

# Situation Awareness

## FAQs

**Issue** 06  
**Date** 2023-06-08



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

---

# Contents

---

<b>1 Product Consulting</b>	<b>1</b>
1.1 What Does SA Do?	1
1.2 Why Is There No Attack Data or Only A Small Amount of Attack Data?	1
1.3 What Is the Data Source of Situation Awareness?	1
1.4 How Do I Get Information About the Most Vulnerable Assets?	2
1.5 What Are the Dependencies and Differences Between SA and Other Security Services?	2
1.6 What Are the Differences Between SA and HSS?	4
1.7 Why Cannot the Total ECS Quota Be Less Than the Number of Existing ECSs?	5
1.8 Can SA Be Used Across Accounts?	6
1.9 How Do I Update My Security Score?	6
1.10 How Do I Handle a Brute-force Attack?	7
1.11 How Do I Assign Operation Permissions to an Account?	8
1.12 How Do I Handle the 403 forbidden Error Reported by SA?	10
1.13 Why Is the Event Data in SA Inconsistent with That in WAF and HSS?	11
1.14 What Are Differences Between SA and SecMaster?	11
<b>2 Purchase Consulting</b>	<b>13</b>
2.1 How Do I Change the SA Specifications?	13
<b>3 Regions and AZs</b>	<b>15</b>
3.1 What Are Regions and AZs?	15
3.2 Can I Use SA Across Regions?	16

# 1 Product Consulting

---

## 1.1 What Does SA Do?

Situation Awareness (SA) is a security management and situation analysis platform of Huawei Cloud. SA comprehensively analyzes attack events, threat alarms, and attack sources by leveraging the big data technique, making it simple for you to understand security situation across all your cloud assets.

For more details, see [Features](#).

## 1.2 Why Is There No Attack Data or Only A Small Amount of Attack Data?

SA can detect a variety of attacks on assets and presents them objectively. If your assets are exposed to little risks, such as port exposure and weak passwords, on the Internet, the attack possibility will greatly reduce and there will be no or little data on SA.

If you believe that SA fails to reflect the attack status of your system, feel free to provide feedback to our customer service.

For details, see [How SA Works](#) and [Functions](#).

## 1.3 What Is the Data Source of Situation Awareness?

Based on the threat data collected from the cloud and other services, SA analyzes and displays the threat posture through big data mining and machine learning, and provides protection suggestions.

- SA presents overall security posture and generates threat alarms by obtaining network-wide traffic data and logs of security protection devices and using AI and big data technologies to analyze the obtained data.
- Additionally, SA aggregates alarm data from other security services, such as Host Security Service (HSS) and Web Application Firewall (WAF). Based on obtained data, SA then performs big data mining, machine learning, and

intelligent AI analysis to identify attacks and intrusions, helping you understand the attack and intrusion processes and providing related protection suggestions.

By analyzing security data that covers every aspect of your services, SA makes it easier for you to understand comprehensive security situation of your services and make informed decisions and handle security events in a timely manner.

For details, see [How SA Works](#).

## 1.4 How Do I Get Information About the Most Vulnerable Assets?

By viewing asset statistics, you can quickly know which assets are most vulnerable and learn details about threats to those assets.

If you are using standard or professional SA, you can view vulnerable assets on the **Resource Manager** page. This function is not included in the basic edition.

For details, see [Resource Manager](#).

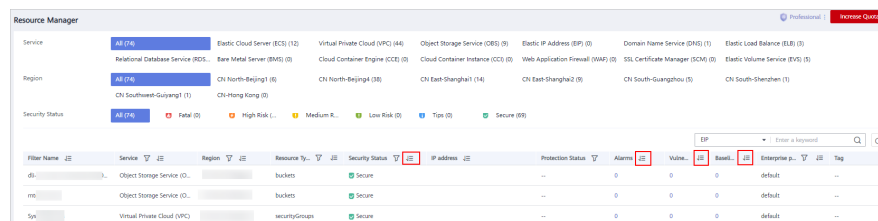
### Procedure

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

**Step 2** Click  in the upper left of the page and choose **Security & Compliance > Situation Awareness > Resource Manager**.

Click the sorting button in the **Security Status, Alarms, Vulnerabilities, or Baseline** column to display assets to meet your needs.

**Figure 1-1** Resource statistics by severity



----End

## 1.5 What Are the Dependencies and Differences Between SA and Other Security Services?

SA can work with other security services such as WAF, HSS, Anti-DDoS, and DBSS.

- How SA Works With Other Services

SA is a security management service that depends on other security services to provide threat detection data so that it can analyze security threat risks, display the global security threat posture, and provide informed suggestions.

Other security services report detected threats to SA and SA aggregates the received data to display the global security posture.

- Differences Between SA and Other Security Services

SA: It is only a visualized threat detection and analysis platform and does not implement any specific protective actions. It must be used together with other security services.

Other security services display the event data detected by themselves only. They can take specific protective actions, but cannot display global threat posture.

**Table 1-1** summarizes SA and other security services.

**Table 1-1** Differences between SA and other services

Service Name	Service Category	Dependency and Difference	Protected Object	Function Details
SA	Security management	SA displays the global security situation, analyzes threat data from other security services and cloud security threats, and provides protection suggestions.	Global security situation	<a href="#">SA Features</a>
Anti-DDoS	Network security	Anti-DDoS detects and defends against DDoS attacks. It synchronizes attack logs and protection data to SA.	Service stability	<a href="#">Anti-DDoS Features</a>
Host Security Service (HSS)	Host security	HSS detects server risks and protects servers with protection policies. It synchronizes alarms and protection data to SA.	Servers	<a href="#">HSS Functions and Features</a>
WAF	Application security	WAF detects and protects website service traffic in multiple dimensions to defend against common attacks and block threats. It synchronizes intrusion logs and alarm data to SA so that SA can display the network-wide security posture.	Web applications	<a href="#">WAF Functions</a>
DBSS	Data security	DBSS protects and audits database access behavior. It synchronizes audit logs and alarm data to SA.	Cloud databases	<a href="#">DBSS Service Overview</a>

## 1.6 What Are the Differences Between SA and HSS?

### Service Positioning

- Situation Awareness (SA) is a GUI-based security management platform for threat detection and analysis. SA focuses on the security threat attack posture of all your cloud assets. By aggregating detection results or events from many security products and analyzing threat data and cloud security threats, it helps you build a security system covering all your cloud assets.
- Host Security Service (HSS) is designed to protect server workloads in hybrid clouds and multi-cloud data centers. It protects servers and containers and prevents web pages from malicious modifications.

In short, SA presents the comprehensive view of security posture, and HSS secures servers and containers.

### Function Differences

- SA aggregates network-wide security data (including alarm data from other security services such as HSS, WAF, and Anti-DDoS) and uses analysis technologies such as big data, AI, and machine learning to display asset security posture by asset, threat alarm, and baseline inspection.
- HSS uses technologies such as AI, machine learning, and deep algorithms to analyze server risks through agents installed on protected servers. It delivers inspection and protection tasks through the console. Through the HSS console, you can manage the security information reported by the agent.

**Table 1-2** Differences between SA and HSS functions

Function		Common Function	Difference
Asset security	Servers	Both can display the overall security posture of servers.	<ul style="list-style-type: none"> <li>• SA synchronizes server risk data from HSS and then displays overall server security posture.</li> <li>• HSS scans accounts, ports, processes, web directories, software information, and automatic startup tasks on servers and displays server security posture.</li> </ul>
	Websites	None	<ul style="list-style-type: none"> <li>• SA checks and scans the overall security posture of website assets from different dimensions.</li> <li>• HSS does not support this function.</li> </ul>

Function		Common Function	Difference
Baseline inspection	Cloud service baseline	None	<ul style="list-style-type: none"> <li>SA can help you check key configurations of cloud services you enabled based on built-in checks that are included in <b>Cloud Security Compliance Check 1.0</b> and <b>Network Security</b>.</li> <li>HSS does not support this function.</li> </ul>
	Unsafe server settings	None	<ul style="list-style-type: none"> <li>SA does not support this function.</li> <li>HSS checks your baseline settings, including checking for weak passwords, and reviewing security policies and configuration details. HSS provides an overview of your configuration security rating, the top 5 configuration risks, detected weak passwords, and the top 5 servers with weak passwords configured.</li> </ul>

## 1.7 Why Cannot the Total ECS Quota Be Less Than the Number of Existing ECSs?

The total ECS quota is the total number of hosts that are authorized to receive detections. When buying SA, ensure that the total ECS quota is greater than or equal to the total number of hosts under the current account. If the total ECS quota is less than the number of hosts, the following impact may occur:

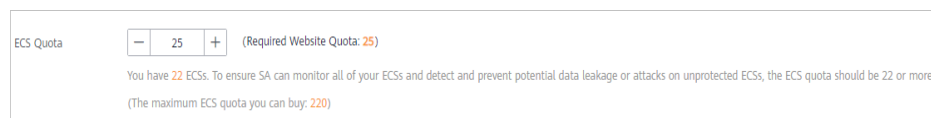
- Unauthorized hosts cannot detect threats in a timely manner after being attacked, resulting in risks such as data leakage.

### Procedure

Log in to the SA console and click **Upgrade**. Configure the total ECS quota based on the planning or the number of existing hosts.

For details, see [Buying the SA Professional Edition](#).

**Figure 1-2** Total ECS Quota



#### NOTE

If the total number of ECSs under an account exceeds the total ECS quota, increase the total ECS quota and change the specifications. For details, see [How Do I Change the Specifications of My Professional SA?](#)



## 1.8 Can SA Be Used Across Accounts?

No.

SA cannot be used across accounts. You can only obtain and manage threat risk data of resources under your current account.

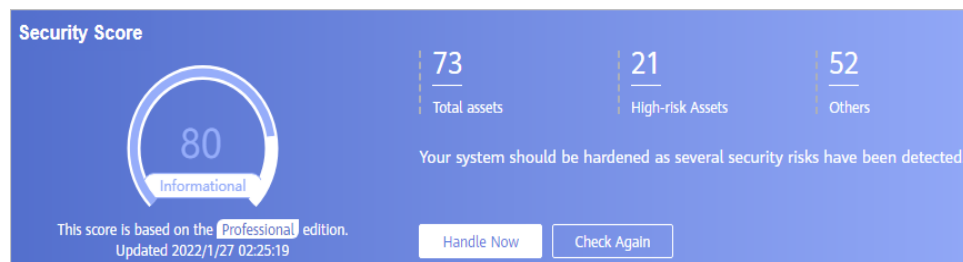
However, all authorized IAM users under an account can share the global threat risk information of the account.

## 1.9 How Do I Update My Security Score?

SA checks your asset health in real time, evaluates the overall security posture, and gives you a security score. A security score helps you quickly understand the overall status of unhandled risks to your assets.


After asset security risks are fixed, manually ignore or handle alarm events and update the alarm event status in the alarm list. The risk severity can be down to a proper level accordingly. Your security score will be updated after you refresh the alarm status and check your environment again.

**Figure 1-3** Security Score



### Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Situation Awareness > Events**.

**Step 3** Ignore an alarm event.

In the **Operation** column of the alarm event, click **Ignore**. The alarm event status changes to **Ignored**.

**Step 4** Mark an alarm event as offline processing.

1. In the **Operation** column of the alarm event, click **Mark as Offline**.
2. In the displayed dialog box, provide details of **Handler**, **Handled**, and **Results**.
3. In the displayed confirmation dialog box, click **OK**. The status of the alarm event changes to **Handled Offline**.

**Step 5** After the alarm event is marked (or handled), return to the **Security Overview** page and click **Check Again**. The security score will be updated then.

 **NOTE**

It takes some time for a check to finish. You can refresh the page to get the new security score five minutes after you start the recheck.

----End

For more details about security scoring, see [Security Overview](#).

## 1.10 How Do I Handle a Brute-force Attack?

Brute-force attacks are common intrusion behavior. Attackers guess and try login usernames and passwords remotely. When they succeed, they can attack and control systems.

SA interworks with HSS to receive alarms for brute force attacks detected by HSS and centrally display and manage alarm events.

### Handling Alarm Events

HSS uses brute-force detection algorithms and an IP address blacklist to effectively prevent brute-force attacks and block attacking IP addresses. Alarm events will be reported.

If you receive an alarm event from HSS, log in to the HSS console to confirm and handle the alarm event.


- If your host is cracked and an intruder successfully logs in to the host, all hosts under your account may have been implanted with malicious programs. Take the following measures to handle the alarm event immediately to prevent further risks to the hosts:
  - a. Check whether the source IP address used to log in to the host is trusted immediately.
  - b. Change passwords of accounts involved.
  - c. Scan for risky accounts and handle suspicious accounts immediately.
  - d. Scan for malicious programs and remove them, if any, immediately.
- If your host is cracked and the attack source IP address is blocked by HSS, take the following measures to harden host security:
  - a. Check the source IP address used to log in to the host and ensure it is trusted.
  - b. Log in to the host and scan for OS risks.
  - c. Upgrade the HSS protection capability if it is possible.
  - d. Harden the host security group and firewall configurations based on site requirements.

For details, see [How Do I Handle a Brute-Force Attack Alarm?](#)

### Marking Alarm Events

After an alarm event is handled, you can mark the alarm event.

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Situation Awareness > Threat Alarms**.

**Step 3** On the **Alarms** tab, select **Brute-force attacks** and refresh the alarm list.

**Step 4** Select an alarm and mark it as handled.

----End

For details, see [Viewing Alarms](#).

## 1.11 How Do I Assign Operation Permissions to an Account?

To use functions in **Baseline Inspection**, **Resource Manager**, and **Logs** modules, your account must have the **Tenant Administrator** permission and IAM-related permissions.

This topic describes how to configure permissions to use a specific SA function.

- [Configuring Permissions to Use Baseline Inspection](#)
- [Configuring Permissions to Use Resource Manager and Logs](#)

### Prerequisites

You have obtained the administrator account and its password.

### Configuring Permissions to Use Baseline Inspection

To use Baseline Inspection, you need to configure permissions and policies as described in the following steps. Do not select other permissions or policies, or this function may still be unavailable after the configuration.

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

**Step 2** Click  in the upper left corner of the page and choose **Management & Governance > Identity and Access Management**.

**Step 3** Add IAM-related permissions.

1. In the navigation pane on the left, choose **Permissions > Policies/Roles**. In the upper right corner of the displayed page, click **Create Custom Policy**.
2. Configure a policy.
  - a. **Policy Name:** Enter a policy name.
  - b. **Scope:** Select **Global services**.
  - c. **Policy View:** Select **JSON**.
  - d. **Policy Content:** Copy the following content and paste it in the text box.

```
{  
  "Version": "1.1",  
  "Statement": [  
    {  
      "Action": "iam:CreatePolicy",  
      "Resource": "arn:aws:iam::*:policy/*",  
      "Effect": "Allow",  
      "Principal": "*" } ]  
}
```

```
"Effect": "Allow",
"Action": [
  "iam:users:getUser",
  "iam:securitypolicies:getLoginPolicy",
  "iam:credentials:listCredentials",
  "iam:users:getUserLoginProtect",
  "iam:agencies:listAgencies",
  "iam:securitypolicies:getProtectPolicy",
  "iam:users:listUsers",
  "iam:securitypolicies:getPasswordPolicy",
  "iam:groups:listGroups",
  "iam:permissions:listRolesForAgencyOnProject",
  "iam:users:listUsersForGroup",
  "iam:projects:listProjectsForUser",
  "iam:permissions:listRolesForAgencyOnDomain"
]
}
```

3. Click **OK**.

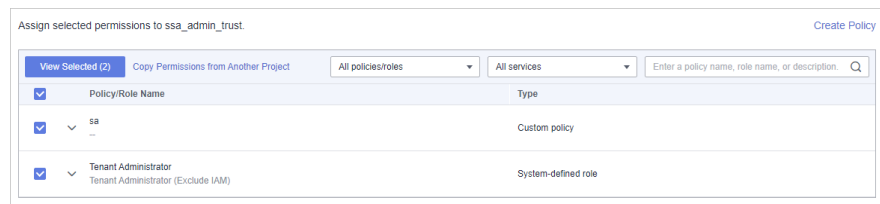
**Step 4** In the navigation pane on the left, choose **Agencies**.

**Step 5** In the agency list, select **ssa\_admin\_trust** to go to the details page.

**Step 6** Click the **Permissions Assigned** tab and click **Assign**.

**Step 7** In the permission configuration area, search for and select **Tenant Administrator** and the permission created in [Step 3](#).

**Figure 1-4** Baseline inspection permissions - Example



**Step 8** Click **Next** in the lower part of the page and set the minimum authorization scope.

**Step 9** Click **OK**.

----End

## Configuring Permissions to Use Resource Manager and Logs

To use Baseline Inspection, you need to configure permissions and policies as described in the following steps. Do not select other permissions or policies, or this function may still be unavailable after the configuration.

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

**Step 2** Click  in the upper left corner of the page and choose **Management & Governance > Identity and Access Management**.

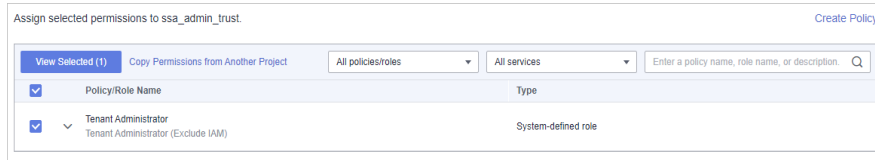
**Step 3** In the navigation pane on the left, choose **Agencies**.

**Step 4** In the agency list, select **ssa\_admin\_trust** to go to the details page.

**Step 5** Click the **Permissions Assigned** tab and click **Assign**.

**Step 6** In the permission configuration area, search for and select **Tenant Administrator**.

**Figure 1-5** Resource Manager permissions



**Step 7** Click **Next** in the lower part of the page and set the minimum authorization scope.

**Step 8** Click **OK**.

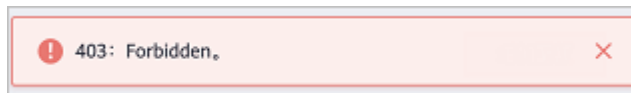
----End

## 1.12 How Do I Handle the 403 forbidden Error Reported by SA?

### Symptom

A 403 Forbidden error as shown in the following figure was returned when a user accessed the **Threat Alarms** page.

**Figure 1-6** Error 403



### Possible Cause

The IAM account had only **SA Full Access** or **SA ReadOnlyAccess** permissions assigned. To access the page, the account must have **Tenant Guest** permissions.

#### NOTE

Currently, the **SA FullAccess** or **SA ReadOnlyAccess** permission can be used only when you have the **Tenant Guest** permission. The details are as follows:

- Configure all SA permissions: **SA FullAccess** and **Tenant Guest**.

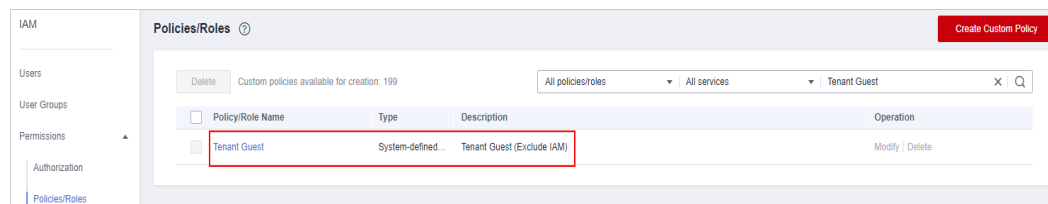
To use **SA Resource Manager** and **Baseline Inspection**, configure the following permissions:

- **Resource Manager**: Configure **SA FullAccess** and **Tenant Administrator**. For details, see [How Do I Assign Operation Permissions to an Account?](#)
- **Baseline Inspection**: Configure **SA FullAccess**, **Tenant Administrator**, and IAM permissions. For details, see [How Do I Assign Operation Permissions to an Account?](#)
- Configure SA read-only permissions: Configure **SA ReadOnlyAccess** and **Tenant Guest**.

## Solution

Use the administrator account to assign **Tenant Guest** permissions to the IAM account.

**Figure 1-7** Tenant Guest



For details about **Tenant Guest** permissions, see [System Permissions](#). To assign **Tenant Guest** permissions to an IAM account, **add the IAM account to a user group** and **assign the permissions to the group**.

## 1.13 Why Is the Event Data in SA Inconsistent with That in WAF and HSS?

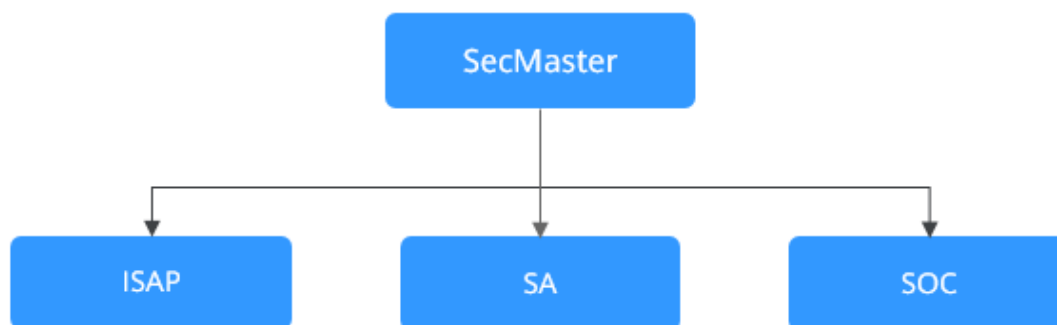
SA aggregates all historical alarm data reported by WAF and HSS, but WAF and HSS display real-time alarm data. As a result, data in SA is inconsistent with that in WAF and HSS.

Therefore, you are advised to go to the corresponding service (WAF or HSS) to view and handle the problem.

## 1.14 What Are Differences Between SA and SecMaster?

Situation Awareness (SA) and SecMaster are security management services provided by Huawei Cloud.

**Figure 1-8** SA and SecMaster



SecMaster integrates Situation Awareness (SA), Intelligent Security Analysis Platform (ISAP), and Security Operations Center (SOC).

- SecMaster is Huawei's next-generation cloud-native security operations center.

Combined with Huawei Cloud years of experience in security and based on cloud-native security capabilities, SecMaster provides cloud asset management, security posture management, security information and incident management, security orchestration, automatic responses, and other functions, helping you implement integrated and automatic security operations management.

- Situation Awareness (SA) is a security management and situation analysis platform of Huawei Cloud.

It gives you a comprehensive overview of your global security situation by leveraging the big data analysis technologies, making it easier for you to analyze attack events, threat alarms, and attack sources.

- Intelligent Security Analysis Platform (ISAP) is a data middle-end system for security operations analysis and modeling.

It supports collection of cloud service security logs, data retrieval, and intelligent modeling and provides professional security analysis capabilities to protect cloud workloads, applications, and data.

- Security Operations Center (SOC) is an operations platform that quickly responds to risky elements, threats, and vulnerabilities during security operation activities on the cloud. It works with the Security Operations, Analytics, and Response (SOAR) system to orchestrate, automate, manage, and control security risks on the cloud.

SOC provides a workbench entry based on a complete security operations service framework. You can use SOC to centrally manage security assets and policies, orchestrate automated responses, and handle security operations workflows.

# 2 Purchase Consulting

---

## 2.1 How Do I Change the SA Specifications?

If the number of your assets increases after SA is purchased, you need to increase **ECS Quota** to get your new assets protected.


---

### NOTICE

- The basic edition does not support unsubscription.
  - The standard edition **cannot** be directly upgraded to the professional edition, and the professional edition **cannot** be directly changed to the standard edition. To use a different edition, unsubscribe from the current edition first.
  - The standard edition can only be billed on a yearly or monthly basis.
  - Only one edition can be used within an account. Purchasing some asset quotas in the standard edition and other asset quotas in the professional edition is not supported.
- 

### Changing the Specifications of Yearly/Monthly SA

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Situation Awareness**.

**Step 3** Click **Increase Quota** in the upper right corner of the page.

**Step 4** Check the current configuration of your SA edition.

**Step 5** Select **Yearly/Monthly** for **Billing Mode**.

**Step 6** Specify **ECS Quota** and confirm **Required Duration**.



 **NOTE**

- **Required Duration** you configured during the increase of **ECS Quota** applies only to the increased quota. This required duration does not affect the quota you purchased in the original order.
- The **Price** is calculated based on the increased quota and required duration. The existing quotas will not be charged again.

**Step 7** After the configuration is complete, click **Next**.


**Step 8** On the **Details** page, confirm the order information, read the *Situation Awareness Disclaimer*, select the check box before "I have read and agree to the Situation Awareness Disclaimer", and click **Pay Now**.

**Step 9** After you complete the payment, go back to the SA console and check the new specifications.

----End

## Changing the quotas of Pay-Per-Use SA

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Situation Awareness**.

**Step 3** Click **Increase Quota** in the upper right corner of the page.

**Step 4** Check the current configuration of your SA edition.

**Step 5** Select **Pay-per-use** for **Billing Mode**. In pay-per-use billing mode, you are billed by the hour.

From the time when the service is enabled to the time when the service is canceled, you are billed for the actual duration by the hour.

**Step 6** Specify **ECS Quota**.

**Step 7** After the configuration is complete, click **Next**.

**Step 8** On the **Details** page, confirm the order information, read the *Situation Awareness Disclaimer*, select the check box before "I have read and agree to the Situation Awareness Disclaimer", and click **Pay Now**.

**Step 9** Go back to the SA console and check the new specifications in the edition management window.

----End

# 3 Regions and AZs

## 3.1 What Are Regions and AZs?

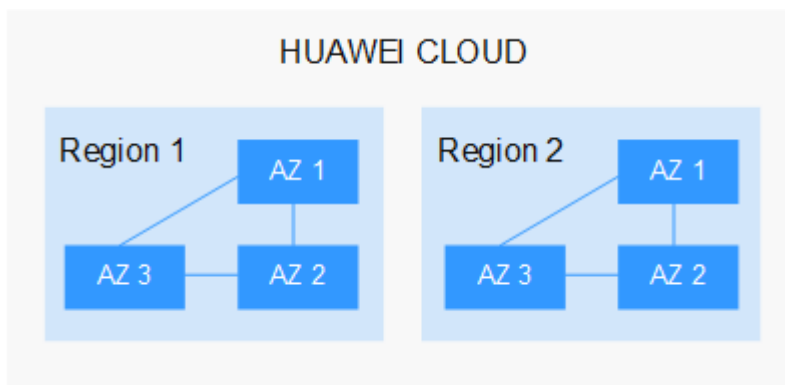
### Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

**Figure 3-1** shows the relationship between the regions and AZs.

**Figure 3-1** Region and AZ



Huawei Cloud provides services in many regions around the world. You can select a region and AZ as needed.

## Selecting a Region

When selecting a region, consider the following factors:

- Location  
You are advised to select a region close to you or your target users. This reduces network latency and improves access rate.
  - If you or your users are in the Asia Pacific region and outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your users are in Africa, select the **AF-Johannesburg** region.
  - If you or your users are in Latin America, select the **LA-Santiago** region.
- Resource price  
Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

## Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

## Regions and Endpoints

Before using an API to call resources, specify its region and endpoint.

## 3.2 Can I Use SA Across Regions?

Yes.

SA is a global service. You can use it without switching between regions.

---

### NOTICE

While, baseline inspection and log management (stored to OBS) are not supported in some regions. For details, see the prompts on the management console.

---