDoS Origin

Anti-DDoS Origin is offered in two editions: Anti-DDoS Origin Basic and Anti-DDoS Origin Enterprise. Anti-DDoS Origin Basic provides a protection capability of up to 5 Gbit/s for the Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, elastic IP addresses (EIPs), and Web Application Firewall (WAF) instances under your Alibaba Cloud account. It is enabled by default and free of charge. Anti-DDoS Origin Enterprise provides unlimited protection against DDoS attacks for all your assets. It is billed on a yearly subscription basis. Protection is provided after you purchase an Anti-DDoS Origin Enterprise instance.

Instance specifications of Anti-DDoS Origin Enterprise

By default, Anti-DDoS Origin Enterprise provides shared and unlimited protection. Unlimited protection provides defense against DDoS attacks. The unlimited protection capability is based on the total number of available resources and strengthens with the increase of the overall network capability of Alibaba Cloud. The increased protection capability is provided free of charge.

Anti-DDoS Origin Enterprise supports the following subscription durations: one year, two years, and three years. The unit price of a yearly subscription Anti-DDoS Origin Enterprise instance varies based on the specific business scale and the number of IP addresses that you choose. Before you use Anti-DDoS Origin Enterprise, you must select instance specifications based on your business scale and complete the payment.

- **Business Scale**: specifies the scale of your business that you want to protect. The business scale is measured in bit/s based on the 95th percentile per month. Valid values: 100 Mbit/s, 300 Mbit/s, 500 Mbit/s, 800 Mbit/s, 1 Gbit/s, 1.5 Gbit/s, 2 Gbit/s, 2.5 Gbit/s, and 3 Gbit/s. For more information about how to determine your business scale, see Business scale estimation.
- **IP Addresses**: specifies the number of IP addresses that you want to protect. The default value is 100. Valid values range from 100 to 255.

Billing methods of Anti-DDoS Origin Enterprise

If you want to protect 100 IP addresses in a single region, the subscription fee for an Anti-DDoS Origin Enterprise instance in the region is calculated by using the following formula: Monthly unit price for the specific business scale × 12 (months) × Subscription duration (years)

If you want to protect more than 100 IP addresses in a single region, the subscription fee for an Anti-DDoS Origin Enterprise instance in the region is calculated by using the following formula: [Monthly unit price for the specific business scale + (Number of IP addresses that you want to protect - 100) × USD 30 per month] × 12 (months) × Subscription duration (years).

The following table lists the monthly unit prices for different business scales.

> **Note** By default, an Anti-DDoS Origin Enterprise instance provides protection for 100 IP addresses in a single region. If you want to protect more than 100 IP addresses, the unit price will be increased by USD 30 per month for each added IP address. If you want to protect IP addresses across regions, you must create multiple instances or submit a ticket to create an Anti-DDoS Origin Enterprise instance with custom specifications.

Prices that are listed in the following table may be different from those on the Anti-DDoS Origin buy page. The prices on the Anti-DDoS Origin buy page prevail.

Note The monthly price unit for an Anti-DDoS Origin Enterprise instance remains unchanged no matter whether IPv4 or IPv6 is used.

Business scale	Unit price (USD per month)
100 Mbit/s	7,016
300 Mbit/s	9,025
500 Mbit/s	11,034
800 Mbit/s	14,047
1 Gbit/s	16,056
1.5 Gbit/s	21,079
2 Gbit/s	26,101
2.5 Gbit/s	31,124
3 Gbit/s	36,146

Note The minimum business scale is 100 Mbit/s, which is also the default value. The maximum business scale is 3 Gbit/s. If the business scale that you specify exceeds 3 Gbit/s, we recommend that you submit a ticket to create an Anti-DDoS Origin Enterprise instance with custom specifications.

Business scale estimation

You can estimate a business scale or clean bandwidth by using the following method:

Sample inbound and outbound bandwidth at five-minute intervals. Calculate the average inbound and outbound bandwidth. Use the greater average value as the bandwidth of the sample point. At the end of each month, sort all sample points in descending order, ignore the top 5% of sample points, and use the first value of the remaining 95% of sample points is as the 95th percentile bandwidth.

The following figure shows how to calculate the bandwidth for billing based on 95th percentile bandwidth within 30 days.

Assume that the actual business bandwidth exceeds the clean bandwidth of an Anti-DDoS Origin Enterprise instance that you purchase.

Anti-DDoS Origin Enterprise allows your clean bandwidth to exceed the purchased business scale for a short period of time. If the period exceeds 36 hours, unlimited protection becomes invalid. Anti-DDoS Origin Enterprise imposes no limit on your clean bandwidth but provides only basic protection.

Refunds

Anti-DDoS Origin instances do not support the 5-day money-back guarantee refund.

Contact us

You can submit a ticket or contact your service manager to create an Anti-DDoS Origin Enterprise instance with custom specifications.

2.Anti-DDoS Pro billing methods

This topic describes the billing methods of Anti-DDoS Pro.

Overview

Anti-DDoS Pro provides **basic protection** and **burstable protection** to safeguard your services that are deployed in mainland China. You are charged for these protection services based on the following billing methods:

- Basic protection: subscription billing (billed monthly)

  Before you use Anti-DDoS Pro, you must purchase an Anti-DDoS Pro instance. When you purchase an Anti-DDoS Pro instance, you must specify the specifications and the subscription period. An Anti-DDoS Pro instance provides basic protection within the subscription period.

  Assume that you have purchased a basic protection bandwidth of 30 Gbit/s for an Anti-DDoS Pro instance. If the peak bandwidth of DDoS attacks is 30 Gbit/s or lower, no additional fees are charged.

- Burstable protection: pay-as-you-go (billed daily)

  You can enable burstable protection based on your business needs. To enable burstable protection, specify a burstable protection bandwidth that is higher than the basic protection bandwidth. When the attack bandwidth is higher than the basic protection bandwidth but no higher than the burstable protection bandwidth, Anti-DDoS Pro can still mitigate DDoS attacks. Burstable protection is charged based on the difference between the peak bandwidth of the DDoS attacks on the day and the basic protection bandwidth.

  For example, the basic protection bandwidth of your Anti-DDoS Pro instance is 30 Gbit/s and the burstable protection bandwidth is 100 Gbit/s. Then, burstable protection is charged for mitigating DDoS attacks with a peak bandwidth between 30 Gbit/s and 100 Gbit/s. If the peak bandwidth of the DDoS attacks exceeds the burstable protection bandwidth, the instance is unable to mitigate the attacks. In this case, no additional fee is charged. If the peak bandwidth of DDoS attacks is 30 Gbit/s or lower, only basic protection is triggered. In this case, no fee is charged for burstable protection.

For more information, visit the Anti-DDoS pricing page.

Basic protection: subscription billing (billed monthly)

The following table lists the prices of an Anti-DDoS Pro instance based on different basic protection bandwidths when the default specifications are used. An Anti-DDoS Pro instance provides a standard function plan and an enhanced function plan. The prices vary based on the function plan. For more information about the standard function plan and the enhanced function plan, see Function plan.

> **Note** If the protection bandwidths listed in the following table cannot meet your business needs, submit a ticket.

Basic protection bandwidth	Line	Price (standard function plan)	Price (enhanced function plan)
30 Gbit/s		USD 3,120/month	USD 4,320/month

Basic protection bandwidth	Line	Price (standard function plan)	Price (enhanced function plan)
60 Gbit/s	Eight BGP lines	USD 7,020/month	USD 8,220/month
100 Gbit/s		USD 49,230/year (available only for annual subscription)	USD 63,630/year (available only for annual subscription)
300 Gbit/s		USD 79,260/year (available only for annual subscription)	USD 93,660/year (available only for annual subscription)
400 Gbit/s		USD 145,300/year (available only for annual subscription)	USD 159,700/year (available only for annual subscription)
500 Gbit/s		USD 563,430/year (available only for annual subscription)	USD 577,830/year (available only for annual subscription)
600 Gbit/s		USD 670,610/year (available only for annual subscription)	USD 685,010/year (available only for annual subscription)

The following table lists the default specifications of an Anti-DDoS Pro instance and the price for upgrades. If the default specifications cannot meet your needs, you can specify higher specifications when you purchase the instance. You can also upgrade the instance after you purchase it.

Specification	Description	Default value	Price for upgrades
Number of protected ports	The number of TCP and UDP ports that the instance protects.	50	Every 5 ports: USD 7.5/month
Number of protected domains	The number of HTTP and HTTPS domains that the instance protects.	50 **Note** The domain names that you add to an instance can belong to up to five top-level domain names.	• Standard function plan: USD 4.5/month for every 10 domains • Enhanced function plan: USD 7.5/month for every 10 domains **Note** For every plan you purchase, the total number of supported top-level domains increases by one.

Specification	Description	Default value	Price for upgrades
Clean bandwidth	The maximum bandwidth that the instance uses to handle services if no attacks are launched.	100 Mbit/s	1 Mbit/s: USD 15/month Note If your clean bandwidth exceeds 600 Mbit/s, you are charged a monthly fee of USD 11/month per Mbit/s for the extra bandwidth usage.
Queries per second (QPS)	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks are launched.	3,000 QPS	Every 100 QPS: USD 1.5/month

Burstable protection (pay-as-you-go on a daily basis)

Anti-DDoS Pro provides burstable protection to safeguard your services when the peak bandwidth of DDoS attacks exceeds the basic protection bandwidth. Burstable protection is charged based on the difference between the peak bandwidth of DDoS attacks on the day and the basic protection bandwidth.

Note If you specify the same value for the burstable protection bandwidth and the basic protection bandwidth, no additional fee is charged. However, your Anti-DDoS Pro instance does not provide burstable protection.

Billing:

- If the peak bandwidth of DDoS attacks on the day is lower than or equal to the basic protection bandwidth, no fee is charged for burstable protection.
- If the peak bandwidth of DDoS attacks on the day is higher than the burstable protection bandwidth, no fee is charged for burstable protection. In this case, network traffic destined for the domain that is protected by an Anti-DDoS Pro instance is routed to the blackhole.
- The bill for the burstable protection service you use each day is generated between 08:00:00 to 09:00:00 the following day.

For example, the basic protection bandwidth of your Anti-DDoS Pro instance is 30 Gbit/s and the burstable protection bandwidth is 100 Gbit/s. Two DDoS attacks are launched against the instance on the same day. The peak bandwidths of the two DDoS attacks are 80 Gbit/s and 40 Gbit/s, both of which exceed the basic protection bandwidth. Burstable protection is charged based on the higher peak bandwidth (80 Gbit/s). The difference between the peak bandwidth and the basic protection bandwidth (30 Gbit/s) is 50 Gbit/s. In this case, Anti-DDoS Pro charges USD 960 for burstable protection.

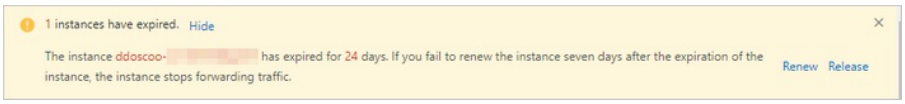
The following table lists prices of burstable protection based on different pricing tiers.

Pricing tier	Price of burstable protection (USD/day)
0 Gbit/s < Bandwidth difference ≤ 5 Gbit/s	120
5 Gbit/s < Bandwidth difference ≤ 10 Gbit/s	180
10 Gbit/s < Bandwidth difference ≤ 20 Gbit/s	330
20 Gbit/s < Bandwidth difference ≤ 30 Gbit/s	540
30 Gbit/s < Bandwidth difference ≤ 40 Gbit/s	730
40 Gbit/s < Bandwidth difference ≤ 50 Gbit/s	960
50 Gbit/s < Bandwidth difference ≤ 60 Gbit/s	1,170
60 Gbit/s < Bandwidth difference ≤ 70 Gbit/s	1,380
70 Gbit/s < Bandwidth difference ≤ 80 Gbit/s	1,590
80 Gbit/s < Bandwidth difference ≤ 100 Gbit/s	1,770
100 Gbit/s < Bandwidth difference ≤ 150 Gbit/s	2,190
150 Gbit/s < Bandwidth difference ≤ 200 Gbit/s	3,240
200 Gbit/s < Bandwidth difference ≤ 300 Gbit/s	4,200
300 Gbit/s < Bandwidth difference ≤ 400 Gbit/s	6,000
400 Gbit/s < Bandwidth difference ≤ 500 Gbit/s	7,510
500 Gbit/s < Bandwidth difference ≤ 600 Gbit/s	9,010
600 Gbit/s < Bandwidth difference ≤ 700 Gbit/s	10,510

Pricing tier	Price of burstable protection (USD/day)
700 Gbit/s < Bandwidth difference ≤ 800 Gbit/s	12,010
800 Gbit/s < Bandwidth difference ≤ 900 Gbit/s	13,510
900 Gbit/s < Bandwidth difference ≤ 1,000 Gbit/s	15,010
1,000 Gbit/s < Bandwidth difference ≤ 1,100 Gbit/s	16,510
1,100 Gbit/s < Bandwidth difference ≤ 1,200 Gbit/s	18,010
1,200 Gbit/s < Bandwidth difference ≤ 1,300 Gbit/s	19,510
1,300 Gbit/s < Bandwidth difference ≤ 1,400 Gbit/s	21,010
1,400 Gbit/s < Bandwidth difference ≤ 1,500 Gbit/s	22,520

Instance expiration

Instance status	Description
Before expiration	Alibaba Cloud sends you text messages, emails, and internal messages seven days, three days, and one day before your Anti-DDoS Pro instance expires to remind you to renew your subscription.
Within seven days after expiration	• Impact on protection: If you do not renew the subscription of your Anti-DDoS Pro instance before the expiration date, the expired instance stops providing burstable protection and restores the protection bandwidth to the default bandwidth (5 Gbit/s). However, the Anti-DDoS Pro instance still forwards your network traffic within seven days after it expires. • Notification: Alibaba Cloud reminds you to renew the expired instance. The instance is valid within seven days after it expires.

Instance status	Description
Seven days after expiration	• Impact on traffic forwarding: If you do not renew the subscription of an Anti-DDoS Pro instance within seven days after the instance expires, the instance stops forwarding traffic. After you renew the expired Anti-DDoS Pro instance, the instance becomes available and can continue to forward traffic. Note If Anti-DDoS Pro stops forwarding traffic, your services may be interrupted. We recommend that you read the notifications of instance expiration and renew the subscription of instances at the earliest opportunity. Alternatively, you can enable auto-renewal.  • Impact on instance configurations: Alibaba Cloud reclaims instance resources on a regular basis. If you do not renew the subscription of an Anti-DDoS Pro instance that has been expired for more than seven days, the instance and the resources that are configured for the instance are released. • Notification: Seven days after the expiration date, Alibaba Cloud notifies you that the expired instance has stopped forwarding traffic.

Refunding

The subscription of an Anti-DDoS Pro instance cannot be canceled before the expiration date. The subscription fees cannot be refunded after you purchase the instance. After an Anti-DDoS Pro instance is created, the fees you paid cannot be refunded.

References

- 开通DDoS高防（新BGP&国际）
- Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance

3.Anti-DDoS premium billing methods

3.1. Billing methods of Insurance Plan and Unlimited Plan

This topic describes the billing methods of Anti-DDoS Premium Insurance Plan and Unlimited Plan.

Overview

Anti-DDoS Premium provides **advanced mitigation**[1] to protect your services that are deployed in regions outside mainland China against DDoS attacks. The number of advanced mitigation sessions that you can use varies based on the mitigation plan that you purchase: **Insurance Plan**[2] and **Unlimited Plan**[3].

Anti-DDoS Premium supports only the **subscription** billing method. Before you use Anti-DDoS Premium to protect your services, you must purchase an Anti-DDoS Premium instance. When you purchase an Anti-DDoS Premium instance, you must specify the mitigation plan, the instance specifications, and the subscription period. An Anti-DDoS Premium instance provides advanced mitigation within the specified subscription period.

[1] Advanced mitigation

Advanced mitigation integrates with all Alibaba Cloud Anti-DDoS scrubbing centers outside mainland China to protect your services from DDoS attacks.

Services protected by Anti-DDoS Premium are less vulnerable to DDoS attacks. In most cases, the goal of DDoS attacks is to cause loss to the victims. However, because the cost of launching a DDoS attack is relatively high, the attackers tend to stop their attack if they cannot achieve their goal within their target time frame.

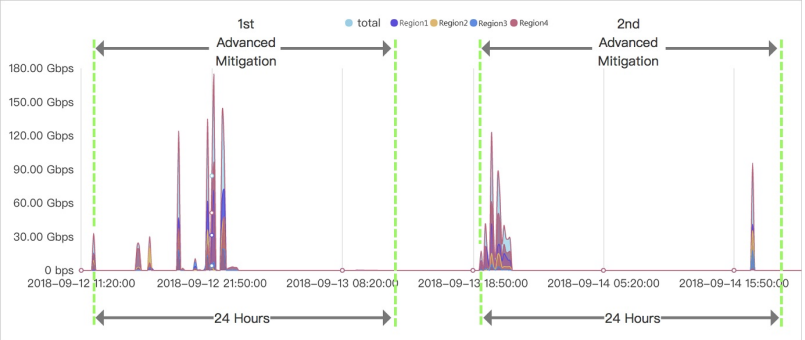
Anti-DDoS Premium provides unlimited advanced mitigation sessions, and integrates with all Alibaba Cloud Anti-DDoS scrubbing centers outside mainland China to safeguard your services.

> **Notice** If the attacks launched against your services threaten the infrastructure of Anti-DDoS scrubbing centers, Alibaba Cloud reserves the rights to throttle the network traffic. If throttling is triggered for your Anti-DDoS Premium instance, your services may be adversely affected. For example, the network traffic may be throttled or even routed to a blackhole in some cases.

[2] Insurance Plan

Insurance Plan is an entry-level mitigation plan for Anti-DDoS Premium. It provides two advanced mitigation sessions per month. Insurance Plan is suitable for users who are less likely to be targeted. If a DDoS attack that is targeted at your services is detected, an advanced mitigation session is triggered to provide unlimited mitigation over the next 24 hours. The number of available advanced mitigation sessions is automatically reset to two on the first day of each month.

For example, a volumetric DDoS attack on a protected IP address is detected at 11:20:00 (UTC+8) on September 12, 2019, and an advanced mitigation session is triggered. One advanced mitigation session is consumed to provide unlimited protection for the IP address over the next 24 hours. Then, another volumetric DDoS attack on the same address is detected at 18:50:00 (UTC+8) on September 13, 2019, and an advanced mitigation session is triggered again. However, because this attack happened more than 24 hours after the first attack, another advanced mitigation session is consumed. This exhausts the two sessions included in Anti-DDoS Premium Insurance Plan for September. The number of available advanced mitigation sessions is reset to two on October 1, 2019.



Note If the two advanced mitigation sessions provided per month cannot meet your business needs, we recommend that you purchase global advanced mitigation. For more information, see Billing methods for global advanced mitigation.

[3] Unlimited Plan

Anti-DDoS Premium Unlimited Plan provides unlimited mitigation sessions. If you purchase Unlimited Plan, Anti-DDoS Premium provides unlimited mitigation sessions to protect your services against DDoS attacks.

Pricing

The following table lists prices of an Anti-DDoS Premium instance based on different clean bandwidths[4] when the default specifications are used. Anti-DDoS Premium provides a standard function plan and an enhanced function plan. Fees vary based on the function plan that you choose. For more information about the standard function plan and the enhanced function plan, see Function plan.

[4] Clean bandwidth

Clean bandwidth refers to the maximum bandwidth that an Anti-DDoS Premium instance can use to handle services if no attacks are launched. The clean bandwidth of an instance must be greater than the peak volume of the inbound and outbound traffic of the protected services.

Warning If the actual bandwidth exceeds the clean bandwidth of the instance, throttling and packet loss can occur. In some cases, your services become unavailable or slow down within a period of time.

> **Note** If the specifications of clean bandwidth listed in the following table cannot meet your business needs, submit a ticket.

Mitigation plan	Clean bandwidth	Unit price in a standard function plan (USD/month)	Unit price in an enhanced function plan (USD/month)
Insurance Plan Two advanced mitigation sessions/month	100 Mbit/s	2,630	3,830
	150 Mbit/s	3,420	4,620
	200 Mbit/s	4,210	5,410
	250 Mbit/s	5,000	6,200
	300 Mbit/s	5,570	6,770
Unlimited Plan Unlimited advanced mitigation sessions	100 Mbit/s	11,560	12,760
	150 Mbit/s	12,610	13,810
	200 Mbit/s	13,660	14,860
	250 Mbit/s	14,720	15,920
	300 Mbit/s	15,770	16,970

The following table lists the default specifications of an Anti-DDoS Premium instance and the prices for upgrades. If the default specifications cannot meet your needs, you can specify higher specifications when you purchase the instance. You can also upgrade the instance after you purchase it.

Specification	Description	Default value	Price for upgrades
Number of protected ports	The number of TCP and UDP ports that the instance protects.	5	Every 5 ports: USD 150/month

Specification	Description	Default value	Price for upgrades
Number of protected domains	The number of HTTP and HTTPS domains that the instance protects.	10 Note The 10 domain names can belong to only one top-level domain name. This means that the domain names protected by an instance must belong to the same top-level domain name.	• Standard function plan: USD 45/month for every 10 domains • Enhanced function plan: USD 75/month for every 10 domains Note For every plan you purchase, the total number of supported top-level domains increases by one.
Queries per second (QPS)	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks are launched.	• Insurance Plan: 500 QPS • Unlimited Plan: 1,000 QPS	Every 100 QPS: USD 150/month

Instance expiration

Instance status	Description
Before expiration	Alibaba Cloud sends you text messages and emails seven days, three days, and one day before your instance expires to remind you to renew your subscription.
Within 30 days after expiration	• Impact on mitigation: If the subscription of an Anti-DDoS Premium instance is not renewed before the expiration date, the protection stops after the instance expires. The mitigation capacity is restored to the default free protection capacity. • Impact on instance configurations: After an Anti-DDoS Premium instance expires, the configurations are retained for 30 days. If you renew the subscription of the instance within 30 days, you can still use the instance with the retained configurations.

Instance status	Description
30 days after expiration	If you do not renew the subscription of your Anti-DDoS Premium instance within 30 days after the instance expires, the instance and the instance configurations are automatically released. If you want to continue using Anti-DDoS Premium, you must purchase another Anti-DDoS Premium instance and complete the configurations.

Refunding

The subscription of an Anti-DDoS Premium instance cannot be canceled before the expiration date. The subscription fees cannot be refunded after you purchase the instance. After an Anti-DDoS Premium instance is created, the fees you paid cannot be refunded.

References

- 开通DDoS高防（新BGP&国际）
- Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance

3.2. Mainland China Acceleration billing methods

This topic describes the billing methods of Anti-DDoS Premium Mainland China Acceleration (MCA). Before you use MCA, you must purchase an Anti-DDoS Premium instance. You can purchase an Anti-DDoS Premium instance to defend against DDoS attacks for services that are deployed outside mainland China. If no attacks are launched, you can use MCA to accelerate service delivery to users in mainland China.

Overview

MCA is suitable for services that are deployed in regions outside mainland China and are protected by Anti-DDoS Premium. If no attack is launched against your Anti-DDoS Premium instance, you can use MCA to accelerate service delivery to users in mainland China.

> **Notice** An MCA instance does not offer any protection and must be used with an Anti-DDoS Premium Insurance Plan or Unlimited Plan instance.

MCA instances support only the **subscription** billing method. Before you use MCA, you must purchase an MCA instance, and specify the specifications and the subscription period. An MCA instance provides acceleration for services that are added to Anti-DDoS Premium within the subscription period.

Pricing

The following table lists the prices of an MCA instance based on different **clean bandwidths**[1].

[1] ***Clean bandwidth***
Clean bandwidth refers to the maximum bandwidth that an MCA instance can use to accelerate service delivery if no attacks are launched. The clean bandwidth of an MCA instance must be greater than the peak volume of the inbound and outbound traffic of the protected services.

> **Warning** If the actual bandwidth exceeds the clean bandwidth of the instance, throttling and packet loss can occur. In some cases, your services become unavailable or slow down within a period of time.

Clean bandwidth	Unit price (USD/month)
10 Mbit/s	1,548
20 Mbit/s	3,096
30 Mbit/s	4,643
40 Mbit/s	6,191
50 Mbit/s	7,739
60 Mbit/s	9,287
70 Mbit/s	10,834
80 Mbit/s	12,382
90 Mbit/s	13,930
100 Mbit/s	15,478

Instance expiration

Instance status	Description
Before expiration	Alibaba Cloud sends you text messages and emails seven days, three days, and one day before your instance expires to remind you to renew your subscription.
Within 30 days after expiration	• Impact on acceleration: You must renew the subscription of your MCA instance before the expiration date. After the MCA instance expires, it stops accelerating service delivery. • Impact on instance configurations: The configurations of an expired MCA instance are retained for 30 days. To continue using the MCA instance with the retained configurations, renew the subscription of your MCA instance within 30 days after the expiration date.
30 days after expiration	If you do not renew the subscription of your MCA instance within 30 days after the instance expires, the instance and the instance configurations are automatically released. To continue using the acceleration service, you must purchase another MCA instance.

References

- 开通DDoS高防（新BGP&国际）

- Configure Anti-DDoS Premium MCA

3.3. Sec-MCA billing methods

This topic describes the billing methods of Anti-DDoS Premium Secure Mainland China Acceleration (Sec-MCA).

Overview

Anti-DDoS Premium Sec-MCA supports only the **subscription** billing method. Before you use Anti-DDoS Premium Sec-MCA to protect your services, you must purchase an Anti-DDoS Premium Sec-MCA instance, and specify the function plan, instance specifications, and subscription period. An Anti-DDoS Premium Sec-MCA instance provides access acceleration and DDoS mitigation services within the subscription period.

Pricing

The following table lists the prices of an Anti-DDoS Premium Sec-MCA instance at different **clean bandwidths**[1] when the default specifications are used. Anti-DDoS Premium Sec-MCA provides a standard function plan and an enhanced function plan. Fees vary based on the function plan that you choose. For more information, see Function plan.

[1] Clean bandwidth

Clean bandwidth refers to the maximum bandwidth that an Anti-DDoS Premium Sec-MCA instance can use to handle services if no attacks are launched. Make sure that the clean bandwidth of the instance is greater than the peak bandwidth of the inbound and outbound traffic of all the protected services.

Warning If the actual bandwidth exceeds the clean bandwidth of the instance, throttling and packet loss can occur. In some cases, your services become unavailable or slow down within a period of time.

Note If the specifications of clean bandwidth listed in the following table cannot meet your business needs, submit a ticket.

Clean bandwidth	Unit price of a standard function plan (USD/month)	Unit price of an enhanced function plan (USD/month)
10 Mbit/s	15,480	16,680
20 Mbit/s	17,028	18,228
30 Mbit/s	18,576	19,776
40 Mbit/s	20,124	21,324
50 Mbit/s	21,672	22,872
60 Mbit/s	23,220	24,420

Clean bandwidth	Unit price of a standard function plan (USD/month)	Unit price of an enhanced function plan (USD/month)
70 Mbit/s	24,768	25,968
80 Mbit/s	26,316	27,516
90 Mbit/s	27,864	29,064
100 Mbit/s	29,412	30,612
150 Mbit/s	37,152	38,352
200 Mbit/s	44,892	46,092

The following table lists the default specifications of an Anti-DDoS Premium Sec-MCA instance and the prices for upgrades. If the default specifications cannot meet your needs, specify higher specifications when you purchase the instance or upgrade the instance after you purchase it.

Specification	Description	Default value	Price for upgrades
Number of protected ports	The number of TCP and UDP ports that the instance protects.	5	Every 5 ports: USD 150/month
Number of protected domains	The number of HTTP and HTTPS domains that the instance protects.	10 Note The 10 domain names can belong to only one top-level domain name. This means that the domain names protected by an instance must belong to the same top-level domain name.	• Standard function plan: USD 45/month for every 10 domains • Enhanced function plan: USD 75/month for every 10 domains Note For every plan you purchase, the total number of supported top-level domains increases by one.

Specification	Description	Default value	Price for upgrades
Queries per second (QPS)	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks are launched.	500 QPS	Every 100 QPS: USD 150/month

Instance expiration

Instance status	Description
Before expiration	Alibaba Cloud sends you text messages and emails seven days, three days, and one day before your instance expires to remind you to renew your subscription.
Within 30 days after expiration	• Impact on mitigation: If you do not renew the subscription of your Anti-DDoS Premium Sec-MCA instance before it expires, the instance stops access acceleration and DDoS attack mitigation upon expiration. The DDoS mitigation capacity for protected assets is restored to the free protection capacity. • Impact on configurations: After an Anti-DDoS Premium Sec-MCA instance expires, the configurations are retained for 30 days. If you renew the subscription of your instance within 30 days, you can still use the instance with the retained configurations.
30 days after expiration	If you do not renew the subscription of your Anti-DDoS Premium Sec-MCA instance within 30 days after the instance expires, the instance and its configurations are released. If you need to continue using Anti-DDoS Premium Sec-MCA, you must purchase another Anti-DDoS Premium Sec-MCA instance and complete the configurations.

Refunding

The subscription of an Anti-DDoS Premium Sec-MCA instance cannot be canceled before the expiration date. The subscription fees cannot be refunded after you purchase the instance. After an Anti-DDoS Premium Sec-MCA instance is created, the fees you paid cannot be refunded.

References

- 开通DDoS高防（新BGP&国际）
- Configure Anti-DDoS Premium Sec-MCA

3.4. Billing methods for global advanced mitigation

This topic describes the billing methods of global advanced mitigation of Anti-DDoS Premium. Global advanced mitigation must be used with Anti-DDoS Premium Insurance Plan. If the two advanced mitigation sessions per month provided by Anti-DDoS Premium Insurance Plan are exhausted, you can purchase global advanced mitigation sessions that provide unlimited bandwidth protection.

Background information

Anti-DDoS Premium Insurance Plan provides two free advanced mitigation sessions per month. When DDoS attacks are detected, Anti-DDoS Premium Insurance Plan protects your services with unlimited capabilities in the following 24 hours. This consumes one advanced mitigation session.

If your services receive frequent volumetric DDoS attacks, the two advanced mitigation sessions are not enough to guarantee service availability. In this case, you can purchase global advanced mitigation sessions for Anti-DDoS instances under your account.

The following table lists the differences between global advanced mitigation and advanced mitigation of Anti-DDoS Premium instances.

Type	Scope	Validity period	Number of sessions
Advanced mitigation of Anti-DDoS Premium Unlimited Plan	Instance	Based on the validity period of instances	Unlimited
Advanced mitigation of Anti-DDoS Premium Insurance Plan	Instances	One month Note Unused advanced mitigation sessions in the current month are not retained for the next month.	Two sessions per month
Global advanced mitigation	Alibaba account	One year	Purchase based on needs

Pricing

The following table shows the pricing of global advanced mitigation.

Item	Description
Payment type	Subscription
Validity period	One year
Unit price	USD 1,580 per session

No refund

The fees paid for global advanced mitigation cannot be refunded.

Related topics

Purchase global advanced mitigation

4.Function plan

Both Anti-DDoS Pro and Anti-DDoS Premium provide standard and enhanced function plans. The enhanced function plan provides the following features in addition to all the features of the standard function plan: static page caching, non-standard ports support, and blocked regions. These features enhance connection capabilities of instances and the ability of Anti-DDoS Pro and Anti-DDoS Premium to prevent DDoS attacks. You can select a mitigation plan as required.

When you purchase Anti-DDoS Pro or Anti-DDoS Premium instances, the standard function plan is selected by default. You can select the enhanced function plan to obtain advanced anti-DDoS protection. The price for each instance that uses the enhanced function plan is USD 1,145 per month.

For a purchased instance that uses the standard function plan, you can scale up the specification to obtain enhanced anti-DDoS protection. For more information, see Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance.

> **Note** After you purchase an instance that uses the enhanced function plan or upgrade an instance to the enhanced function plan, you need to configure the domain names to enable the enhanced capabilities.

Comparison of the standard and enhanced function plans

The following table describes feature differences between the standard and enhanced function plans.

Category	Feature	Description	Standard function plan	Enhanced function plan
Protection algorithm	Protection against volumetric DDoS attacks	Supports protection against volumetric DDoS attacks such as malformed packet attacks and flood attacks.	✓	✓
	Protection against resource exhaustion DDoS attacks	Supports protection against common HTTP flood attacks at the transport layer, such as HTTP GET floods and HTTP POST floods. For more information, see Configure frequency control.	✓	✓

Category	Feature	Description	Standard function plan	Enhanced function plan
	Intelligent protection	• Supports intelligent protection against application-layer floods and mitigates HTTP flood attacks. • Supports intelligent protection against transport-layer floods and mitigates TCP flood attacks. For more information, see Configure intelligent protection.	✓	✓
Protection rule	Black lists and white lists	A blacklist and whitelist for each protected domain name can each contain a maximum of 200 IP addresses. For more information, see Configure blacklists and whitelists for domain names.	✓	✓
	Accurate access control	Supports fine-grained access control based on HTTP. For more information, see 设置精准访问控制.	For each protected domain name, you can configure a maximum of five rules based on the following fields: IP, URL, Referer, and User-Agent.	For each protected domain name, you can configure a maximum of 10 rules.
	Blocked regions	Blocks traffic based on geographic locations. For more information, see Configure blocked regions for domain names.	✗	✓

Category	Feature	Description	Standard function plan	Enhanced function plan
Connection methods	Standard HTTP ports (80 and 8080) and HTTPS ports (443 and 8443)	Supports anti-DDoS protections based on standard HTTP ports (80 and 8080) and HTTPS ports (443 and 8443).	✓	✓
	Non-standard HTTP and HTTPS ports	Supports DDoS prevention based on non-standard HTTP and HTTPS ports. Note For each instance, you can configure a maximum of 10 port forwarding rules that use non-standard ports.	✗	✓
Other	Static page caching	Supports static page caching to reduce page loading time. Note Static page caching is in the public preview stage. For each protected domain name, you can configure a maximum of three rules. For more information, see Configure static page caching.	✗	✓