Anti-DDoS Service (AAD)

Billing Description

Issue   01

Date   2023-09-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
             Qianzhong Avenue
             Gui'an New District
             Gui Zhou 550029
             People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Billing Overview

In this document, you will learn about the billing modes, billing items, renewal, and arrear of Huawei Cloud DDoS Mitigation service.

- **Billing modes**

  DDoS Mitigation supports the yearly/monthly billing mode. Yearly/Monthly: You pay upfront for the amount of time you expect to use the service for. You will need to make sure you have a top-up account with a sufficient balance or have a valid payment method configured first. For details, see **Overview**.

- **Billed Items**

  The billing items of DDoS Mitigation include the number of instances, number of protected domain names/IP addresses, number of protected ports, number of protection times, self-service unblocking packages, line resources, basic protection bandwidth, elastic protection bandwidth, and purchased duration. The billing items vary depending on the edition. For details about DDoS Mitigation billing items and calculation formulas, see **Billing Items**.

- **Renewing Subscriptions**

  After a DDoS Mitigation instance purchased in yearly/monthly mode expires, its protection functions will be unavailable. If you want to continue using the protection functions of DDoS Mitigation, you need to renew your DDoS Mitigation instance within the specified period. Otherwise, resources such as the instance will be automatically removed, and domain name/IP configuration data may be lost. You can renew your subscription manually or automatically. For more details about renewal, see **Overview**.

- **Viewing Bills**

  You can go to **Billing & Costs** > **Bills** to view bills and expenditures for Anti-DDoS Service resources. For details, see **Bills**.

- **Arrears**

  Your account goes into arrears when the balance is less than the bill to be settled. If you are in arrears, your DDoS Mitigation instances may not run correctly. Please top up in time. For details, see **Arrears**.

- **Stopping Billing**

  If you no longer need a cloud service resource, you can unsubscribe from or delete it to stop the billing. For details, see **Stopping Billing**.

- **Managing Costs**

DDoS Mitigation costs include resource costs and O&M costs. You can optimize costs through cost collection, resource optimization, upgrade, thrift, and automatic O&M. For details, see **Cost Management**.

2 Billing Modes

2.1 Overview

DDoS Mitigation supports the yearly/monthly billing mode. In this mode, you need to pay first, and will be billed based on the required duration in your order. The longer you use the service, the more discounts you get. This mode is applicable to mature services that have long-term and stable device requirements. However, in some DDoS Mitigation editions, there are postpaid billing items.

2.2 Yearly/Monthly Billing

Yearly/Monthly billing is a prepaid billing mode in which you pay before using resources. It is suitable when your resource requirements are fixed because you can pay less by using longer. In the yearly/monthly billing mode, we offer discounts to you. This topic describes the billing rules of yearly/monthly DDoS Mitigation resources.

Application Scenarios

If you want to ensure resource stability over a certain period of time, yearly/monthly billing is a good choice. The yearly/monthly billing mode is recommended for the following workloads:

- Long-term workloads with stable resource requirements, such as official websites, online malls, and blogs.
- Long-term projects, such as scientific research projects and large-scale events.
- Workloads with predictable traffic bursts, for example, e-commerce promotions or festivals.
- Workloads with high data security requirements

Billing items

Table 2-1 lists the yearly/monthly billing items supported by different editions of the DDoS Mitigation service.

Table 2-1 Billing Item

Edition	Billing Item	Description
CNAD Unlimited Protection Basic Edition	Instances	Billed by the number of purchased instances.
	Protected IP addresses	Number of IP addresses protected by each instance
	Service bandwidth	Bandwidth resources used your services
CNAD Unlimited Protection Advanced Edition	Instances	Billed by the number of purchased instances.
	Protected IP addresses	Number of IP addresses protected by each instance
	Service bandwidth	Bandwidth resources used your services
AAD	Number of instances	Billed by the number of purchased instances.
	Basic protection bandwidth	Prepaid by month or year
	Elastic protection bandwidth	Postpaid by day
	Service bandwidth	100 Mbit/s is provided for free. If the bandwidth exceeds 100 Mbit/s, you need to pay for the extra bandwidth by month or year.
	Protected domain names (domain name access)	Number of domain names protected by each instance. This billing item is available only for the domain name access type.
	Forwarding rules (IP access)	TCP/UDP forwarding rules that can be added to each instance. This billing item is available only for the IP access type.
AAD International	Instances	Billed by the number of purchased instances.
	Basic protection bandwidth	Prepaid by month or year
	Service bandwidth	Prepaid by month or year
	Protected domain names	Number of domain names protected by each instance

Edition	Billing Item	Description
	Forwarding rules	TCP/UDP forwarding rules that can be added to each instance

Billing Periods

The billing period of yearly/monthly DDoS Mitigation instance is determined by purchase duration (UTC+8). The billing starts when you activated or renewed the subscription (accurate to seconds), and ends at 23:59:59 of the expiry date.

For example, if you purchased a one-month DDoS Mitigation instance on March 08, 2023, 15:50:04, the billed usage period is from March 08, 2023, 15:50:04 to April 08, 2023, 23:59:59.

Billing Examples

Assume that you purchase an instance of the basic edition at 15:50:04 on March 8, 2023. The billing resources include the number of protected IP addresses and service bandwidth. Your subscription is 3 months and you manually renew the subscription for another 3 months before the subscription expires. The billing details will be as follows:
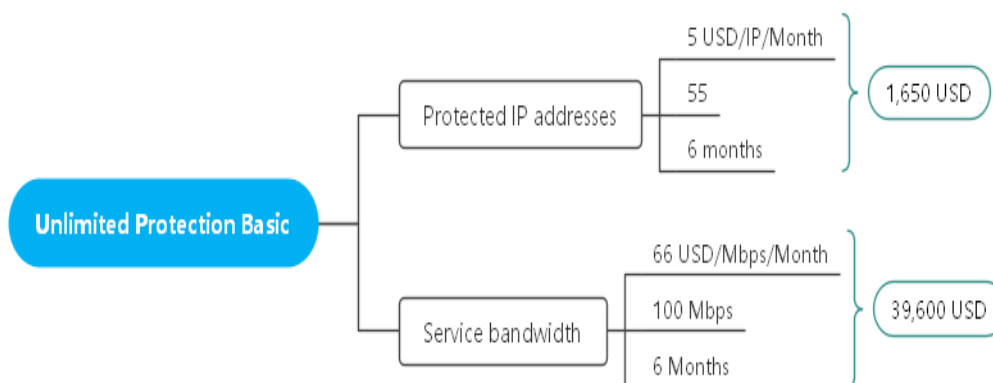
- The first billing period is from to 2023-03-08 15:50:04 to 2023-06-08 23:59:59.
- The second billing period is from 2023-08-08 23:59:59 to 2023-09-08 23:59:59.

Figure 2-1 shows the billing calculation.

NOTICE

The price in the figure is only an example. The actual price is based on that on the DDoS Mitigation console.

Figure 2-1 Fee calculation example

Price Change After Specification Change

If the specifications of the current yearly/monthly DDoS Mitigation resources do not meet your requirements, you can modify the specifications on the DDoS Mitigation console. The system will calculate the DDoS Mitigation fee based on the following rules:

● If you upgrade your DDoS Mitigation specifications, you need to pay the difference in price.

● Resource specification downgrade: Currently, DDoS Mitigation instances do not support specification downgrade.

If you want to upgrade the specifications of BGP 10 GB billed by month (for example, CNY8700/month) to the BGP Pro 10 GB billed by month (for example, CNY9800/month), the remaining days of your current specifications are 20 days.

The formula is as follows:

Specification upgrade fee = (Monthly price of the new specifications/30 – Monthly price of the old specifications/30) x Remaining period

The additional fee is (9800/30-8700/30) x 20 = 733.34 CNY.

For more information, see **Pricing of a Changed Specification**.

Impacts of Expiration

Figure 2-2 describes the status of each stage of a yearly/monthly DDoS Mitigation instance. After a DDoS Mitigation instance is purchased, it enters the valid period and runs normally during this period. If the instance is not renewed after it expires, before being deleted, it first enters a grace period and then a retention period.

Figure 2-2 DDoS Mitigation instance lifecycle
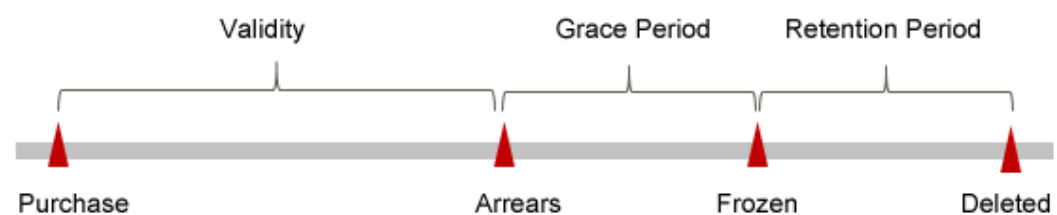
Expiration Reminder

From the 7th day before a yearly/monthly DDoS Mitigation instance expires, the system will send an expiration reminder to the creator of the account by email, SMS, and internal message.

Impact of Expiration

If your yearly/monthly DDoS Mitigation instance is not renewed after it expires, it changes to the **Expired** state and enters a grace period. During the grace period, you can still use your DDoS Mitigation instance, but the following operations will be restricted:

- Upgrading specifications

If the yearly/monthly DDoS Mitigation instance is not renewed after the grace period ends, its status turns to **Frozen** and it enters a retention period. You cannot perform any operations on the DDoS Mitigation instance while it is in the retention period.

If the instance is not renewed after the retention period expires, the instance will be removed and data cannot be restored.

📖 **NOTE**

- Huawei Cloud offers a 15-day grace period and a 15-day retention period.
- For details about renewal, see **Overview**.

3 Billing Items

3.1 CNAD Unlimited Protection - Basic Edition

Billing Description

The billing items of the basic edition consist of the number of instances, number of protected objects, and service bandwidth. **Table 3-1** describes the billing items.

Table 3-1 Billing Item

Edition	Billing Mode	Billed Item	Description
CNAD unlimited protection basic edition	Yearly/ Monthly	Number of instances	Billed by the number of purchased instances.
		Protected IP addresses	Number of IP addresses protected by each instance
		Service bandwidth	Bandwidth resources used your services

Billing Examples

Assume that you purchase an instance of the basic edition at 15:50:04 on March 8, 2023. The billing resources include the number of protected IP addresses and service bandwidth. Your subscription is 3 months and you manually renew the subscription for another 3 months before the subscription expires. The billing details will be as follows:
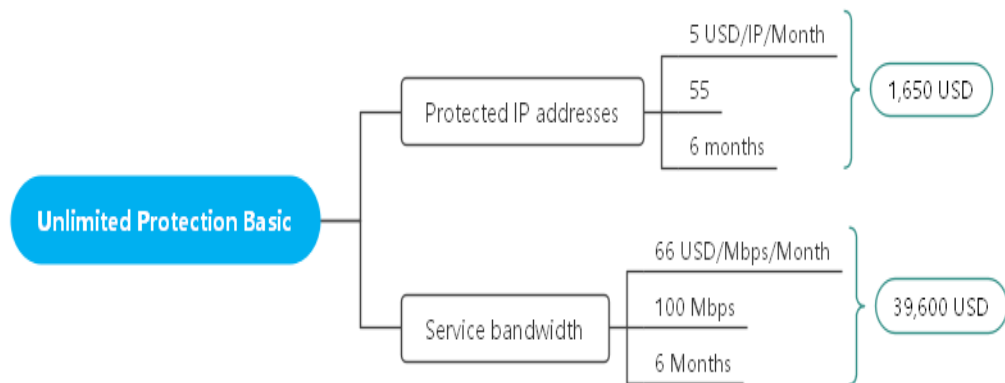
- The first billing period is from to 2023-03-08 15:50:04 to 2023-06-08 23:59:59.

- The second billing period is from 2023-08-08 23:59:59 to 2023-09-08 23:59:59.

Figure 3-1 shows the billing calculation.

> **NOTICE**
>
> The price in the figure is only an example. The actual price is based on that on the DDoS Mitigation console.

Figure 3-1 Fee calculation example

3.2 CNAD Unlimited Protection - Advanced Edition

Billing Description

The billing items of the advanced edition consist of the number of instances, number of protected IP addresses, service bandwidth, and back-to-source bandwidth. **Table 3-2** describes the billing items.

Table 3-2 Billing items of the CNAD Unlimited Protection - Advanced Edition

Edition	Billing Mode	Billed Item	Description
CNAD unlimited protection advanced edition	Yearly/Monthly	Number of instances	Billed by the number of purchased instances.
		Unlimited protection	Unlimited protection capability
		Protected IP addresses	Number of IP addresses protected by each instance
		Service bandwidth	Bandwidth resources used your services

Billing Examples

Assume that you purchase an instance of the advanced edition at 15:50:04 on March 8, 2023. The billing resources include the number of protected IP addresses

and service bandwidth. Your subscription is 3 months and you manually renew the subscription for another 3 months before the subscription expires. The billing details will be as follows:

- The first billing period is from to 2023-03-08 15:50:04 to 2023-06-08 23:59:59.
- The second billing period is from 2023-08-08 23:59:59 to 2023-09-08 23:59:59.

Figure 3-2 shows the billing calculation.

> **NOTICE**
>
> The price in the figure is only an example. The actual price is based on that on the DDoS Mitigation console.

Figure 3-2 Fee calculation example
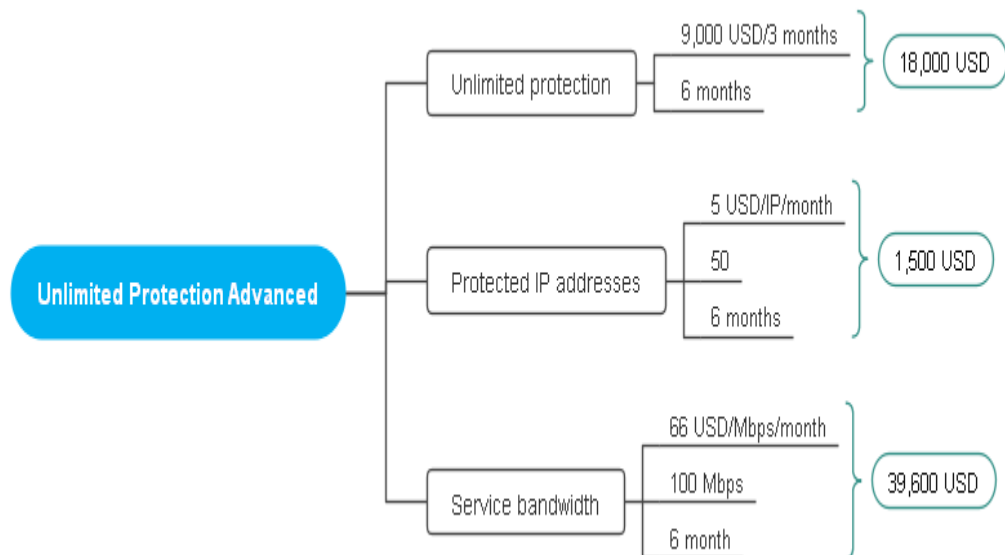
3.3 Anti-DDoS Service (AAD)

Billing Description

The billing items of AAD consist of the number of instances, basic protection bandwidth, elastic protection bandwidth, service bandwidth, number of protected domain names, and number of forwarding rules. **Table 3-3** lists the billing items of AAD

Table 3-3 AAD Billing item

Edition	Billing Mode	Billing Item	Description
AAD	Yearly/ Monthly (including postpaid items)	Number of instances	Billed by the number of purchased instances.
		Basic protection bandwidth	Prepaid by month or year
		Elastic protection bandwidth	Postpaid by day If the peak attack traffic on the current day is less than or equal to the basic protection bandwidth, no elastic protection bandwidth fee is generated.
		Service bandwidth	100 Mbit/s is provided for free. If the bandwidth exceeds 100 Mbit/s, you need to pay for the extra bandwidth by month or year.
		Protected domain names (domain name access)	Number of domain names protected by each instance. This billing item is available only for the domain name access type.
		Forwarding rules (IP access)	TCP/UDP forwarding rules that can be added to each instance. This billing item is available only for the IP access type.

Billing Examples

Assume you purchase an AAD instance through website access at 15:50:04 on March 8, 2023. The billing resources include line resources, basic protection bandwidth, elastic protection bandwidth, service bandwidth, and number of protected domain names, Your subscription is one month and you manually renew the subscription for one month before the subscription expires. The billing details will be as follows:

- March 08, 2023, 15:50:04 to April 08, 2023, 23:59:59
- April 08, 2023, 23:59:59 to May 08, 2023, 23:59:59

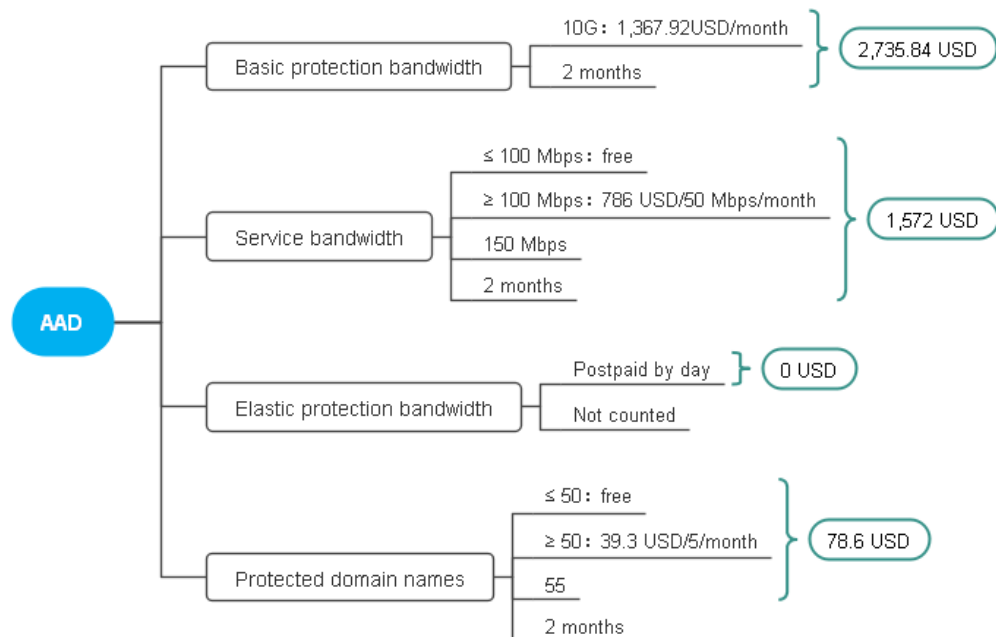**Figure 3-3** shows the billing calculation.

NOTICE

The price in the figure is only an example. The actual price is based on that on the DDoS Mitigation console.

Figure 3-3 Fee calculation example

3.4 AAD - International Edition

Billing Description

The billing items of AAD (international edition) consist of the number of instances, basic protection bandwidth, service bandwidth, number of protected domain names, and number of forwarding rules. **Table 3-4** describes the billing items.

Table 3-4 AAD (International) billing items

Edition	Billing Mode	Billing Item	Description
AAD International	Yearly/ Monthly Billing	Number of Instances	Billed by the number of purchased instances.
		Basic protection bandwidth	Prepaid by month or year
		Service bandwidth	Prepaid by month or year
		Protected domain names	Number of domain names protected by each instance
		Forwarding rules	TCP/UDP forwarding rules that can be added to each instance

Billing Examples

Assume that you purchase an instance of AAD (International) at 15:50:04 on March 8, 2023. The billing resources include the basic protection bandwidth, service bandwidth, number of protected domain names, and number of forwarding rules. Your subscription is 3 months and you manually renew the subscription for another 3 months before the subscription expires. The billing details will be as follows:
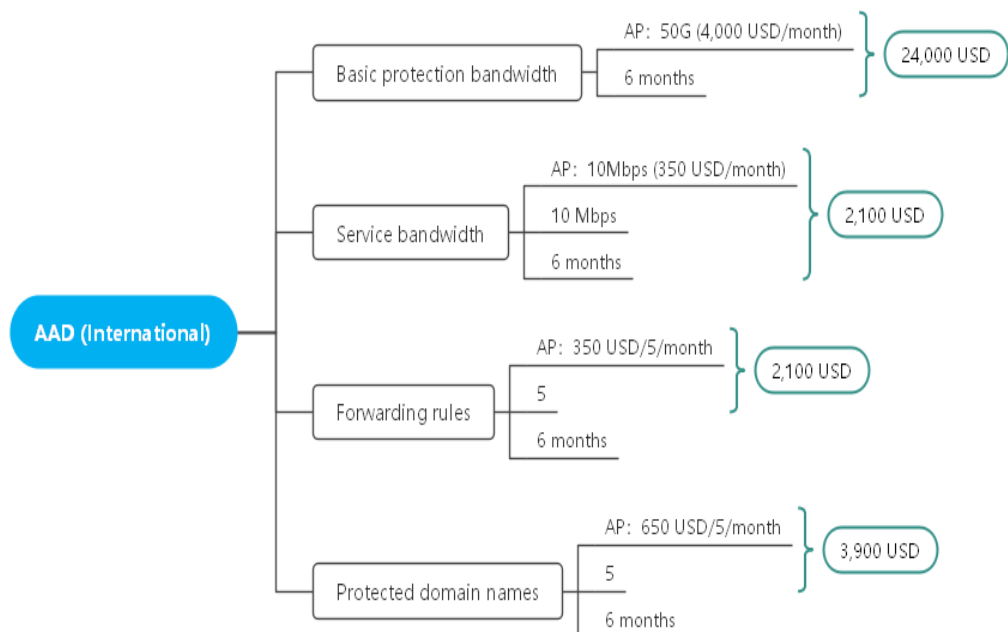
- The first billing period is from to 2023-03-08 15:50:04 to 2023-06-08 23:59:59.

- The second billing period is from 2023-08-08 23:59:59 to 2023-09-08 23:59:59.

Figure 3-4 shows the billing calculation.

NOTICE

The price in the figure is only an example. The actual price is based on that on the DDoS Mitigation console.

Figure 3-4 Fee calculation example

4 Renewing Subscriptions

4.1 Overview

Renewal Introduction

If you do not renew a DDoS Mitigation instance that is billed in yearly/monthly mode upon its expiration, a grace period and a retention period will be granted.

During the grace period, the customer can access and use DDoS Mitigation resources. During this period, the resources cannot be accessed, but the resource data stored will be retained. For details, see **What Is a Grace Period of Huawei Cloud?**

When your purchased instances expire, DDoS Mitigation stops providing services. To prevent security issues from occurring, it is recommended that you renew the DDoS Mitigation instance before its retention period expires.

If you do not renew the subscription, you cannot use the DDoS Mitigation service, but your services are not affected.

You can renew your resources on the **Renewals** page of the management console. For details, see **Renewal Rules**.

Renewal Methods

**Table 4-1** describes the renewal methods of the DDoS Mitigation service

Table 4-1 Renewal methods

Method	Description
Manually Renewing DDoS Mitigation	From the time when you purchase an instance to the time when the instance is automatically deleted, you can renew the instance on the DDoS Mitigation console at any time.

Method	Description
Auto-renewing DDoS Mitigation	After auto-renewal is enabled, DDoS Mitigation instances are automatically renewed before the subscription expires. This prevents resources from being automatically deleted in the event that you forget to manually renew the subscription.

In different phases of the lifecycle of a yearly/monthly DDoS Mitigation instance, you can choose a renewal method as required. For details, see **Figure 4-1**.

Figure 4-1 Lifecycle of an ECS
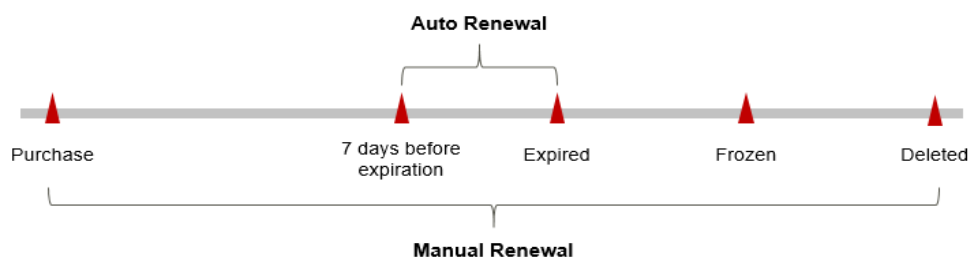
- A DDoS Mitigation instance is in the **Running** state from the time when it is purchased to the time when it expires.

- When an DDoS Mitigation subscription expires, the resource status will change from **Running** to **Expired**.

- If the DDoS Mitigation instance is not renewed upon expiration, it enters the grace period. If it is not renewed after the grace period ends, the status changes to **Frozen**.

- If you do not renew your subscription after the grace period expires, your resources enter a retention period. If you do not renew the subscription within the retention period, your resources will be automatically deleted.

Auto-renewal can be enabled anytime before a DDoS Mitigation instance expires. The system attempts to automatically renew the instance at 03:00 seven days before the instance expires. If the fee deduction fails, there will be one attempt at 03:00 every day until the instance expires or the renewal is successful. You can change the auto-payment date for renewal as required.

4.2 Manually Renewing DDoS Mitigation

CNAD Advanced and AAD support renewal on the console or in the Billing Center. You are advised to renew an AAD (international) instance in the Billing Center.

Renewing a Subscription on the Console (CNAD Advanced)
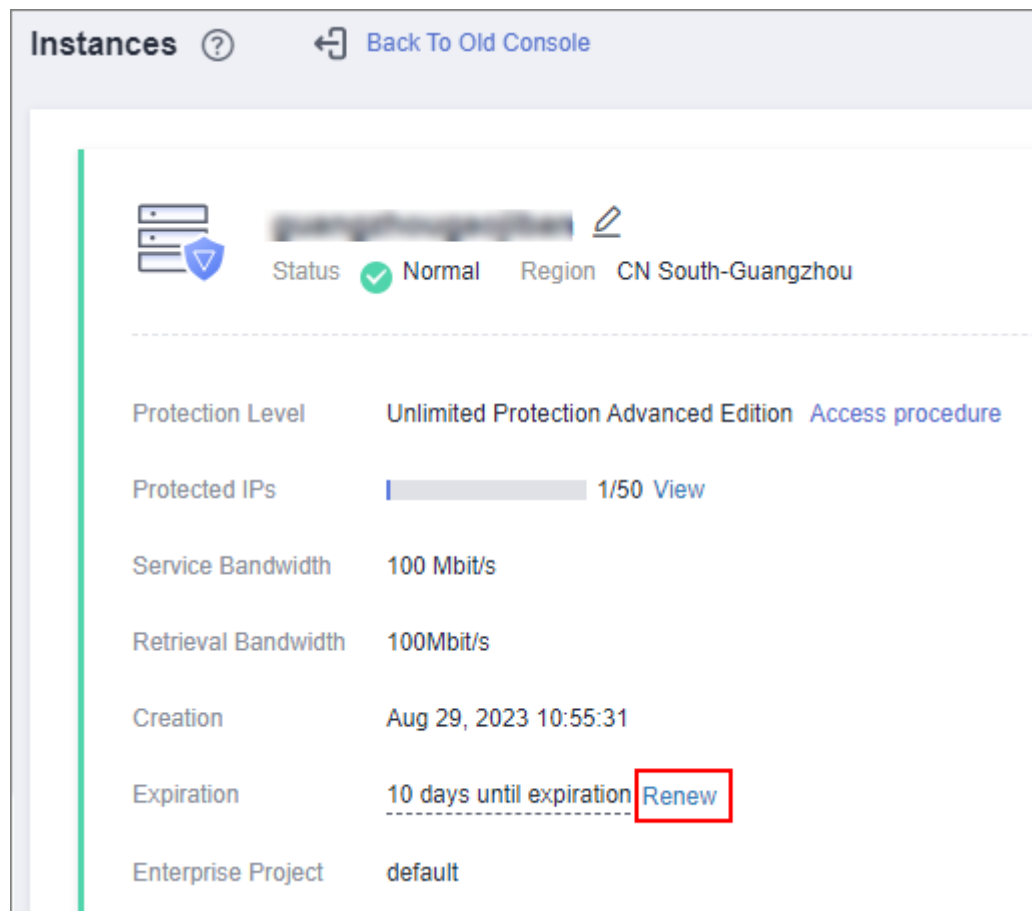
Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner of the console and select a region or project.

Step 3 Click in the navigation tree on the left and choose **Security & Compliance** > **DDoS Mitigation**. The DDoS Mitigation console is displayed.

Step 4 In the navigation pane on the left, choose **Cloud Native Anti-DDoS Advanced** > **Instances**. The **Instances** page is displayed.

Step 5 Under the instance to be renewed, click **Renew**.

Figure 4-2 Renewing subscriptions

Step 6 On the **Renew** page, select a renewal duration and click **Pay** to complete the payment.

----End

Renewing a Subscription on the Console (AAD)

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner of the console and select a region or project.

Step 3 Click in the navigation tree on the left and choose **Security & Compliance** > **DDoS Mitigation**. The DDoS Mitigation console is displayed.

Step 4 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Instances**. The **Instances** page is displayed.

Step 5 Under the instance to be renewed, click **Renew**.

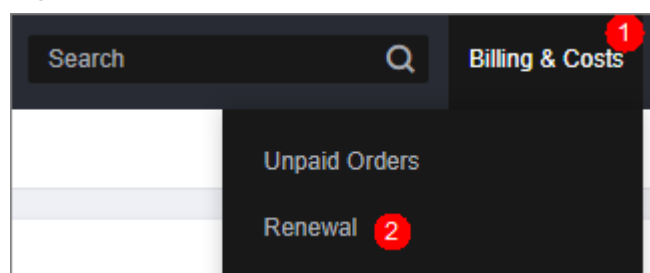**Figure 4-3** Renewing Subscriptions

Step 6 On the **Renew** page, select a renewal duration and click **Pay** to complete the payment.

----End

Renewing a Subscription in the Billing Center

Step 1 **Log in to the management console**.

Step 2 On the top navigation bar, choose **Billing and Costs** > **Renewal**. The **Renewal** page is displayed.

Figure 4-4 Renewals

Step 3 Complete the renewal by referring to **Renewal Rules**.

----End

Setting the Same Renewal Day for Yearly/Monthly Resources

If you have multiple DDoS Mitigation instances with different expiration dates, you can set a fixed expiration date to facilitate routine management and renewal.

In **Figure 4-5**, a user sets the same renewal day for two resources that will expire at different dates.

Figure 4-5 Setting the same renewal day for resources with different expiry dates
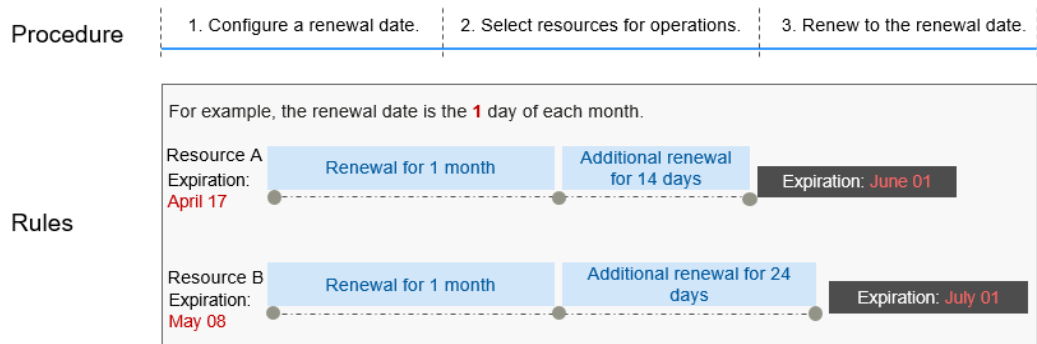
For details, see **Setting a Renewal Date**.

4.3 Auto-renewing DDoS Mitigation

Auto-renewal can prevent DDoS Mitigation instances from being automatically deleted if you forget to manually renew them. The auto-renewal rules are as follows:

- The first auto-renewal date and billing period are calculated based on the expiration date of the DDoS Mitigation instance.

- The auto-renewal period of a DDoS Mitigation instance depends on the subscription duration. For example, if you select 3-month renewal duration, your DDoS Mitigation is automatically renewed for three months before each expiration.

- Auto-renewal can be enabled anytime before a DDoS Mitigation instance expires. The system attempts to automatically renew the instance at 03:00 seven days before the instance expires. If the fee deduction fails, there will be one attempt at 03:00 every day until the instance expires or the renewal is successful.

- After auto-renewal is enabled, you can still manually renew your DDoS Mitigation instance. After a manual renewal is complete, auto-renewal is still valid, and the renewal fee will be deducted from your account seven days before the new expiry date.

- By default, the system automatically deducts fees from your account 7 days before your instance expires. You can change the renewal payment date if needed, for example, 6 days or 5 days before the instance expires.
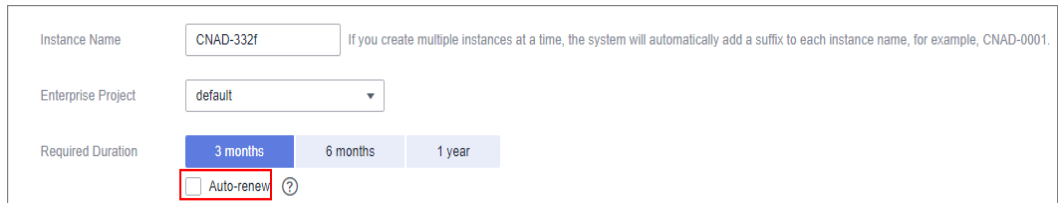
For details, see **Auto-Renewal Rules**.

Prerequisites

The yearly/monthly DDoS Mitigation instance has not expired.

Enabling Auto-Renewal on the Purchase Page

You can enable auto-renewal on the purchase page. The renewal period is the subscription period, as shown in **Figure 4-6**.

Figure 4-6 Auto-renewing DDoS Mitigation

Enabling Auto-renewal on the Renewal Page

Step 1 **Log in to the management console**.

Step 2 On the top navigation bar, choose **Billing and Costs** > **Renewal**. The **Renewal** page is displayed.

Figure 4-7 Renewal
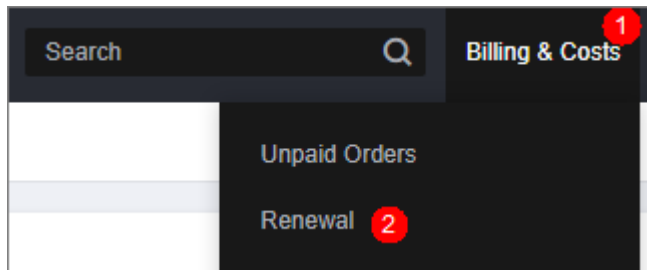
Step 3 Select the search criteria.

- On the **Auto Renewals** page, you can view the resources for which auto-renewal has been enabled.

- You can enable auto-renewal for resources on the **Manual Renewals**, **Pay-per-Use After Expiration**, and **Renewals Canceled** pages.

Step 4 Locate the target instance and click **Enable Auto-Renew** in the **Operation** column.

Step 5 Select the renewal duration and the number of auto-renewal times.

Step 6 Click **Enable**.

For more details, see **Enabling Auto-Renewal**.

----End

5 Bills

You can view the bill of a resource in the **Billing** section of Billing Center to learn about its usage and billing information in a certain period.

Bill Reporting Period

After yearly/monthly resources are paid, a bill is reported to the billing system for settlement.

The usage of pay-per-use resources is reported to the billing system at a fixed interval for settlement. The elastic protection bandwidth of AAD is billed by day based on the actual peak value of each day minus the basic protection bandwidth purchased by the customer.

The fee deduction time of pay-per-use resources may be later than the settlement period. On the **Billing Center** > **Billing** > **Transactions** and **Detailed Bills** > **Transaction Bills** page, **Expenditure Time** indicates the time when a pay-per-use product is used.

6 Arrears

Your account goes into arrears when the balance is less than the bill to be settled. To continue using DDoS Mitigation, top up your account in time.

Arrears Reasons

- Auto-renewal has been enabled, but your account balance is insufficient to pay for the renewal.
- You have purchased an AAD instance, and the peak attack traffic exceeds the basic protection bandwidth, incurring elastic protection bandwidth fees. In addition, the account balance is insufficient so that fees can be deducted.

Impact of Arrears

For a yearly/monthly DDoS instance, you have paid the instance fee in advance. Therefore, you can still use the existing DDoS instance resources even if your account is in arrears. However, you cannot perform other operations that may incur fees, such as upgrading specifications or renewing subscriptions.

Avoiding and Handling Arrears

You need to top up your account once it is in arrears.

If they are no longer used, you can delete the resources to stop billing.

Configure the **Balance Alert** function on the **Billing Center** > **Overview** page. When the total amount of the available quota, general cash coupons, and cash coupons is lower than the threshold, the system automatically notifies you by SMS or email.

If your account is in arrears, top up your account in time.

7 Stopping Billing

Yearly/Monthly Resources

You pay for a resource billed in yearly/monthly mode, such as a yearly/monthly DDoS Mitigation instance, when you purchase it. Billing automatically stops when the subscription expires.

- If a yearly/monthly resource is no longer needed before the subscription expires, you can unsubscribe from the resource. The system will return a certain amount of money to your account based on whether the resource is subject to five-day unconditional unsubscription or whether cash coupons or discount coupons are used. For details, see **Unsubscription**.

- If you have enabled the auto-renewal function, disable it before the auto-renewal deduction date (seven days before the expiration date by default) to avoid unexpected fees.
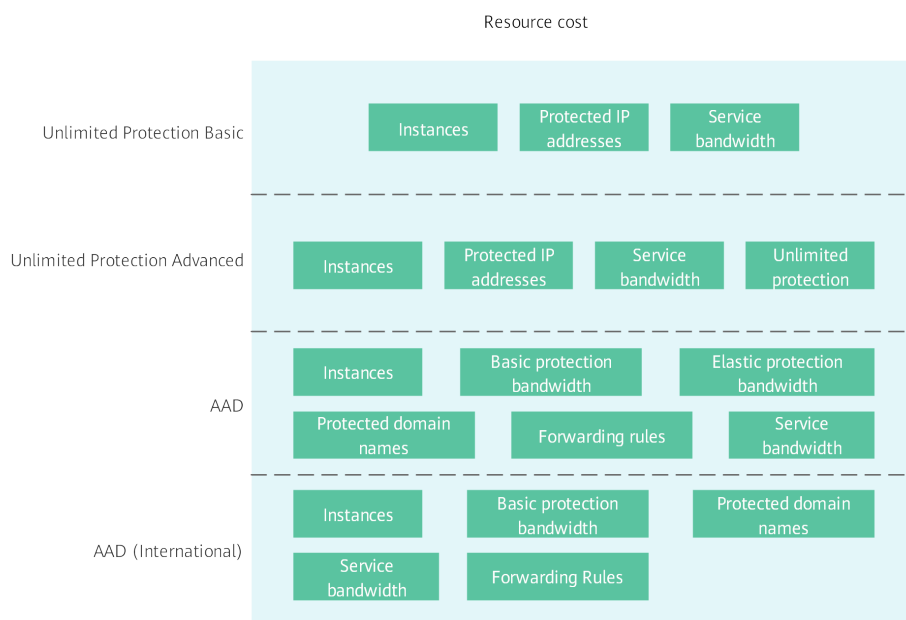
8 Cost Management

As you migrate more of your services to the cloud, managing cloud costs becomes more important. For example, you may be more concerned with cost management when using DDoS Mitigation. The following describes how to manage costs in terms of cost composition, allocation, analysis, and optimization. Optimizing costs can help you maximize return on investment.

Cost Composition

When you use the DDoS Mitigation service on Huawei Cloud, the costs are mainly resource costs, which depend on the billing items. For details, see **Billing Items**.

Figure 8-1 Resource costs

Resource cost

Unlimited Protection Basic

Instances | Protected IP addresses | Service bandwidth

Unlimited Protection Advanced

Instances | Protected IP addresses | Service bandwidth | Unlimited protection

AAD

Instances | Basic protection bandwidth | Elastic protection bandwidth

Protected domain names | Forwarding rules | Service bandwidth

AAD (International)

Instances | Basic protection bandwidth | Protected domain names

Service bandwidth | Forwarding Rules

Cost Allocation

A good cost accountability system is a prerequisite for cost management. It ensures that departments, business teams, and owners are accountable for their

respective cloud costs. An enterprise can allocate cloud costs to different teams or projects so as to have a clear picture of their respective costs.

Huawei Cloud **Cost Center** provides various tools for you to group costs in different ways. You can experiment with these tools and find a way that works best for you.

- **By linked account**

  The enterprise master account can manage costs by grouping the costs of its member accounts by linked account. For details, see **Viewing Costs by Linked Account**.

- **By enterprise project**

  Before allocating costs, enable Enterprise Project Management Service (EPS) and plan your enterprise projects based on your organizational structure or service needs. When purchasing cloud resources, select an enterprise project so that the costs of the resources will be allocated to the selected enterprise project. For details, see **Viewing Costs by Enterprise Project**.

- **By cost tag**

  You use tags to sort your Huawei Cloud resources in a variety of different ways, for example, by purpose, owner, or environment. The following is the process of managing costs by predefined tags (recommended).

  Figure 8-2 Adding a tag to an ECS
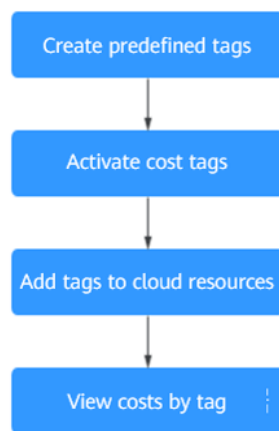
  For details, see **Viewing Costs by Cost Tag**.

- **By cost category**

  You can use **Cost Categories** provided by **Cost Center** to split shared costs. Shared costs are the costs of resources (compute, network, storage, or resource packages) shared across multiple departments or the costs that cannot be directly split by cost tag or enterprise project. These costs are not directly attributable to a singular owner, and they cannot be categorized into a singular cost type. In this case, you can define cost splitting rules to fairly allocate these costs among teams or business units. For details, see **Viewing Cost By Cost Category**.

Cost Analysis

To precisely control and optimize your costs, you need a clear understanding of what parts of your enterprise incurred different costs. **Cost Center** visualizes your original costs and amortized costs using various dimensions and display filters for cost analysis so that you can analyze the trends and drivers of your service usage and costs from a variety of perspectives or within different defined scopes.

You can also use **Cost Anomaly Detection** provided by **Cost Center** to detect unexpected expenses in a timely manner. In this way, costs can be monitored, analyzed, and traced.

For details, see **Performing Cost Analysis to Explore Costs and Usage** and **Enabling Cost Anomaly Detection to Identify Anomalies**.

Cost Optimization

- **Cost control**

  You can create different types of budgets on the **Budgets** page of Cost Center to track your costs against the budgeted amount you specified. If the budget thresholds you defined are reached, Cost Center will send alerts to the recipients you configured. You can also create budget reports and specify recipients to receive budget alerts if any at a frequency you configured.
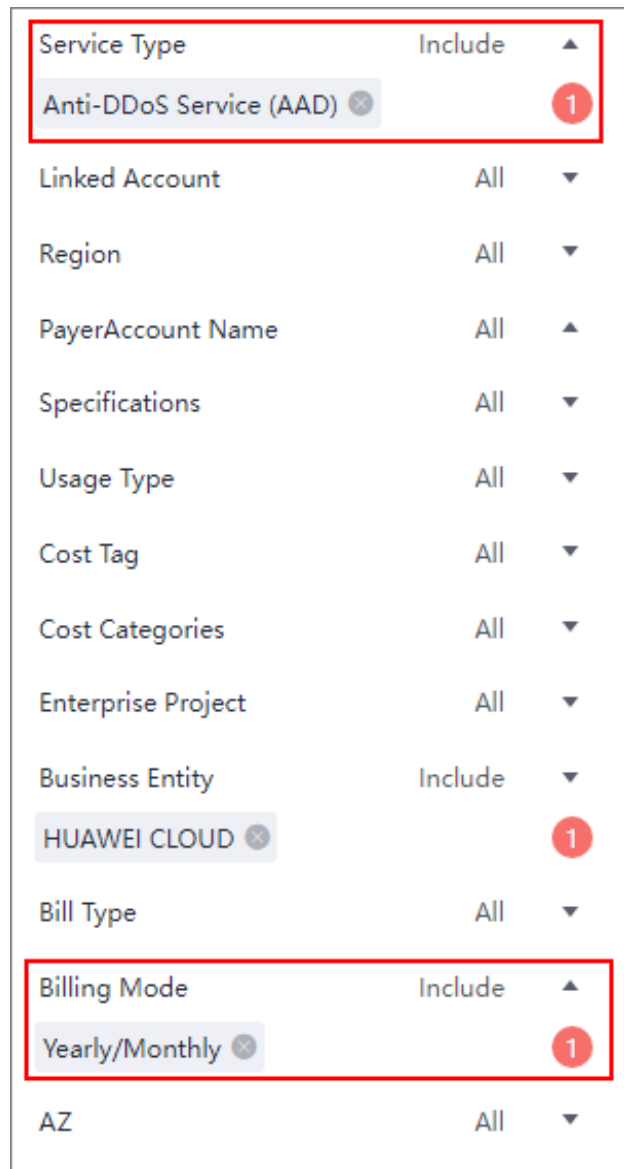
  For example, an enterprise needs to create a quarterly cost budget for DDoS Mitigation. The quarterly budget is 5,000 USD. The system should send an alarm when the forecast amount is greater than 80% of the budget amount. You can refer to the following budget information.
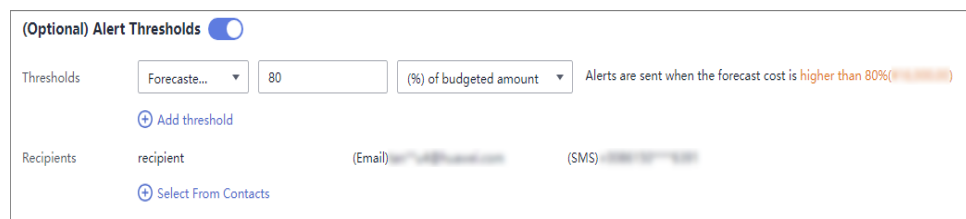
  Figure 8-3 Basic budget information

Figure 8-4 Defining the budget scope

Figure 8-5 Setting a budget alert

For details, see **Enabling Forecasting and Creating Budgets to Track Cost and Usage**.

- **Resource rightsizing**

  Cost Center can help monitor the historical expenditures and resource usage of the DDoS Mitigation service, identify idle resources, and provide optimization suggestions so that you can reduce costs as much as possible.

You can also identify resources with high costs based on the analysis results in the **cost analysis** phase and use Cloud Eye to monitor resource usage. By doing this, you can determine the causes of high costs and take optimization measures accordingly.

9 Billing FAQs

9.1 General FAQs

9.1.1 Will Traffic Be Forwarded and Charged After Protocol Blocking or Geo-Blocking Is Enabled?

Cloud Native Anti-DDoS Advanced: After protocol blocking or geo-blocking is enabled, traffic is still scrubbed and charged.

Advanced Anti-DDoS: After protocol blocking or geo-blocking is enabled, traffic is still scrubbed and charged.

9.2 Billing FAQs of AAD

9.2.1 How Is AAD Billed?

Pricing

To use AAD, you need to purchase AAD instances.

Billing Mode

AAD instances are charged by the service bandwidth, basic protection bandwidth, and elastic protection bandwidth you configure.

Table 9-1 Billing items

Billing Item	Billing Modes	Pricing details
Service Bandwidth	Prepaid by month or year	Service bandwidth for the AAD server room to forward scrubbed traffic to origin servers. **NOTE** If the AAD server room is outside HUAWEI CLOUD, it is recommended that the service bandwidth be greater than or equal to the egress bandwidth of the origin servers.
Basic Protection Bandwidth	Prepaid by month or year	Basic bandwidth for defending against attacks. Traffic that does not exceed this bandwidth will be scrubbed by AAD without incurring additional fees.
Elastic Protection Bandwidth	Postpaid by day	Maximum available bandwidth for defending against attacks. For details about the billing rules, see **How Is the Elastic Bandwidth Charged?**.

Billing details for elastic protection bandwidth:

- Billing standard: It depends on the peak attack traffic on the day. If multiple attacks occur on a day, only the attack with the peak traffic counts.

- Postpaid: Elastic protection fees are generated based on the attack traffic peak. If there is no attack, no elastic protection fee is generated.

- Specifications adjustment: You can adjust the elastic protection bandwidth on the AAD console. Once adjusted, the new elastic protection bandwidth takes effect immediately.

- Free-to-use: If the elastic protection bandwidth is set to the same value as the basic protection bandwidth, you do not need to pay for elastic protection.

9.2.2 Why Does My Payment Status Not Update After I Make a Payment?

If you have not received any payment information after making a payment, and the payment status on the platform is not updated, the possible causes may be as follows:

- Check whether the recharge number is correct in the transaction record.

- The payment SMS message sent by the carrier is delayed. Contact the carrier or Huawei customer service to query the payment status.

9.2.3 Will I Be Charged If I Buy an Elastic Protection Bandwidth and My Elastic IP Address Is Not Attacked for the Whole Month?

Yes, you will be charged for the basic protection bandwidth only.

9.2.4 What Happens If the Attack Traffic Exceeds the Elastic Protection Bandwidth?

A black hole will be triggered, which means access traffic to the IP address will be blocked.

9.2.5 Can I Adjust My Elastic Protection Bandwidth From 100 Gbit/s to 200 Gbit/s When I Find 100 Gbit/s Is Insufficient?

Yes. AAD supports dynamic adjustment of elastic protection bandwidth.

> **NOTICE**
>
> Adjusted bandwidth takes effect immediately. The charge depends on the peak attack traffic of the day.

9.2.6 What Is the Charge If My IP Address Is Attacked Many Times a Day?

You will be charged only once based on the peak attack traffic of the day (0:00 to 23:00). For example, if your IP address is attacked three times and the attack traffic is 50 Gbit/s, 100 Gbit/s, and 200 Gbit/s, you will be charged based on 200 Gbit/s.

9.2.7 How Do I Stop Elastic Protection to Avoid Being Charged for the Elastic Protection Bandwidth?

Set the elastic protection bandwidth to the same value as the basic protection bandwidth.

9.2.8 How Can I Renew the AAD Service?

You can renew an AAD instance on the AAD management console.

> **NOTICE**
>
> Ensure that the account used for renewing the AAD instance has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.
>
> - **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
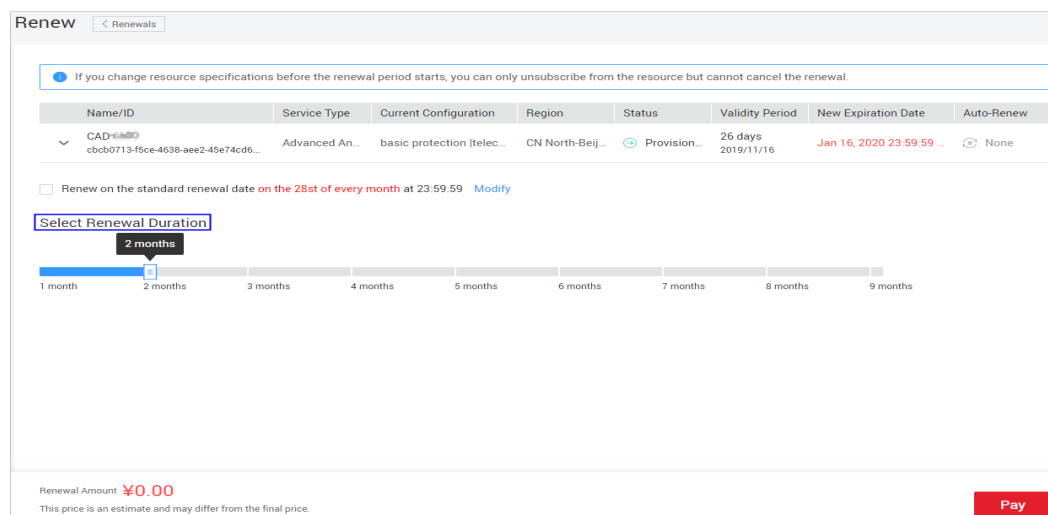> - **Tenant Administrator**: has all permissions on all services except on IAM.

Step 1 Log in to the management console.

Step 2 Select a region in the upper part of the page, click ☰ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS** page is displayed.

Step 3 In the navigation pane on the left, choose **Advanced Anti-DDoS > Instance List**. The **Instance List** page is displayed.

Step 4 Click **Renew** under the instance name.

Step 5 On the **Renew** page, select a renewal duration and click **Pay** to complete the payment.

----**End**

9.2.9 How Can I Unsubscribe from the AAD Service?

The AAD service does not support unconditional unsubscription. If the unsubscription conditions are met, contact the customer service to apply for unsubscription

Unsubscription Conditions

If the service does not match your business requirements during your purchase or use, contact the customer service personnel to unsubscribe from the service. For example, if your servers are deployed outside China but you have purchased the

AAD service from the Chinese Mainland region, the AAD service cannot be used and in this case you can apply for service cancellation.

An AAD instance that has been put to use does not allow cancellation.

9.2.10 How Should I Automatically Renew AAD?

You can enable auto renewal for your AAD instance. The system automatically renews your service subscription according to the required duration specified in your previous purchase upon expiration of the service.

> **NOTICE**
>
> Ensure that the account for which the automatic renewal is to be enabled has both the CAD Administrator and BSS Administrator roles or has the Tenant Administrator role.
>
> - **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
> - **Tenant Administrator**: has all permissions on all services except on IAM.

If you are currently purchasing AAD, you can enable the auto renewal function as follows:

1. When purchasing AAD, you can tick the **Auto-renew** option to configure automatic renewal.

   The procedure is as follows:

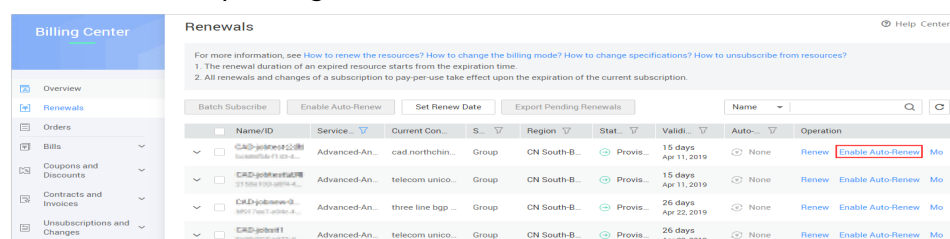   Choose **Buy AAD** > **Required Duration** > **Auto-renew**.

If you have purchased AAD, you can enable the auto renewal function as follows:

1. Go to the **Renewals** page, configure automatic renewal.

   The procedure is as follows:

   a. Log in to the management console and click **Fees** at the top right.

      The **Billing Center** page is displayed.

   b. In the navigation pane on the left, choose **Renewals**.

   c. Select the corresponding AAD instance for automatic renewal.

9.2.11 Can the Original Configuration Data Be Saved After I Unsubscribe from an AAD Instance?

No. After you unsubscribe from an AAD instance, it will not keep your original configuration data. Therefore, you need to connect your services to the newly-purchased AAD instance.

For details about unsubscription, see **How Can I Unsubscribe from the AAD Service?**.

To connect a service to the AAD, perform the following steps:

- If your system provides services through a domain name, you need to modify the DNS configuration to resolve the domain name to the CNAME record provided by Huawei Cloud.

- If your system provides services through an IP address, change the IP address to a high-defense IP address.

9.2.12 How Is the Elastic Bandwidth Charged?

Billing Description

The elastic bandwidth of AAD instances is charged based on the peak traffic of DDoS attacks on the current day. The fees in different scenarios are described as follows:

- Peak DDoS attack traffic on the current day ≤ Basic protection bandwidth: No elastic protection bandwidth fee is generated.

- Basic protection bandwidth < Peak DDoS attack traffic on the current day < Elastic protection bandwidth: Elastic protection bandwidth fees will be generated.

- If the peak DDoS attack traffic on the current day is greater than or equal to the configured elastic protection bandwidth, you will be charged for the elastic protection bandwidth.

Billing Examples

- Basic protection bandwidth < Peak attack traffic < Elastic protection bandwidth: **Elastic protection bandwidth usage (billed) = Peak attack traffic on the current day – Basic protection bandwidth**

- Peak attack traffic ≥ Elastic protection bandwidth: **Elastic protection bandwidth usage (billed) = Elastic protection bandwidth – Basic protection bandwidth**

For example, for three AAD instances, each has a basic protection bandwidth of 20 Gbit/s and an elastic protection bandwidth of 100 Gbit/s. If the three instances are under multiple DDoS attacks on the same day, the billing rules of the elastic protection bandwidth are as follows:

Table 9-2 Billing rules

Instance	Peak Attack Traffic	Generate Fee	Description
Instance A	20Gbps	No	The peak attack traffic does not exceed the basic protection bandwidth, no fee is generated.
Instance B	80Gbps	Yes	Billed protection bandwidth: 80 Gbit/s - 20 Gbit/s = 60 Gbit/s.
Instance C	120Gbps	Yes	120 Gbit/s is greater than the elastic protection bandwidth 100 Gbit/s. Billable protection bandwidth: 100 Gbit/s - 20 Gbit/s = 80 Gbit/s.