

Situation Awareness

User Guide

Issue 02
Date 2023-04-24



Copyright © Huawei Technologies Co., Ltd. 2023. 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 Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks 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 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

1 Service Overview	1
1.1 What Is Situation Awareness?	1
1.2 Features	1
1.3 Application Scenarios	7
1.4 Edition Differences	7
1.5 Billing	9
1.6 Basic Concepts	9
1.7 Permissions Management	11
1.8 SA and Other Services	12
2 Edition Upgrade	13
3 Permissions Management	15
3.1 Creating a User and Granting Permissions	15
3.2 SA Custom Policies	17
3.3 SA Permissions and Supported Actions	18
4 Editions	19
4.1 Increasing Asset Quotas	19
4.2 Unsubscribing from SA	20
5 Security Overview	21
5.1 Overview	21
5.2 Security Score	25
6 Resource Manager	27
7 Threat Alarms	30
7.1 Threat Alarms Overview	30
7.2 Viewing Alarms	33
7.3 Viewing Threat Analysis	35
7.4 Handling Alarms and Events	35
7.4.1 Brute Force Attacks	35
7.4.2 Web Attacks	38
7.4.3 Trojan	38
7.4.4 Exploits	38
7.4.5 Zombie	39

7.4.6 Command and Control.....	40
7.4.7 Abnormal Behavior.....	40
8 Baseline Inspection.....	42
8.1 Cloud Service Baseline Overview.....	42
8.2 Configuring Permissions to Use Baseline Inspection.....	42
8.3 Configuring a Baseline Inspection Plan.....	44
8.4 Executing a Baseline Inspection Plan.....	46
8.5 Performing a Manual Check.....	48
8.6 Viewing Baseline Inspection Results.....	49
8.7 Handling Baseline Inspection Results.....	52
9 Events.....	56
9.1 Viewing Events.....	56
9.2 Handling Events.....	57
9.3 Exporting Events.....	58
9.4 Customizing the Event List.....	59
9.5 Managing Filters.....	59
10 Logs.....	62
11 Integrations.....	64
11.1 Managing Integrations.....	64
11.2 Viewing Integrations.....	65
11.3 Checking the Connection Status of an Integration.....	66
12 Settings.....	68
12.1 Check Settings.....	68
13 FAQs.....	70
13.1 Product Consulting.....	70
13.1.1 What Does SA Do?.....	70
13.1.2 Why Is There No Attack Data or Only A Small Amount of Attack Data?.....	70
13.1.3 What Is the Data Source of Situation Awareness?.....	70
13.1.4 How Do I Get Information About the Most Vulnerable Assets?.....	71
13.1.5 What Are the Dependencies and Differences Between SA and Other Security Services?.....	71
13.1.6 Why Cannot the Total ECS Quota Be Less Than the Number of Existing ECSs?.....	72
13.1.7 How Do I Update My Security Score?.....	73
13.1.8 How Do I Handle a Brute-force Attack?.....	74
13.1.9 How Do I Assign Operation Permissions to an Account?.....	75
13.1.10 Why Is the Event Data in SA Inconsistent with That in WAF and HSS?.....	77
13.2 Purchase Consulting.....	77
13.2.1 How Do I Change the SA Specifications?.....	77
13.2.2 How Is SA Billed?.....	77
13.2.3 How Do I Cancel My Subscription to SA?.....	77
13.2.4 Can I Use SA for Free?.....	78

A Change History..... 79

1 Service Overview

1.1 What Is Situation Awareness?

Situation Awareness (SA) is a visualized threat detection and analysis platform. SA 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.

How SA Works

SA collects network-wide traffic data and security device logs and identifies threat alarms using a big data analysis platform. You can count on SA to make better informed decisions on handling security events.

1.2 Features

With SA, you can manage security posture of all your cloud assets in one place. SA provides many functional modules, including [Security Overview](#), [Resource Manager](#), [Threat Alarms](#), [Baseline Inspection](#), [Events](#), [Logs](#), and [Integrations](#).

Security Overview

The **Security Overview** page gives you a comprehensive overview of your asset security posture together with other linked cloud security services to collectively display security assessment findings.

Table 1-1 Security Overview Functions

Function Module	Description
Security Score	SA evaluates and scores your cloud asset security. You can quickly learn of unhandled risks and their threats to your assets. The lower the security score, the greater the overall asset security risk.
Security Monitoring	You can view how many threats, vulnerabilities, and compliance violations that are not handled and view their details.
Your Security Score over Time	You can view your security scores for the last 7 days.

Resource Manager

SA displays the real-time security status of assets on the cloud.

Table 1-2 Resources functions

Function Module	Description
Resource Manager	SA synchronizes the security status statistics of all resources in the current account. You can quickly locate unhealthy resources and find the solutions by viewing the resource name and security status as well as cloud services involved.

Threat Alarms

In this module, SA reports alarms based on real-time monitoring, displays details of alarms for the last 180 days, and defends against typical threats by using varied preset protection policies.

SA can detect and display varied types of threats, including distributed denial of service (DDoS) attacks, brute-force attacks, web attacks, Trojans, zombie computers, Command-and-Control (C&C) attacks, abnormal behavior, and exploits.

Table 1-3 Function modules in Threat Alarms

Function Module	Description
Alarms	SA lists statistics on threat alarms. You can view details of threat alarms and details of threatened assets. You can also export all alarms.
Threat Analysis	SA allows you to query threats or attacks by Attack source or Attacked asset .
Alarm Monitoring	SA allows you to customize the threat list, alarm type, and risk severity to view only concerned threat alarms.
Alarm Notifications	SA allows you to customize alarm notifications. You can set scheduled daily alarm notifications and real-time alarm notifications to learn about threat risks in a timely manner.

Threat Alarm Events

SA monitors your network in real time and reports alarms when threats are detected. SA can detect varied types of threats, including DDoS attacks, brute-force attacks, web attacks, backdoor Trojans, zombies, abnormal behavior, exploits, and C&C attacks.

Table 1-4 Threat alarm event description

Alarm Name	Alarm Description
DDoS	<p>SA detects DDoS attacks on any of your protected hosts in real time.</p> <p>More than 100 types of DDoS threats can be detected, including:</p> <ul style="list-style-type: none"> ● Network layer attacks NTP flood and CC attacks ● Transport layer DDoS attacks SYN and ACK flood attacks ● Session layer attacks SSL DDoS attacks ● Application layer attacks HTTP-GET DDoS flood attacks and HTTP-POST DDoS flood attacks

Alarm Name	Alarm Description
Brute-force attacks	<p>SA detects intrusions and internal risks on your hosts in real time, including brute force attacks on accounts, such as SSH, RDP, FTP, SQL Server and MySQL accounts, as well as abnormal logins.</p> <p>The following 22 types of brute-force attacks can be reported, including:</p> <ul style="list-style-type: none"> • Brute-force attacks that can be detected by SA SSH (2 types), RDP, Microsoft SQL, MySQL, FTP, SMB (3 types), HTTP (4 types), and Telnet brute force attacks • Alarms reported by HSS SSH, RDP, FTP, MySQL, IRC, and Webmin brute force attacks, brute force attacks on other ports, and brute force attacks on OSs
Web attacks	<p>SA detects web threats such as malicious web scanners, malicious IP addresses, and web Trojans in real time.</p> <p>The following 38 types of web threats can be detected:</p> <ul style="list-style-type: none"> • Web attacks Web shell attacks (3 types), cross-site scripting (XSS) attacks, code injection attacks (7 types), SQL injection attacks (9 types), and command injection attacks. • Alarms reported by HSS Web shells, Linux web page tampering, and Windows web page tampering. • Alarms reported by WAF Cross-site scripting (XSS) attacks, command injection attacks, SQL injection attacks, directory traversal attacks, local file inclusion, remote file inclusion, remote code execution, back doors, website information leakage, exploits, IP reputation databases exploits, malicious web crawlers, web page tampering, and web page crawlers
Trojan	<p>SA detects Trojans and malicious requests to compromised hosts in real time.</p> <p>The following 5 types of Trojans can be detected:</p> <ul style="list-style-type: none"> • Trojan files, such as PHP and JSP files, in the web directory on hosts • Characteristics of Trojans on compromised hosts Trojan: Win32/Ramnit Checkin, WannaCry ransomware request resolution, Trojan downloading, and access to HTTP File Server (HFS) download servers

Alarm Name	Alarm Description
Zombie	<p>SA detects threats initiated by zombies in real time.</p> <p>The following 7 types of attacks initiated by zombie hosts can be detected:</p> <ul style="list-style-type: none"> ● SSH brute-force attacks ● RDP brute-force attacks ● Web brute-force attacks ● MySQL brute-force attacks ● SQL Server brute-force attacks ● DDoS attacks ● Mining software
Abnormal behavior	<p>SA detects abnormal changes and operations to the operating systems (OSs) on assets in real time.</p> <p>The following 21 types of abnormal behavior can be detected:</p> <ul style="list-style-type: none"> ● Abnormal behavior that can be detected by SA Unauthorized file system scans, CMS V1.0 vulnerabilities, and unauthorized sensitive file access ● Alarms reported by HSS Alarms generated by abnormal logins, critical file changes, network interface cards (NICs) in promiscuous mode, unsafe accounts, reverse shells, abnormal shells, high-risk command execution, abnormal automatic startups, file privilege escalation, process privilege escalation, and rootkits ● Alarms reported by WAF Alarms generated against custom rules, whitelist, blacklist, geographical access control rules, malicious scanners & crawlers, IP blacklist or whitelist rules, and unauthorized access blocking
Exploit	<p>SA detects in real time the potential compromised assets that may be used to initiate attacks.</p> <p>The following 2 types of vulnerabilities can be detected:</p> <ul style="list-style-type: none"> ● Web-CMS exploits
Command Control	<p>SA detects command and control (C&C) servers in real time. A C&C server may remotely control host assets to access or establish links with malware.</p> <p>The following 3 types of C&C threats can be detected:</p> <ul style="list-style-type: none"> ● Access to Domain Generation Algorithm (DGA) domain names ● Access to malicious C&C domain names ● Malicious communication channels between C&C servers and host assets

Baseline Inspection

SA can scan cloud baseline configurations to find out unsafe settings, report alarms for events, and offer hardening suggestions to you.

Table 1-5 Baseline inspection description

Function Module	Description
Cloud Service Baseline	You can start a one-time scan or configure scheduled scans to let SA display results by category and provide hardening suggestions for you to fix unsafe settings.

Events

SA aggregates detection data from a variety of related services so that you can monitor all events in one place.

Table 1-6 Description of events

Function Module	Description
Events	<p>Multiple event types are included. You can mark and export events, and customize the event list.</p> <ul style="list-style-type: none"> Event types include: Threat alarms, vulnerabilities, risks, compliance checks, violations, public opinions, and security notices

Logs

You can authorize Object Storage Service (OBS) to store SA logs in OBS buckets. This makes it easier for you to store and export SA logs securely and meet audit requirements for storing logs for 180 days.

Table 1-7 Log management description

Function Module	Description
Logs	You can store SA logs in OBS to meet log audit and disaster recovery requirements.

Integrations

SA integrates a variety of security products to aggregate their detection data and manage the data sources of events.

Table 1-8 Product integration function descriptions

Function Module	Description
Integration s	By integrating other security services, SA makes it easy for you to aggregate detection results or events reported by different products, manage the sources of events, view the transmitted data volume, and manage the health status of reporting detection data to SA.

1.3 Application Scenarios

Asset Management

To keep up with your business expansion, you may need more cloud assets. With more cloud assets used, the risks to your services also increase.

SA monitors the security status of all assets in the cloud in real time and displays vulnerabilities, threats, and attacks on servers, helping you easily handle risks.

Threat Alarms

For various security threats on the cloud, SA collects network-wide traffic data and security protection device logs, and detects and monitors security risks on the cloud in real time, making it easier for you to view alarm event statistics in real time.

System Configuration Management

SA can scan cloud services for risks in key configuration items, report scan results by category, generate alarms for events, and provide hardening suggestions and guidelines.

1.4 Edition Differences

Situation Awareness (SA) includes a basic edition and professional edition. For more details, see [Features](#).

Function Differences Between SA Editions

 **NOTE**

Functions of each module in different editions are shown in the following tables, where:

- X: indicates that the function is unavailable in the corresponding edition.
- √: indicates that the function is available in the corresponding edition.

Table 1-9 Function differences between SA editions

Function	Function Module	Description	Basic Edition	Professional
Security Overview	Security Score	SA scores security posture of your system, sorts out risks by severity, and summarizes the risk defense capabilities of your system.	√	√
	Security Monitoring	SA summarizes the alarms, vulnerabilities, and abnormal baseline settings that have not been handled.	√	√
	Your Security Score over Time	SA displays your security scores for the last 7 days.	√	√
Resource Manager	Resource security situation	SA synchronizes information about your resources and displays overall security posture in one place.	×	√
Threat Alarms	Alarms	SA displays threat alarm event statistics and allows you to export alarm events.	√	√
		SA allows you to ignore an alarm or mark an alarm for offline processing.	×	√
	Threat Analysis	SA allows you to query the information about the attacked asset by IP address of the attack source, or query the information about the threat attack source by IP address of the attacked asset.	×	√
Baseline Inspection	Cloud Service Baseline	SA scans cloud service baselines in one-click and displays the inspection results by category.	×	√
		SA scans cloud service baselines in one-click and displays the inspection results by category. SA allows users to view details of check results and provides fixing suggestions.	×	√
Events	Events	SA displays the events or detection results of security products in a centralized manner. You can export and mark events.	√	√
Logs	Logs	You can authorize OBS to store SA logs. This helps you meet log audit and disaster recovery requirements.	×	√

Function	Function Module	Description	Basic Edition	Professional
Integrations	Integration of security products	SA integrates a variety of security products to aggregate their detection data and manage the data sources of events.	√	√

1.5 Billing

Billing Items

The basic edition is free of charge. The professional edition is billed based on how many asset quotas you purchase.

Table 1-10 SA billing items

Edition	Billing Items	Description
Basic edition	None	Free trial
Professional edition	Asset quotas	Billed based on purchased asset quota, including the total ECS quota and website quota.
	Pay-per-use billing	Enabled or disabled at any time and billed for usage by the hour.

Billing Modes

SA is billed on a pay-per-use basis. You are billed for usage duration by the hour. This billing mode allows you to enable or disable the SA service at any time.

Changing Billing Options

- Changing asset quotas
When the number of your assets increases, you can increase the asset quota in the same billing mode. A scale-down of purchased quotas is not supported.

1.6 Basic Concepts

This section describes concepts about SA.

Security Risk

Security risk is a comprehensive evaluation of your assets, reflecting the security level of your assets within a period of time by a security score. A security score is for your reference to learn of the security situation of your assets.

Threat Alarm

In general, threat alarms refer to threats that, due to natural, human, software, or hardware reasons, are detrimental to information systems or cause negative effects on the society. In SA, threat alarms are detected security incidents that threaten asset security through big data technology.

Website Vulnerability

A website vulnerability is the vulnerability detected by the web crawler and intelligent comparison of vulnerability features. SA can scan over 22 types of vulnerabilities and can also detect OWASP top 10 and WASC vulnerabilities. The scan rules are automatically updated on the cloud and take effect on the entire network, covering the latest vulnerabilities. HTTPS scan is as well as supported.

Cloud Service Baseline

Cloud service baseline helps you detect unsafe configurations in cloud-based products in cloud scenarios and provides recovery suggestions.

Attack Types

- Brute-force attack
A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found to decrypt any encrypted data.
- Web attack
A web attack is an attack against the Internet access or devices such as web servers. Common web attacks include SQL injection, cross-site scripting (XSS), and cross-site request forgery (XSRF) attacks.
- Zombie
A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus, or Trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction. Attackers send commands to "zombies" through control channels and order them to send forged or junk packets to targets. As a result, the targets fail to respond and deny normal services. This is a common DDoS attack. Now, as virtual currencies, such as Bitcoins, grow in value, attackers start using zombies to mine Bitcoins.
- Abnormal behavior
Abnormal behavior refers to the events that should not occur on hosts. For example, a user logs in to the system during an unauthorized time period, some file directories are changed unexpectedly, and unexpected actions were performed by a process. We should keep alert for those anomalies as most of

them are caused by malware. The abnormal behavior data in SA is mainly reported by Host Security Service (HSS).

- Vulnerability exploit

A vulnerability is a weakness that can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system. Gaining access, stealing sensitive data, or sabotaging software and hardware systems are all vulnerability exploits.

1.7 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your SA resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure the access to your cloud resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to control their access to specific resource types. For example, some software developers in your enterprise need to use SA resources but must not delete them or perform any high-risk operations. To this end, you can create IAM users for the software developers and grant them only the permissions required for using SA resources.

If your account does not need individual IAM users for permissions management, then you may skip over this chapter.

SA Permissions

By default, new IAM users do not have any permissions assigned. You can add a user to one or more groups to allow them to inherit the permissions from the groups to which they are added.

You can create IAM users in any region. SA is a global service for all geographic regions. SA permissions are assigned to IAM users in the global project, so IAM users can access SA in any region without having to switch over among regions.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. If one role has a dependency role required for accessing SA, assign both roles to the users. Roles are not ideal for fine-grained authorization and secure access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you can grant SA users only the permissions for managing a certain type of resources. For the API actions supported by SA, see [SA Permissions and Supported Actions](#).

[Table 1-11](#) lists all the system-defined roles and policies supported by SA.

Table 1-11 System-defined permissions supported by SA

Policy Name	Description	Type	Dependency
SA FullAccess	All permissions for SA	System-defined policy	None
SA ReadOnlyAccess	Read-only permission for SA. Users with the read-only permission can only query SA information but cannot perform configuration in SA.	System-defined policy	None

 **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**.

1.8 SA and Other Services

This topic describes SA and its linked services.

Security Services

SA helps you get insights into attacks and intrusions against your cloud assets and provides protective suggestions for you. To this end, SA aggregates detection results from varied security products and analyzes received data with big data, machine learning, and AI technologies.

ECS

SA detects threats to your Elastic Cloud Servers (ECSs) with linked service HSS, comprehensively displays ECS security risks, and provides protection suggestions.

OBS

With Object Storage Service (OBS), you can store SA logs in OBS buckets to prevent log loss and achieve data persistence.

2 Edition Upgrade

SA provides basic and professional editions for you.


- The basic edition helps you detect only some threat risks and check security posture of your assets on the cloud.
- To have a comprehensive picture for your asset security on the cloud in a timely manner, upgrade the basic edition to the professional edition.
 - The professional edition provides more types of threat detection and analysis services, including threat analysis, alarm settings, and baseline inspection.
 - For more details, see [Edition Differences](#).


Prerequisites

You have obtained an account for logging in to the management console.

Procedure

Step 1 Log in to the management console.

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

Step 3 Click  in the upper left corner of the page and choose **Security > Situation Awareness**.

Step 4 Click **Upgrade** in the upper right corner.

Step 5 Select intended users.

You can select IT O&M personnel, security O&M personnel, compliance personnel, or CSO/CIO/CISO. Different configurations are recommended for different users.

Step 6 Select a billing mode. You can select **Yearly/Monthly** or **Pay-per-use**.

Step 7 Select the SA edition. The professional edition is selected by default.

Step 8 Configure **ECS Quota**.

The maximum number of ECSs that require protection from SA.

The total ECS quota must be greater than or equal to the total number of hosts within your account. This value cannot be changed to a smaller one after your purchase is complete.

The maximum ECS quota varies depending on how many ECSs you have.

- If the total number of ECSs within your account is less than or equal to 10, the maximum ECS quota is 100.
- If the total number of ECSs within your account is greater than 10, the maximum ECS quota is the result of total number of ECSs within your account multiplied by 10.

For example, if there are 20 ECSs within your account, the maximum ECS quota you can configure is 200 (20 x 10).

 **NOTE**

If some of your ECSs are not protected by SA, threats to them cannot be detected in a timely manner, which may result in security risks, such as data leakage. To prevent this, increase the ECS quota upon an increase of the ECS quantity.

Step 9 If you select **Yearly/Monthly** for **Billing Mode**, specify **Required Duration**.

Step 10 Confirm the product details and click **Next**.

Step 11 Confirm the order details and click **Pay Now**.

Step 12 On the payment page, select a payment method and pay for your order.

----End

Follow-up Operations

If you no longer need the professional edition, click **Cancel** to unsubscribe from it. However, the basic edition remains available for you.

3 Permissions Management

3.1 Creating a User and Granting Permissions

This section describes how to use Identity and Access Management (IAM) to implement fine-grained permissions control for your SA resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to SA resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your SA resources.

If your account does not require individual IAM users, skip over this section.

The following walks you through how to grant permissions. [Figure 3-1](#) shows the process.

Prerequisites

Learn about the permissions (see [Permissions Management](#)) supported by SA and choose policies or roles according to your requirements.

[Table 3-1](#) lists all the system-defined roles and policies supported by SA.

Table 3-1 System-defined permissions supported by SA

Policy Name	Description	Type	Dependency
SA FullAccess	All permissions for SA	System-defined policy	None

Policy Name	Description	Type	Dependency
SA ReadOnlyAccess	Read-only permission for SA. Users with the read-only permission can only query SA information but cannot perform configuration in SA.	System-defined policy	None

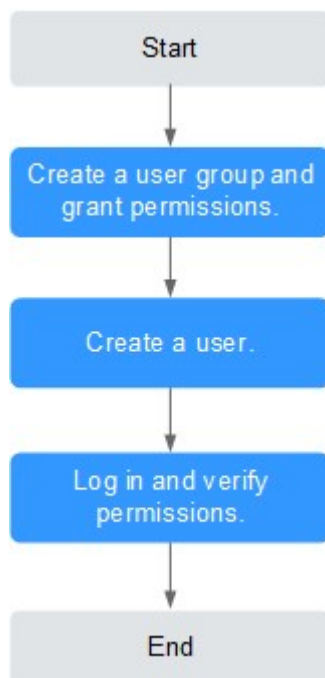
NOTE

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**.

Authorization Process

Figure 3-1 Process for granting permissions



1. Create a user group and assign permissions.
Create a user group on the IAM console. Then, assign the **SA FullAccess** and **Tenant Guest** permissions to the group.

2. Create a user and add it to a user group.
Create a user on the IAM console and add the user to the group created in **1**.
3. Log in and verify the permissions.
Log in to the SA console as the created user, and verify that the user only has read permissions for SA.
Choose any other service from **Service List**. If a message appears indicating that you do not have permissions to access the service, the **SA FullAccess** policy has already taken effect.
4. Configure an agency.
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?](#)

3.2 SA Custom Policies

Custom policies can be created to supplement the system-defined policies of SA.

Example Custom Policies

- Example 1: Authorizing a user to obtain the alarm list and threat analysis results

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sa:threatevent:getList",
        "sa:threatevent:getAnalyze"
      ]
    }
  ]
}
```

- Example 2: Preventing users from modifying alarm configurations

A deny policy must be used together with other policies. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used to create a custom policy to disallow users who have the **SA FullAccess** policy assigned to modify alarm configurations. Assign both **SA FullAccess** and the custom policies to the group to which the user belongs. Then the user can perform all operations on SA except modifying alarm configurations. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "sa:subscribe:operate"
      ],

```

```

        "Effect": "Deny"
      }
    ]
  }

```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sa:cssb:operate",
        "sa:cssb:get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:GetReplicationConfiguration",
        "obs:bucket:PutReplicationConfiguration",
        "obs:bucket>DeleteReplicationConfiguration"
      ],
      "Resource": [
        "obs:*:bucket:*"
      ]
    }
  ]
}

```

3.3 SA Permissions and Supported Actions

This section describes fine-grained permissions management for your SA. If your account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using roles and policies. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

SA provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.

4 Editions

4.1 Increasing Asset Quotas

SA allows you to increase **ECS Quota** and change required duration at any time after you make a purchase.

Constraints

- The ECS quota is the total number of ECSs that are authorized to receive checks. The maximum ECS quota varies depending on how many ECSs you have.

Table 4-1 Maximum ECS quota


ECSs Within Your Account	Maximum ECS Quota
10 and below	100
Above 10	Quantity of ECSs within your account multiplied by 10 For example, if you have 20 ECSs within your account, the maximum ECS quota you can configure is 200 (20 x 10).

- When buying SA, ensure that the ECS quota is greater than or equal to the total number of ECSs you have within your current account. If you configure ECS quota to a number smaller than the number of ECSs you have, the following impact may occur:

A lack of awareness of the threats to ECSs that are not covered by SA. This may cause server risks such as data leakage.

Pay-Per-Use Billing Mode

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**. Note that you only need to increase quotas for ECSs you expect to add.

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

Step 8 After you complete the payment, return to the SA console. You can then start to protect the newly added hosts based on increased quota.

----End


4.2 Unsubscribing from SA

If you no longer need SA, cancel it within just a few clicks.

- Pay-per-use billing mode: pay for what you use by the hour. This mode allows you to enable or disable resources at any time. One-click resource cancellation is also supported.

Canceling Pay-Per-Use SA Resources

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 **Professional** in the upper right corner. The edition management window is displayed.

Step 4 In the row of the SA edition purchased in pay-per-use billing mode, click **Cancel** to release the purchased SA resources.

Go to the edition management window and verify that the subscription to resources billed on a pay-per-use basis is canceled.

----End

5 Security Overview

5.1 Overview

The **Security Overview** page gives you a comprehensive overview of your asset security posture in real time together with other linked cloud security services to collectively display security assessment findings. On the **Security Overview** page, you can view the security status of your cloud resources, take required actions with just a few clicks, and manage risks centrally.

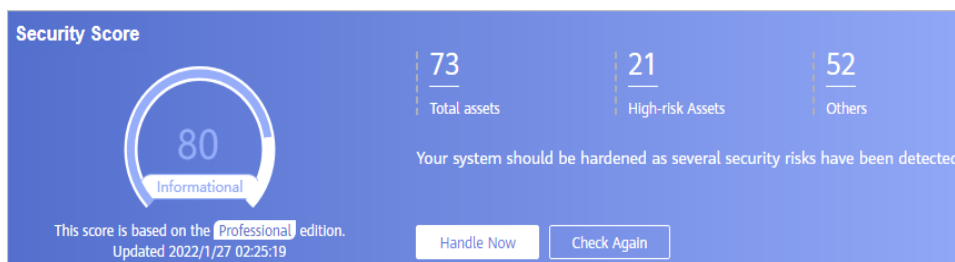
On the **Security Overview** page, you can view the overall security posture of your assets and take actions accordingly. The **Security Overview** page consists of the following parts:

- [Security Score](#)
- [Security Monitoring](#)
- [Your Security Score over Time](#)

Security Score

The security score shows the overall health status of your workloads on the cloud based on the SA edition you are using. You can quickly learn about unhandled risks and their threats to your assets. [Figure 5-1](#) shows an example.

Figure 5-1 Security Score



- The score ranges from 0 to 100. The higher the security score, the more secure your assets. For details, see [Security Score](#).

- Different color blocks in the security score ring chart indicate different severity levels. For example, yellow indicates that your security is medium.
- If you click **Handle Now**, the **Risks** pane is displayed on the right. You can handle risks by referring to the corresponding guidance.
 - The **Risks** pane lists all threats that you should handle as soon as possible. Those threats are included in the **Threat Alarms** and **Compliance Check** areas.
 - The **Risks** pane displays the latest alarms found in the last scan. The **Events** page shows all alarms found in all previous scans. So, you will find the threat number on the **Risks** pane is less than that on the **Events** page. You can click **Handle** for an alarm on the **Risks** pane to go to the **Events** page quickly.
 - Handling detected security risks:
 - i. In the **Security Score** area, click **Handle Now**. The **Risks** pane is displayed on the right.
 - ii. On the **Risks** pane, locate a risk and click **Handle** in the corresponding row. The **Events** page is displayed.
 - iii. Select one or more events in the **Unhandled** status and click **Ignore** or **Mark as Offline** above the result list to handle all selected events at a time.
 - **Ignore**: If the event does not cause any harm, ignore the result. After click **Ignore**, record the **Handler** and **Reason** in the **Ignore Risk** dialog box.
 - **Mark as Offline**: If the event has been handled offline, click **Mark as Offline** in the **Operation** column. In the displayed dialog box, fill in **Processor**, **Processing Time**, and **Processing Result**, and click **OK**.
- The security score is updated when you refresh the status of an alarm event after the risk is handled. After you address the risks, you can click **Check Again** so that SA can check and score your system again.

 **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.
- After risks are fixed, you can manually ignore or handle alarm events and update the alarm event status in the alarm list. The risk severity will then be downgraded accordingly.
- The security score reflects the security situation of your system last time you let SA check the system. To obtain the latest score, click **Check Again**.

Security Monitoring

The **Security Monitoring** area includes **Threat Alarms** and **Compliance Check**, which sort risks that have not been handled.

Figure 5-2 Security Monitoring

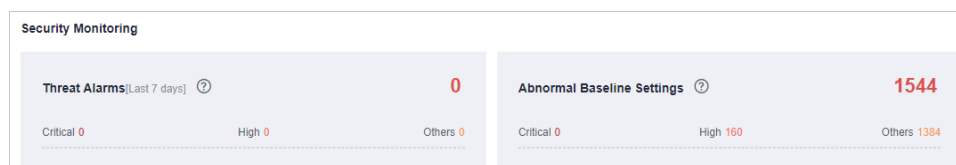


Table 5-1 Security Monitoring parameters

Parameter	Description
Threat Alarms	<p>This panel displays the unhandled threat alarms for the last 7 days. You can quickly learn of the total number of unhandled threat alarms and the number of vulnerabilities at each severity level.</p> <ul style="list-style-type: none"> • Risk severity levels: <ul style="list-style-type: none"> - Critical: Unauthorized access to your workloads has been detected, and you should view alarm details and handle the alarm in a timely manner. - High: There are abnormal events on your workloads, and you should view alarm details and handle the alarm in a timely manner. - Others: There are risky events that are marked as medium-risk, low-risk, and informational alarms detected in your systems, and you should view alarm details and take necessary actions. • To quickly view details of the top 5 threat alarms for the last 7 days, click the Threat Alarms panel. <ul style="list-style-type: none"> - You can view details of those threats, including the threat alarm name, severity, asset name, and discovery time. - If there is no data available, that means that no threat alarms have been triggered in the last 7 days. - You can click View More to go to the Events tab and view more alarms. You can apply custom search filters to query alarms.

Parameter	Description
<p>Compliance Check</p>	<p>This panel displays the total number of compliance violations detected for the last 30 days. You can quickly learn of total number of violations and the number of violations at each severity level.</p> <ul style="list-style-type: none"> ● Risk severity levels: <ul style="list-style-type: none"> - Critical: There are some configurations that failed compliance checks on your workload, and you should view their details and handle them in a timely manner. - High: There are abnormal settings on your workloads, and you should view details about compliance violations and handle them in a timely manner. - Others: There are risky events that are marked as medium-risk, low-risk, and informational alarms detected in your systems, and you should view the compliance check details and take the necessary actions. ● To quickly view details of the top 5 abnormal compliance risks discovered in the last 30 days, click the Compliance Check panel. <ul style="list-style-type: none"> - You can view details such as the check item name, severity, asset name, and discovery time. - If there is no data available, that means no violations have been detected in the last 30 days. - You can click View More to go to the Events tab and view more compliance risks. You can apply custom search filters to make an advanced search.

Your Security Score over Time

SA displays your security scores for the last 7 days.

Figure 5-3 Your Security Score over Time



5.2 Security Score

SA assesses the overall security of your cloud assets in real time and scores your assets based on the SA edition you are using.

This topic describes how your security score is calculated.

Security Score

SA evaluates the over security posture of your assets based on the SA edition you are using.

- There are five risk severity levels, **Secure**, **Informational**, **Low**, **Medium**, **High**, and **Critical**.
- The score ranges from 0 to 100. The higher the security score, the safer your assets are.
- The security score starts from **0** and the risk severity level is escalated up from **Secure** to the next level every 20 points. For example, for scores ranging from **40** to **60**, the risk severity is **Medium**.
- The color key listed on the right of the chart shows what level each color on the chart represents. Different colors represent different risk severity levels. For example, yellow indicates that your asset risk is **Medium**.
- The security score is updated when you refresh the status of an alarm event after the risk is handled.

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.
- After risks are fixed, you can manually ignore or handle alarm events and update the alarm event status in the alarm list. The risk severity will then be downgraded accordingly.

Table 5-2 Security score table

Severity	Security Score	Description
Secure	100	Congratulations. Your assets are secure.
Informational	$80 \leq$ Security Score < 100	Your system should be hardened as several risks have been detected.
Low	$60 \leq$ Security Score < 80	Your system should be hardened in a timely manner as numerous risks have been detected.
Medium	$40 \leq$ Security Score < 60	Your system should be hardened ASAP. Your assets are vulnerable to attacks.

Severity	Security Score	Description
High	$20 \leq$ Security Score < 40	Detected risks should be handled ASAP. Your assets are vulnerable to attacks.
Critical	$0 \leq$ Security Score < 20	Detected risks should be handled immediately. Your assets are likely to be attacked.

Unscored Check Items

Table 5-3 lists the security check items and corresponding points.

Table 5-3 Unscored check items

Category	Unscored Item	Points	Suggestion	Maximum Unscored Point
Compliance Check	Critical non-compliance items not fixed	10	Fix risky items that failed compliance check by referring to corresponding suggestions and start a new scan. The security score will be updated.	20
	High-risk non-compliance items not fixed	5		
	Medium-risk non-compliance items not fixed	2		
	Low-risk non-compliance items not fixed	0.1		
Threat Alarms	Critical alarms not fixed	10	Fix the threats by referring to the suggestions and start a new scan. The security score will be updated accordingly.	30
	High-risk alarms not fixed	5		
	Medium-risk alarms not fixed	2		
	Low-risk alarms not fixed	0.1		

6 Resource Manager

You can use SA to manage your cloud resources. On the **Resource Manager** page, you can view the security status statistics of all resources under your account, including the resource name, service, and security status. This helps you quickly locate security risks and find solutions.

Prerequisites

- Your account must have required permissions. To manage resources, your account should have the **SA FullAccess**, **SA ReadOnlyAccess**, and **Tenant Administrator** permissions.
For details about **Tenant Administrator**, see [Configuring Permissions to Use Resource Manager and Logs](#)
- Your professional edition SA is available.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > Situation Awareness**.
- Step 3** In the navigation pane on the left, choose **Resource Manager**.
- Step 4** View the security status of all resources. [Table 6-1](#) describes related parameters.

Figure 6-1 Resource Manager

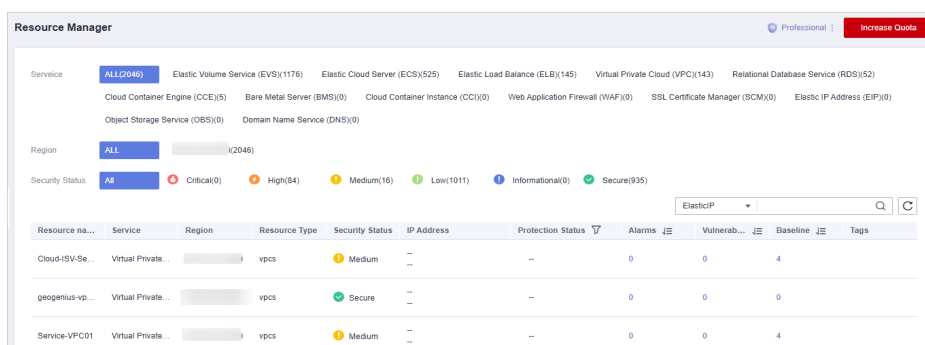



Table 6-1 Parameters for resource security status

Parameter	Description
Resource Name	Resource name.
Service	Service the resource belongs to.
Resource Type	Type of the resource. For example, cloud servers, disks, and instances.
Security Status	<p>Risk severity of the resource.</p> <ul style="list-style-type: none"> • Risk is classified as Critical, High, Medium, Low, Informational, and Secure. • This column only displays the highest risk severity of the current resource. For example, if an ECS has high-risk, low-risk, and informational alarms, High is displayed for the resource. • You can click  to list resources by risk severity.
IP Address	IP address of the resource.
Protection Status	Whether protection is enabled for the resource. If protection is not enabled, click Enable .
Alarms	<p>The total number of threat alarms for the resource in the last 7 days.</p> <p>To view more threat alarm information, click the number of alarms to go to the Events page. You can apply custom search filters to create an advanced query.</p>
Vulnerabilities	<p>The total number of vulnerabilities that have not been fixed within the last 24 hours.</p> <ul style="list-style-type: none"> • To view more information, click the number of vulnerabilities to go to the Events page. You can also customize filter criteria to create an advanced query. • The Resource Manager page displays the latest events found in the last scan, but the Events page displays all events found in previous scans. This means you may see more risks on the Events page than on the Resource Manager page.


Parameter	Description
Baseline	<p>The total number of baseline risks for a resource in the last 30 days.</p> <ul style="list-style-type: none"> To view more information, click the number of baseline risks to go to the Events page. You can apply custom search filters to create an advanced query. The Resource Manager page displays the latest events found in the last scan, but the Events page displays all events found in previous scans. This means you may see more risks on the Events page than on the Resource Manager page.
Enterprise Project	The enterprise project where the resource is managed.
Tag	<p>Tags added to the resource.</p> <p>If a tag is added to a resource on the current day, the tag will be displayed in this column the next day.</p>

Step 5 Filter resources by specific information and view their security status.

Click an option next to **Service**, **Region**, or **Security Status** to display the resources that meet your filter criteria.

- **Service:** sorts resources by specific service. After you select a service, you can view the security status of resources by **Resource Type**.
- **Region:** sorts resources by region.
- **Security Status:** sorts resources by risk severity.
Risk severity levels include **Critical**, **High**, **Medium**, **Low**, **Informational**, and **Secure**.

Step 6 (Optional) If a large number of resources are listed, query a specific resource by filtering.

You can search for resources by **EIP**, **Name**, or **Private IP**. In the search box, enter the keyword and click  to view the security status of the resource.

----End

7 Threat Alarms

7.1 Threat Alarms Overview

Overview

SA can aggregate alarms reported by other security products. All those alarms are centrally displayed in the **Threat Alarms** module. In this module, you can learn of threats and security events discovered in your cloud resources in a timely manner.

Beyond that, this module sorts threats by attack source and attacked asset so that you can quickly learn of vulnerable assets and learn the security posture of your assets in real time.

The threat alarms module includes the following functions:

- **Alarms**
SA monitors threat events on the cloud in real time, provides alarm notifications using linked services HSS and WAF, and displays details about alarms for the last 180 days.
- **Threat Analysis**
Allows you to query threats or attacks by **Attack source** or **Attacked asset**.

Alarm Types

Currently, SA includes eight categories of check items, including more than 200 event types.

DDoS Alarm Events

SA can protect all your hosts from DDoS attacks no matter where your hosts are deployed.

More than 100 types of DDoS threats can be detected.

- Network layer attacks
NTP flood and CC attacks

- Transport layer DDoS attacks
SYN and ACK flood attacks
- Session layer attacks
SSL DDoS attacks
- Application layer attacks
HTTP-GET DDoS flood attacks and HTTP-POST DDoS flood attacks

Brute-force Attack Alarms

SA detects intrusion behaviors and internal risks to your host assets in real time. It checks whether accounts, such as SSH, RDP, FTP, SQL Server and MySQL accounts, are experiencing password cracking attacks, and detects whether asset accounts have been cracked for abnormal logins.

Currently, 22 types of brute-force attacks can be detected.

- Brute-force attacks that can be detected by SA
SSH brute force attacks (2 types), RDP brute force attacks, Microsoft SQL brute force attacks, MySQL brute force attacks, FTP brute force attacks, SMB brute force attacks (3 types), HTTP brute force attacks (4 types), and Telnet brute force attacks.
- Alarms from the linked HSS service
SSH, RDP, FTP, MySQL, IRC, and Webmin brute force attacks, brute force attacks on other ports, and brute force attacks on OSs

Web Attack Alarms

SA detects web threats such as malicious web scanners, malicious IP addresses, and web Trojans in real time.

Currently, 38 types of web threats can be detected.

- Web attacks that can be detected by SA
Web shell attacks (3 types), cross-site scripting (XSS) attacks, code injection attacks (7 types), SQL injection attacks (9 types), and command injection attacks.
- Alarms from the linked HSS service
Web shells, Linux web page tampering, and Windows web page tampering.
- Alarms from the linked WAF service
Cross-site scripting (XSS) attacks, command injection attacks, SQL injection attacks, directory traversal attacks, local file inclusion, remote file inclusion, remote code execution, Trojans, website information leakage, exploits, IP reputation database, malicious crawlers, web page anti-tampering, and web page anti-crawler.

Trojan Attack Alarms

SA detects Trojans and malicious requests to compromised hosts in real time.

Currently, 5 types of Trojans can be detected.

- Trojans in PHP and JSP files in the web directory on hosts
- Trojans on compromised hosts
Trojans such as Win32/Ramnit Checkin, WannaCry ransomware request resolution, Trojan downloading, and access to HTTP File Server (HFS) download servers

Zombie Alarms

SA detects threats initiated by zombie hosts in real time. The following 7 types of zombie attacks can be detected:

- SSH brute-force attacks
- RDP brute-force attacks
- Web brute-force attacks
- MySQL brute-force attacks
- SQL Server brute-force attacks
- DDoS attacks
- Mining software

Abnormal Behavior Alarms

SA detects abnormal changes and operations of the operating systems (OSs) on assets in real time. The following 21 types of abnormal behavior can be scanned for:

The following 21 types of abnormal behavior can be scanned for:

- Abnormal behavior that can be scanned for by SA
Unauthorized scanning over the file system, CMS V1.0 vulnerabilities, and unauthorized sensitive file access.
- Alarms reported by HSS
Abnormal logins, critical file changes, network interface cards (NIC) in promiscuous mode, unsafe accounts, reverse shells, abnormal shells, high-risk command execution, abnormal automatic startups, file privilege escalation, process privilege escalation, and Rootkits
- Alarms reported by WAF
Alarms generated against custom rules, whitelist, blacklist, geographical access control rules, malicious scanners & crawlers, IP blacklist or whitelist rules, and unauthorized access blocking

Exploit Alarms

In real time, SA scans the potentially compromised assets that may be used to initiate attacks. The following 2 types of vulnerabilities can be detected:

- Web-CMS vulnerability attacks

C&C Alarms

SA detects command and control (C&C) servers in real time. A C&C server may remotely control the hosts to access or establish links with malware.

The following 3 types of C&C threats can be detected:

- Access to Domain Generation Algorithm (DGA) domain names
- Access to malicious C&C domain names
- Malicious communication channels between C&C servers and host assets

7.2 Viewing Alarms

On the **Alarms** tab, you can query alarms from the last 180 days. You can view the alarm details, including alarm name, type, risk severity, and generation time. By applying custom filters, such as the alarm name, risk severity, and time, you can quickly query information about specific alarms.


This makes it easier to handle alarms in a timely manner, marking the alarm processing statuses or exporting all alarms in the last 180 days in a click or two.

Constraints

- Ignoring or marking an alarm event is only supported in the professional edition.
- Exporting only a certain type of alarms is not supported. You can export all alarms for the last 180 days.
- When search filters are applied to search for alarms, a maximum of 10,000 alarms can be displayed.

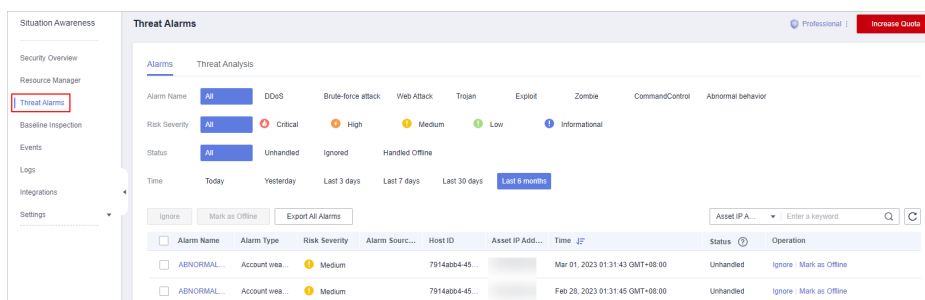
Viewing Alarm Details

Step 1 Log in to the management console.

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

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

Figure 7-1 Threat Alarms




Step 4 Specify **Alarm Name**, **Risk Severity**, **Time**, and/or **Status** to display only alarms that meet the filter criteria you specified.

- **Alarm Name** is the category that the alarm belongs to.
- **Risk Severity** is severity of an alarm. The options are **Critical**, **High**, **Medium**, **Low**, and **Informational**.

- **Status** is the handling status of an alarm. The options are **Unhandled**, **Ignored**, and **Handled Offline**.
- **Time** indicates a time range to display alarms generated during such range. The options are **Today**, **Yesterday**, **Last 3 days**, **Last 7 days**, **Last 30 days**, and **Last 6 months**.

Step 5 If a large number of alarms are displayed after applying your search filters, you can use the search function to quickly locate specific alarms.

You can select **Asset IP Address**, **Alarm Source IP Address**, or **Host ID** from the drop-down list, enter an IP address or ID in the search box, and click  to locate information about alarms generated for a specified asset.

Step 6 Viewing alarm details.

Click an alarm name in the alarm list. The **Alarm Details** window slides out from the right. You can view the basic information, detection source, attack source, and affected users of the alarm, and change the alarm processing status.

----End

Marking Alarm Events

You can manually mark an alarm event reported by SA.

Step 1 On the **Alarms** tab, mark the processing status of alarms.

- **Ignore**: If an alarm does not cause any harm, it can be marked as **Ignored**.
- **Mark as Offline**: If the alarm has been handled offline, click **Mark as Offline** in the **Operation** column. In the displayed dialog box, fill in **Processor**, **Processing Time**, and **Processing Result**, and click **OK**.

Step 2 Marks the processing status of multiple alarms once.

Select one or more alarms in the **Unhandled** status and click **Ignore** or **Mark as Offline** above the alarm list to handle all selected alarms at a time.

Step 3 Marks the processing status of a single alarm.

In the **Operation** column of the target alarm, click **Ignore** or **Mark as Offline** to handle the alarm.

Step 4 Cancel the alarm processing status marking.

To change the processing status of an alarm, locate the target row and click **Unignore** or **Unmark** in the **Operation** column to restore the alarm to the **Unhandled** status and then re-mark the alarm processing status.

----End

Exporting Alarm Events

On the **Alarms** tab, click **Export All Alarms** above the alarm list to export all threat alarms into an Excel file and save the file locally. After all alarms are exported, you can view them offline.

The exported Excel file contains information such as **Event ID**, **Affected Resource**, **Severity**, and **Discovered**.

 NOTE

Currently, only all alarm events generated for the last 180 days can be exported.


7.3 Viewing Threat Analysis

On the **Threat Analysis** page, you can analyze attacks based on the **Attack source** or **Attacked asset**.

Prerequisites

Your professional edition SA is available.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > Situation Awareness > Threat Alarms > Alarms**.
- Step 3** In the navigation pane on the left, choose **Threat Alarms**. On the displayed page, click the **Threat Analysis** tab.
- Step 4** Select **Attack source** or **Attacked asset** from the drop-down list, set occurrence time, enter the IP address to be queried, and click **Start Analysis**.

 NOTE

The time can be **Today**, **Yesterday**, **Last 3 days**, **Last 7 days**, **Last 30 days**, or **Last 6 months**.

- Step 5** In the list, you can view all threat information that meets the filtering conditions. You can view which assets have been attacked, what types of attacks there have been, or which sources attacks have come.

----End

7.4 Handling Alarms and Events

7.4.1 Brute Force Attacks

Overview

In a brute force attack, every possible login credential is systematically tested until the actual result password is identified. Attackers guess and try login usernames and passwords remotely. If they guess correctly, they can attack and control systems.

Suggestion

If a brute force attack threat is detected, handle the threat by following the instructions in [Table 7-1](#).

Table 7-1 Suggestions on handling some brute force attack threats

Threat Alarm	Severity	Threat Description	Suggestion
SSH brute-force attack	Medium	Continuous attempts to log in to an ECS instance over SSH were detected, indicating that an attacker is attempting to hack into the ECS instance using SSH.	<p>The SSH port is open to the public network. You are advised to perform the following operations:</p> <ol style="list-style-type: none"> 1. In the security group settings, forbid external SSH access. 2. Configure hosts.deny in the ECS operating system.
RDP brute force attack	Medium	Continuous attempts to log in to an ECS instance over RDP were detected, indicating that an attacker is attempting to hack into the ECS instance using RDP.	<p>The RDP port is open to the public network. You are advised to perform the following operations:</p> <ol style="list-style-type: none"> 1. In the security group settings, forbid external RDP access. 2. Limit remote desktop access using tools like the Windows firewall in the ECS operating system.
Web brute force attack	Medium	Continuous attempts to log in to your web service (such as a login page) were detected, indicating that an attacker is attempting to hack into the web service (such as the web application login page).	<p>The background management pages (such as phpMyAdmin and Tomcat management pages) of the application are open to the public network, and login verification is not performed for login pages for services that need to be accessed from the public network. You are advised to perform the following operations:</p> <ol style="list-style-type: none"> 1. In the security group settings, forbid external access to the background management system page. 2. Configure brute force attack defenses for web applications, for instance, SMS two-factor verification and image verification codes.

Threat Alarm	Severity	Threat Description	Suggestion
MySQL brute-force attack	Medium	Continuous attempts to log in to MySQL instance on an ECS instance, indicating that an attacker is attempting to hack into the MySQL instance on the ECS instance.	The MySQL service port is open to the public network. You are advised to perform the following operations: <ol style="list-style-type: none"> 1. In the security group settings, forbid external access to the MySQL instance. 2. Configure the firewall policy on the OS to forbid external access. 3. Unbind the EIP from the ECS where the MySQL instance is installed.
Microsoft SQL brute force attack	Medium	Continuous attempts to log in to Microsoft SQL Server on an ECS instance were detected, indicating that an attacker is attempting to hack into Microsoft SQL Server on the ECS instance.	The Microsoft SQL Server service port is open to the public network. You are advised to perform the following operations: <ol style="list-style-type: none"> 1. In the security group settings, forbid external access to the Microsoft SQL Server instance. 2. Configure the firewall policy on the OS to forbid external access. 3. Unbind the EIP from the ECS where the Microsoft SQL Server instance is installed.
System brute force attack detection event	Medium	A brute force attack was detected. There are continuous attempts to log in to your ECS instance.	Log in to the HSS console and handle the issue.
Unauthorized system account	Medium	A brute force attack was detected. There are continuous attempts to log in to the ECS instance using an unauthorized system account.	Log in to the HSS console and handle the issue.
System crack success detection event	High	One of your ECS instances was hacked.	Log in to the HSS console and handle the issue.

7.4.2 Web Attacks

Overview

A web attack is an attack on a device used to access the Internet or on devices on the Internet, like web servers. Common web attacks include SQL injection, cross-site scripting (XSS), and cross-site request forgery (XSRF) attacks.

Suggestion

If SA detects a web attack, an attacker is attempting to exploit a vulnerability in the web application. The severity of this type of threat is **Medium** or lower. You are advised to perform the following operations:

1. Check the web application logic for vulnerabilities.
2. Purchase WAF.

7.4.3 Trojan

Overview

A Trojan horse, or just "Trojan", is any malicious computer program which misleads users of its true intent. It acts like a legitimate application program or file to deceive victims into executing or spreading it. When victims execute it, attackers gain unauthorized access to target hosts to steal data, such as usernames, passwords, and encrypted files. Trojan typically serves as a foundation for further attacks.

Suggestion

If a Trojan is detected and the ECS instance has network requests coming from Trojans, the ECS instance has been infected. For example, the ECS instance cloud attempt to send DNS resolution requests related to WannaCry ransomware or to download .exe Trojans. The severity of this type of threat is **High**. You are advised to perform the following operations:

1. Disable the ECS instance that is infected.
2. Check whether other hosts on the subnet where the instance resides are infected.
3. Purchase HSS.

7.4.4 Exploits

Overview

A vulnerability is a weakness that can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system. Attackers exploit vulnerabilities to obtain rights, steal sensitive data, or sabotage software and hardware systems.

Suggestion

If an exploit is detected, handle the threat by following the instructions in [Table 7-2](#).

Table 7-2 Suggestions for handling exploits

Threat Alarm	Severity	Threat Description	Suggestion
MySQL exploit	Low	If SA detects that an ECS instance is attacked using the MySQL vulnerability, the ECS instance is attacked using the MySQL vulnerability.	The main cause of the attack is that the MySQL service is enabled on the public network for the ECS instance. Therefore, you are advised to perform the following operations: <ol style="list-style-type: none"> 1. Configure security group rules and forbid the MySQL service from accessing the public network. 2. Unbind the ELB, and disable the MySQL service from accessing the public network.
Redis exploit	Low	If SA detects that an ECS instance is attacked using the Redis vulnerability, the ECS instance is attacked using the Redis vulnerability.	The main cause of the attack is that the Redis service is enabled on the public network for the ECS instance. Therefore, you are advised to perform the following operations: <ol style="list-style-type: none"> 1. Configure security group rules and forbid the Redis service from accessing the public network. 2. Unbind the ELB, and disable the Redis service from accessing the public network.

7.4.5 Zombie

Overview

A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus, or Trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction. Attackers send commands to "zombies" through control channels and order them to send forged or junk packets to targets. As a result, the targets fail to respond and deny normal services. This is a common DDoS attack. Now, as virtual currencies, such as Bitcoins, grow in value, attackers start using zombies to mine Bitcoins.

Suggestion

When a zombie threat is detected, the ECS instance is detected to have mining behavior (for example, accessing the address of the mining pool), or initiate DDoS

attacks or brute force attacks, the ECS instance may have been implanted with mining Trojan horses or backdoor programs and may become a botnet. The severity of this type of threat is **High**. Therefore, you are advised to perform the following operations:

1. Scan for and remove viruses and Trojan horses on the ECS instance. If the scanning and removal fail, disable the instance.
2. Check whether other hosts on the subnet where the instance resides are intruded.
3. Purchase HSS.

7.4.6 Command and Control

Overview

A Domain Generation Algorithm (DGA) is an algorithm that uses random characters to generate command and control (C&C) domain names. It is commonly used by attackers to avoid domain name blacklist detection. Attackers register with malicious domain names generated by DGA and point them to C&C servers. When victims run malicious programs, their hosts connect to C&C servers through the malicious domain names. Then, attackers can remotely control the hosts.

Suggestion

If a C&C threat is detected, the ECS instance may access the DGA domain name, access the remote C&C server, or establish a channel to connect to the C&C server. A malicious software access or connection behavior indicates that the ECS instance may be remotely controlled by the C&C server and may become a member of the botnet. The severity of this type of threat is **High**. Therefore, you are advised to perform the following operations:

1. Scan for and remove viruses and Trojan horses on the ECS instance. If the scanning and removal fail, disable the instance.
2. Check whether other hosts on the subnet where the instance resides are intruded.
3. Purchase HSS.

7.4.7 Abnormal Behavior

Overview

Abnormal behavior refers to the events that should not occur on hosts. For example, a user logs in to the system during an unauthorized time period, some file directories are changed unexpectedly, or an error occurs in the process. Many of these events are caused by malware. We should keep alert for abnormal behavior. Abnormal behavior data in SA mainly comes from linked services Host Security Service (HSS) and Web Application Firewall (WAF).

Suggestion

If an abnormal behavior threat is detected, handle the threat by following the instructions in [Table 7-3](#).

Table 7-3 Suggestions on handling some abnormal behavior threats

Threat Alarm	Severity	Threat Description	Suggestion
File directory change monitoring event	Informational	Malicious modifications on key file of ECS instances.	Log in to the HSS console and perform the processing.
System login audit event	Informational	Abnormal logins to ECS instances.	Log in to the HSS console and perform the processing.
Abnormal process behavior	Low	Process exceptions on ECS instances, which may be a malicious program.	Log in to the HSS console and perform the processing.

8 Baseline Inspection

8.1 Cloud Service Baseline Overview

SA can check cloud service baseline settings. SA can scan cloud services for risks in key configuration items, report scan results by category, generate alarms for events, and provide hardening suggestions and guidelines.

Limitations and Constraints

- The SA basic edition does not support baseline inspection. To learn about the cloud service configuration status and keep cloud service configuration appropriate, we recommend the professional edition.
- Your account must have required permissions. To use baseline inspections, ensure that the **SA FullAccess**, **SA ReadOnlyAccess**, **Tenant Administrator**, and IAM-related permissions are assigned to the account you want to use. For details about how to configure the **Tenant Administrator** permission and IAM-related permissions, see [Configuring Permissions to Use Baseline Inspection](#).

8.2 Configuring Permissions to Use Baseline Inspection

To use functions in the **Baseline Inspection** module, 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.

Prerequisites

You have obtained the administrator account and its password.

Configuring Permissions to Use Baseline Inspection

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": [
    {
      "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**.

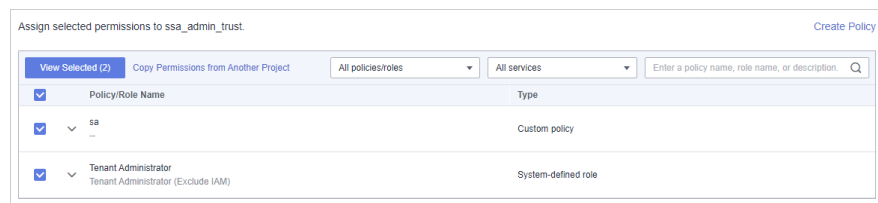
Step 4 In the navigation pane on the left, choose **Agencies**.

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 8-1 Baseline inspection permissions



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

Step 9 Click **OK**.

----End

8.3 Configuring a Baseline Inspection Plan

You can configure a baseline inspection plan and let SA check whether there are unsafe baseline configurations on your servers.

This document describes how to add, edit, and delete a baseline inspection plan.

Background

After you enable baseline inspection, SA will check all of your assets based on the default check plan. By default, the default check plan works as follows:


- **Schedule:** The default check plan checks your assets every three days from 00:00 to 06:00.
- **Objects:** All assets under your account in the current region will be checked.

Constraints

A security standard can be added to only one check plan.

Creating a Check Plan

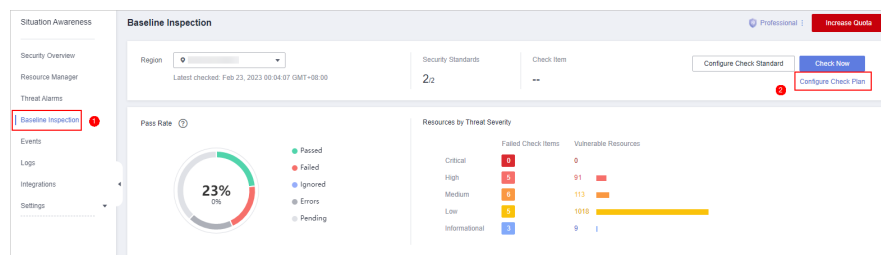
Step 1 Log in to the management console.

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

Step 3 Go to the page for configuring a check plan by following either method below:

- **Method 1**
 - a. In the navigation pane on the left, choose **Baseline Inspection**.
 - b. Click **Configure Check Plan** in the upper right corner of the page.

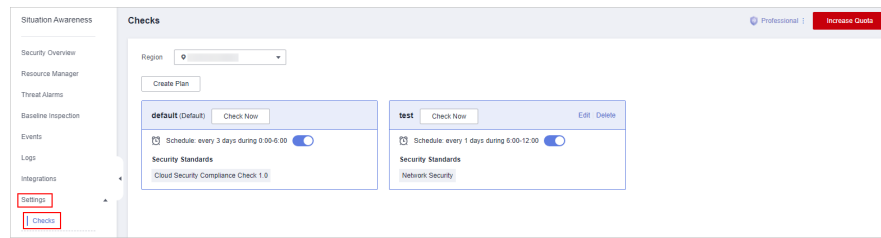
Figure 8-2 Accessing the page for configuring check plans



- **Method 2**

In the navigation pane on the left, choose **Settings > Checks**.

Figure 8-3 Configuring checks



Step 4 On the **Checks** page, select a region for the plan and click **Create Plan**. The pane for creating a check plan is displayed on the right.

Step 5 Configure the check plan.

1. Enter the basic information by referring to [Table 8-1](#).

Table 8-1 Basic information about a check plan


Parameter	Description
Name	Name you specify for the check plan.
Schedule	Select how often and when the check plan is executed. <ul style="list-style-type: none"> - Schedule: every day, every 3 days, every 7 days, every 15 days, or every 30 days - Check triggering time: 00:00-06:00, 06:00-12:00, 12:00-18:00, and 18:00-24:00

2. Select a security standard for the plan.
Select the baseline check items to be checked. For details, see [Cloud Service Baseline Overview](#).
3. Click **OK**.
The check plan is created.
SA will scan the cloud service baseline at the specified time. You can view the scanning results on the **Baseline Inspection** page.

----End

Follow-up Operations

After a baseline check plan is created, you can view, edit, or delete the check plan.

- Viewing a check plan
 - a. Log in to the management console.
 - b. Click  in the upper left corner of the page and choose **Security > Situation Awareness**.
 - c. In the navigation pane on the left, choose **Settings > Checks**.
 - d. On the **Checks** page, view the check plans of baseline inspection.

- Editing a check plan
 - a. In the upper right corner of the check plan box, click **Edit**. The pane for editing the check plan is displayed on the right.
 - b. Edit check plan settings.
 - c. Click **OK**.
- Deleting a check plan
 - a. In the upper right corner of the check plan box, click **Delete**.
 - b. In the displayed dialog box, click **Yes**.

8.4 Executing a Baseline Inspection Plan

Baseline check items are classified into automatic check items and manual check items. This topic describes how to perform automatic check items.

To learn about the latest status of the cloud service baseline configurations, execute or let SA execute a check plan. Then you can view which configurations are unsafe in the check results.

The baseline inspection supports periodic and immediate checks.

- Periodic check: SA periodically executes the default check plan or the check plans you configure. SA executes the default check plan at 00:00 every three days.
- Immediate check: You can add or modify a custom check plan and start the check plan immediately. In this way, you can check whether the servers have certain unsafe configurations in real time.

Constraints

- An immediate check task can be executed only once within 10 minutes.
- A periodic check can be manually started only once within 10 minutes.


Prerequisites

You have created your own check plans.

Immediately Executing the All Configured Security Standard

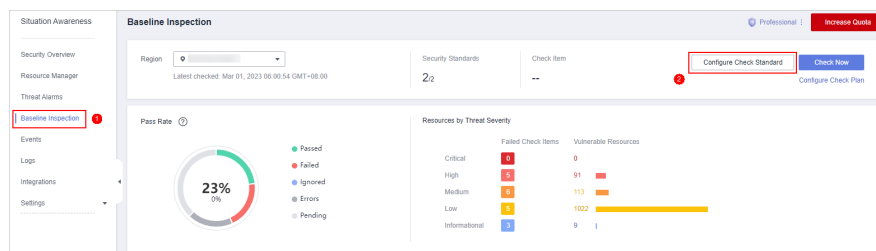
SA will immediately execute check plan you configured.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Baseline Inspection**. In the upper right corner of the page, click **Configure Check standard**.

Figure 8-4 Baseline Inspection



Step 4 In the displayed **Select Check Standard** dialog box, select a standard and click **OK**.

Step 5 In the upper right corner of the page, click **Check Now**.

Refresh the page and check the details next to **Latest Checked** to ensure that the latest check result is displayed.


The system executes the configured security standard immediately.

----End

Executing a Specific Check Plan Immediately

The following describes how to manually execute a check plan immediately.

Step 1 Log in to the management console.

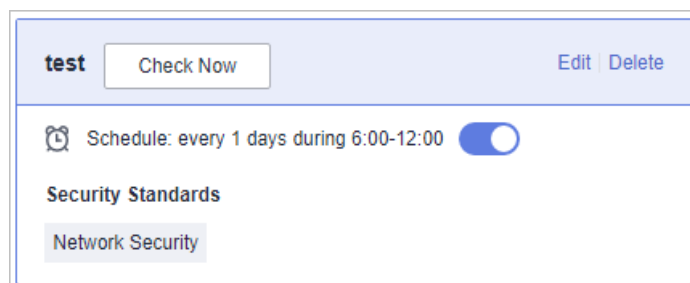
Step 2 Click  in the upper left corner of the page and choose **Security > Situation Awareness**.

Step 3 In the navigation pane on the left, choose **Settings > Checks**.

Step 4 On the **Checks** page, select a region for the check plan.

Step 5 Locate the row that contains the check plan you want and click **Check Now**.

Figure 8-5 Executing a specific check plan



SA immediately executes the selected baseline check plan.

----End

8.5 Performing a Manual Check

Baseline check items are classified into automatic check items and manual check items. This topic describes how to perform manual check items.

There are some manual check items included in baseline inspection. After you finish a manual check, report the check results to SA. The pass rate is calculated based on results from both manual and automatic checks.

Prerequisites

- You have completed the check offline.

Constraints and Limitations

Manual check results must be reported every 7 days as your feedback is valid only for 7 days.

Procedure


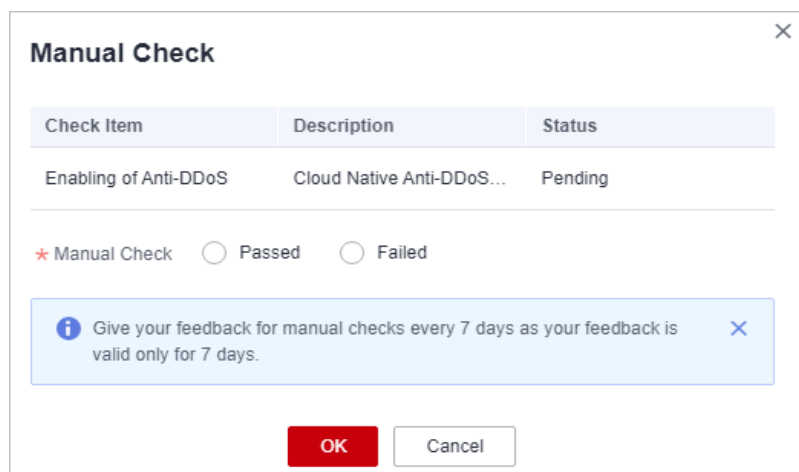
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > Situation Awareness**.
- Step 3** In the navigation pane on the left, choose **Baseline Inspection**.
- Step 4** Select the region where the check result to be viewed is located.
- Step 5** In the **Operation** column of the target manual check item, click **Manual Check**.
- Step 6** In the displayed dialog box, select a result and click **OK**.

Figure 8-6 Reporting manual check results to SA



 NOTE

Report manual check results every 7 days as your feedback is valid only for 7 days.

----End

8.6 Viewing Baseline Inspection Results

This topic describes how to view the baseline inspection results. You can learn about the affected assets and details about check items of baseline inspection.


Prerequisites

- The cloud service baseline has been scanned.

Viewing All Check Results

View the check results of all check items in a region.

Step 1 Log in to the management console.

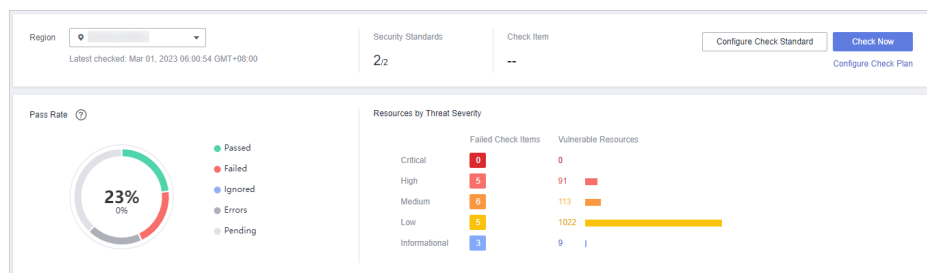
Step 2 Click  in the upper left corner of the page and choose **Security > Situation Awareness**.

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

Step 4 Select a region you want to view results. The system will display the check result data for the selected region only.

Step 5 View the baseline check result statistic of the selected region.

Figure 8-7 Check Result Statistics




- **Security Standards:** number of security standards involved in the latest check/Total security standards
- **Check Item:** number of all check items in the latest baseline check.
- **Pass Rate:** check item pass rate of the latest baseline check.
Overall pass rate = Passed check items/Total check items
Total check items include check items for every standard
The check result can be **Passed, Failed, Errors, or Pending**.
- **Resources by Threat Severity:** displays the number of vulnerable resources by severity.

Severity: Critical, High, Medium, Low, and Informational.

----End

Viewing Baseline Inspection Security Standards

Step 1 Log in to the management console.

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

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

Step 4 Select a region you want to view the results for and click the **Security Standards** tab.

Step 5 Select **All**. The system displays all security standards and their details for the current region.

The **Security Standards** tab displays all baseline check standards and other details, including the check item, status, category, vulnerable resources, description, and latest check time.


NOTE

You can select a baseline check standard and view the baseline check items included in the standard.

----End

Viewing Details About a Specific Security Standard

Step 1 Log in to the management console.

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

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

Step 4 Select a region for the security standard you want and click the **Security Standards** tab.

Step 5 In the security standards list, locate the security standard you want and click **View Details** in the **Operation**.

Step 6 On the check item details page, view the detailed information about the check item.


View the detailed description, check message, and check result of the check item.

----End

Viewing Checked Resources

Only checked resources are listed.

Step 1 Log in to the management console.

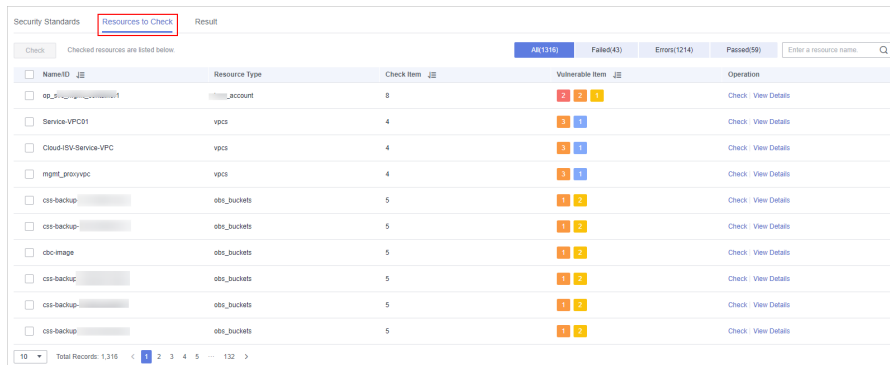
Step 2 Click  in the upper left corner of the page and choose **Security > Situation Awareness**.

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

Step 4 Select a region you want.

Step 5 Click the **Resources to Check** tab. All checked resources in the current region and their details are displayed.

Figure 8-8 All resources to check




Check	NameID	Resource Type	Check Item	Vulnerable Item	Operation
<input type="checkbox"/>	op_...	account	8	2 2 1	Check View Details
<input type="checkbox"/>	Service-VPC01	vpcs	4	3 1	Check View Details
<input type="checkbox"/>	Cloud-ISV-Service-VPC	vpcs	4	3 1	Check View Details
<input type="checkbox"/>	mngt_errorypc	vpcs	4	3 1	Check View Details
<input type="checkbox"/>	oss-backup-	obs_buckets	5	1 1 2	Check View Details
<input type="checkbox"/>	oss-backup-	obs_buckets	5	1 1 2	Check View Details
<input type="checkbox"/>	obs-image	obs_buckets	5	1 1 2	Check View Details
<input type="checkbox"/>	oss-backup-	obs_buckets	5	1 1 2	Check View Details
<input type="checkbox"/>	oss-backup-	obs_buckets	5	1 1 2	Check View Details

The **Resources to Check** tab displays all checked resources and their details, including the resource name, resource type, check items, and vulnerable items.

----End

Viewing Check Details of A Specific Resource

Step 1 Log in to the management console.

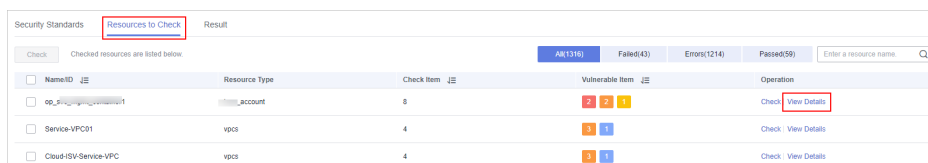
Step 2 Click  in the upper left corner of the page and choose **Security > Situation Awareness**.

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

Step 4 Select a region you want and click the **Resources to Check** tab.

Step 5 In the checked resource list, locate the resource you want and click **View Details** in the **Operation** column.

Figure 8-9 Resources to Check



Check	NameID	Resource Type	Check Item	Vulnerable Item	Operation
<input type="checkbox"/>	op_...	account	8	2 2 1	Check View Details
<input type="checkbox"/>	Service-VPC01	vpcs	4	3 1	Check View Details
<input type="checkbox"/>	Cloud-ISV-Service-VPC	vpcs	4	3 1	Check View Details

Step 6 On the displayed page, view the resource details.

View the check items, status, check method, and latest check time.

Figure 8-10 Details page of a checked resource

Resource Name	Resource Type	Result	Latest Check	Recommendation	Operation
Service-VPC 5cb5a7cd-3e...	vpc	Failed	Mar 01, 2023 00:00:12 GMT+08:00	This is a high-risk operation. Exercise caut...	Check View Details
Service-VPC 5cb5a7cd-3e...	vpc	Failed	Mar 01, 2023 00:00:03 GMT+08:00	--	Check View Details
Service-VPC 5cb5a7cd-3e...	vpc	Failed	Mar 01, 2023 00:00:02 GMT+08:00	--	Check View Details
Service-VPC 5cb5a7cd-3e...	vpc	Failed	Mar 01, 2023 00:00:04 GMT+08:00	--	Check View Details

----End

Viewing Check Results


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > Situation Awareness**.
- Step 3** In the navigation pane on the left, choose **Baseline Inspection**.
- Step 4** Select a region you want.
- Step 5** Click the **Result** tab. All the check results in the current region and their details are displayed.

Figure 8-11 All check results

Check Item	Result	Resource Type	Resource Name/ID	Schedule	Operation
Administrator Account AK39K	Failed	account	...	Mar 01, 2023 00:00:37 GMT+08:00	Check View Details
OBS bucket ACL permissions	Passed	obs_buckets	...	Mar 01, 2023 00:00:49 GMT+08:00	Check View Details
SA professional edition	Passed	project	...	Mar 01, 2023 00:00:47 GMT+08:00	Check View Details
OBS bucket server-side encryption	Failed	obs_buckets	...	Mar 01, 2023 00:00:48 GMT+08:00	Check View Details
Security group inbound rules	Failed	security_groups	...	Mar 01, 2023 00:00:48 GMT+08:00	Check View Details
Security group inbound rules	Failed	security_groups	...	Mar 01, 2023 00:00:48 GMT+08:00	Check View Details
Security group inbound rules	Failed	security_groups	...	Mar 01, 2023 00:00:48 GMT+08:00	Check View Details
Log metric filtering and alarm events (net...	Failed	vpc	...	Feb 27, 2023 00:00:43 GMT+08:00	Check View Details
Log metric filtering and alarm events (net...	Failed	vpc	...	Feb 27, 2023 00:00:43 GMT+08:00	Check View Details
Session timeout policy	Failed	account	...	Feb 27, 2023 00:00:47 GMT+08:00	Check View Details

The **Result** tab lists all check results and their details, including the check items, check results, resource types, resource names, and latest check time.

----End

8.7 Handling Baseline Inspection Results

This topic describes how to handle unsafe settings by referring to recommended fixes and how to report manual check results to SA.

Prerequisites

- The cloud service baseline has been scanned.

Handling Unsafe Settings


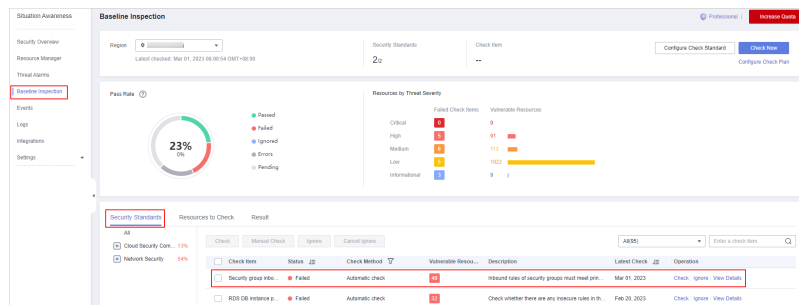
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > Situation Awareness**.
- Step 3** In the navigation pane on the left, choose **Baseline Inspection**.
- Step 4** Select the region where the check result to be viewed is located.
- Step 5** On the **Security Standards** tab, select a check item, and view its risk status.

Figure 8-12 Check item status



- If the icon of a check item status is green, the configuration is correct and no unsafe settings found.
- If the icon of a check item status is red, there may be inappropriate configurations and the assets may have potential risks.

- Step 6** In the **Operation** column of the specific check, click **View Details**.
- Step 7** View the risk details and fix the unsafe settings by referring to **Result** and **Reference**.

Table 8-2 Check item description

Parameter	Description
Status	Displays the check status of the current check item. <ul style="list-style-type: none"> If the result is Passed, the configuration corresponding to the check item is appropriate. If the result is Failed, the configuration corresponding to the check item is inappropriate. The check results will be listed.
Latest Check	Last time when the current check item was performed.
Check Method	Method used by the current check item.

Parameter	Description
Severity	Severity of the unsafe settings discovered against the current check item.
Impact	Security impact caused by unsafe settings discovered against the current check item.
Standard and Category	Security standard and category of the current check item.
Description	Check content of the current check items.
Check Process	Check process of the current check item.
Reference	Links of documentation related to the check item. Click the reference link to go to the detailed page.
Resource	Resource to which the current check item belongs. The check result can be Passed or Failed . <ul style="list-style-type: none"> • If the result is Passed, the configuration corresponding to the check item is appropriate. • If unsafe settings are found, the detailed information is listed. You can click the button in the Operation column to go to page and fix the configuration.


Step 8 After all unsafe configurations are rectified, click **Check** to verify that all risky items have been rectified.

----End

Reporting Manual Check Results to SA

For manual check items, after you finish each check, report the check results to SA. The pass rate is calculated based on results from both manual and automatic checks.

Step 1 Log in to the management console.

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

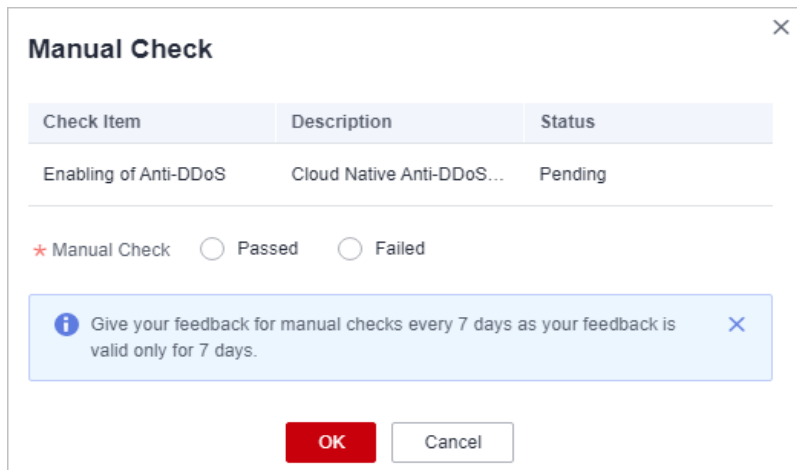
Step 3 In the navigation pane on the left, choose **Baseline Inspection**.

Step 4 Select the region where the check result to be viewed is located.

Step 5 In the **Operation** column of the target manual check item, click **Manual Check**.

Step 6 In the displayed dialog box, select a result and click **OK**.

Figure 8-13 Reporting manual check results to SA



NOTE

Report manual check results every 7 days as your feedback is valid only for 7 days.

----End

9 Events

9.1 Viewing Events

The **Events** page gives you a full view of your asset security status, helping you determine the priority of handling the events in a timely manner and analyze the security trends.

On the **Events** page, you can:

- View information about threat alarms, vulnerabilities, risks, compliance check, violations, and public opinions.
- View real-time detection data from other security products.
- Filter events by time range or filter. The events of the last seven days are displayed by default.
- View detailed events on the console or view them in JSON format.
- Customize the event list.
- Mark the processing status of events

Constraints


- When you search for events by filter, a maximum of 10,000 events can be displayed.
- Only the events of the last 180 days can be displayed.

Prerequisites

- SA has received the detection results or events from other security products.

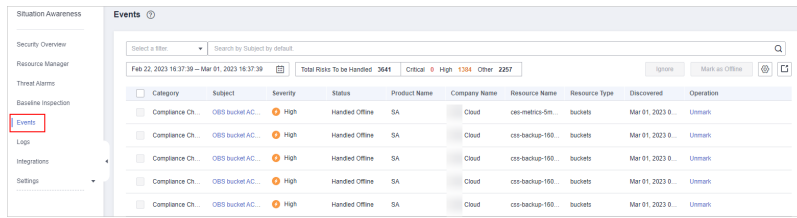
Procedure

Step 1 Log in to the management console.



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

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

Figure 9-1 Viewing Events



Step 4 Filter and view events.

- Select a filter, click , and view the event displayed.
- If there are still a large number of events after filtering, add one or more filter criteria and/or select a time range to quickly search for events you want.
 - To add one or more filter criteria, configure the corresponding categories in the filter box and then click .
 - To specify a time range, configure a time period in the time filter box and click **OK**.

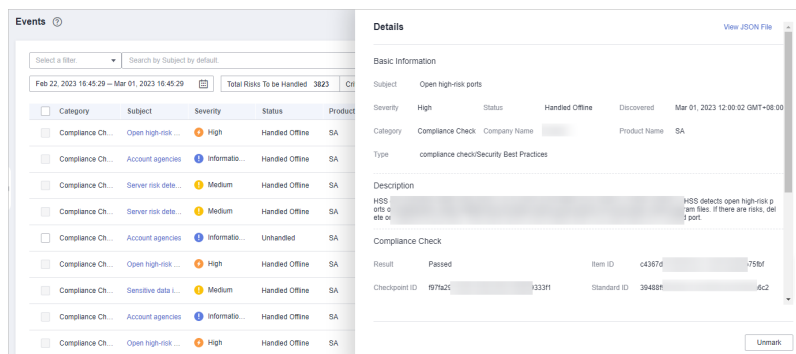
Step 5 View the event list.

In the displayed list, only the events matching the filter criteria are displayed, as well as their statistics.

Step 6 View the details of an event.

1. Locate the row of the event you want to view, click the subject in the **Subject** column. The **Details** pane is displayed on the right.

Figure 9-2 Details



2. On this pane, the **Basic Information**, **Description**, **Resource Information**, **Attack Information**, and **Tenant Information** are listed.
3. On the **Details** pane, Click **View JSON File** in the upper right corner to view the event details in a JSON file.

----End

9.2 Handling Events

After you receive an event, you can mark its processing status.

- **Ignore:** If the event does not cause any harm, ignore the result. After click **Ignore**, record the **Handler** and **Reason** in the **Ignore Risk** dialog box.
- **Mark as Offline:** If the event has been handled offline, click **Mark as Offline** in the **Operation** column. In the displayed dialog box, fill in **Processor**, **Processing Time**, and **Processing Result**, and click **OK**.

 **NOTE**

On the **Events** page, SA also aggregates alarm data reported by other security services, such as Host Security Service (HSS), and Web Application Firewall (WAF). When you handle these alarms, follow the sequence below:

1. View the **Product Name** column to locate the source service that reports an alarm to SA.
2. Go to the source service to handle the alarm.
3. Mark the alarm in SA after it is handled in the source service.


For example, if an event is reported by HSS, it is recommended that you handle the alarm on the HSS console first and then mark the alarm in SA.

Prerequisites

SA has received events from other security products.

Procedure

Step 1 Log in to the management console.

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

Step 3 Filter events.

Step 4 Mark events in batches.

Select one or more events in the **Unhandled** status and click **Ignore** or **Mark as Offline** above the result list to handle all selected events at a time.

Step 5 Mark an event.

- In the **Operation** column of the event you want to mark, click **Ignore** or **Mark as Offline**.
- Alternatively, you can mark a single event on its **Result Details** page by clicking **Ignore** or **Mark as Offline** at the lower right corner.

----End

9.3 Exporting Events

You can export all events with just a few clicks.

The exported Excel file contains **Product Name**, **Company Name**, **Affected Resources**, **Category**, **Severity**, **Subject**, **Discovered**, **Occurrences**, **Confidence**, **Importance**, and **Status**.

Constraints


- When you search events with a filter, a maximum of 10,000 events can be exported.
- Only the events of the last 180 days can be exported.

Prerequisites


- SA has received the events from other security products.

Procedure

Step 1 Log in to the management console.

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

Step 3 Filter events.

Step 4 Click  to export the filtered events to a .csv file and save it locally.
You can then view them offline.

----End

9.4 Customizing the Event List


You can customize the event list.


Prerequisites

- SA has received the events from other security products.

Procedure

Step 1 Log in to the management console.

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

Step 3 Click  to expand all column options of the event list.

Step 4 Select the columns you want to display.

Step 5 Refresh the event list.

----End

9.5 Managing Filters

You can create different filters to let SA show the events you expect. For example, you can create a filter by adding the product name and resource type, such as

Host Security Service and **ECS instance**. Then you can select this filter to search events meeting both of those two conditions.

Currently, the following conditions and attributes can be added to a filter:

- **Subject:** indicates the title of the event. You can enter keywords. By default, **Subject** is selected.
- **Severity:** indicates severity of the event. The options are **Critical, High, Medium, Low, and Informational**.
- **Category:** indicates the category of the event. The options include **Threat alarm, Vulnerability, Violation, Risk, Public opinion, Security notice, and Compliance check**.
- **Status:** indicates the processing status of the event. The options are **Unhandled, Ignored, and Handled Offline**.
- **Resource Name:** indicates the name of the resource for which an event is generated. Enter the full name of the resource.
- **Resource Type:** indicates the type of the resource for which an event is generated. The options are **ECS instance, VPC, Security Group, EIP, Disk, and Others**.
- **Company Name:** indicates the name of the company from whose product the event is reported. Enter the full name of the company.
- **Product Name:** indicates the name of the product from which the event is reported. Enter the full product name.


Constraints

A filter can contain only one:

- **Subject**
- **Resource Name**
- **Company Name**
- **Product Name**

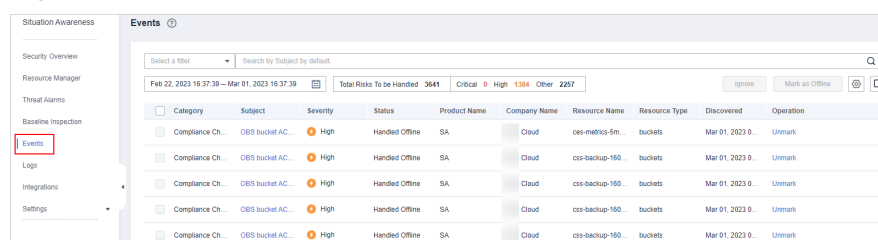
Creating a Filter

Step 1 Log in to the management console.

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

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


Figure 9-3 Events




Category	Subject	Severity	Status	Product Name	Company Name	Resource Name	Resource Type	Discovered	Operation
Compliance Ch...	OBS bucket AC...	High	Handled Offline	SA		oss-metrics-5m...	buckets	Mar 01, 2023 0...	Unmark
Compliance Ch...	OBS bucket AC...	High	Handled Offline	SA		css-backup-100...	buckets	Mar 01, 2023 0...	Unmark
Compliance Ch...	OBS bucket AC...	High	Handled Offline	SA		css-backup-100...	buckets	Mar 01, 2023 0...	Unmark
Compliance Ch...	OBS bucket AC...	High	Handled Offline	SA		css-backup-100...	buckets	Mar 01, 2023 0...	Unmark
Compliance Ch...	OBS bucket AC...	High	Handled Offline	SA		css-backup-100...	buckets	Mar 01, 2023 0...	Unmark

- Step 4** Add conditions to the filter.
- Click the search box, select one or more filter criteria, and set attributes.
 - In the time filter box, select a time range.
- Step 5** Click **Save** on the right of the search box. The **Save as Filter** dialog box is displayed.
- Step 6** Configure the filter.
- Set the **Filter Name**.
 - (Optional) Select **Set as default filter**.
- Step 7** Click **OK**.
- End

Modifying a Filter

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > Situation Awareness**.
- Step 3** In the navigation pane on the left, choose **Events**.
- Step 4** In the filter area, select a filter.
- Step 5** Click **Edit** next to the filter box.
- Step 6** Modify the filter name.
- Step 7** Click **OK**.
- End

Deleting a Filter

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > Situation Awareness**.
- Step 3** In the navigation pane on the left, choose **Events**.
- Step 4** In the filter area, select a filter.
- Step 5** Click **Edit** next to the filter box.
- Step 6** Click **Delete**.
- End

10 Logs

You can authorize Object Storage Service (OBS) to store SA logs in OBS buckets. This makes it easier for you to store and export SA logs securely and meet audit requirements for storing logs for 180 days.

Overview

OBS allows you to store SA logs as long as you want and export all the logs you want at any time. Logs transferred to OBS buckets can be stored permanently and downloaded locally.

Prerequisites


- Your professional edition SA is available.
- Your account must have required permissions. To manage resources, your account should have the **SA FullAccess**, **SA ReadOnlyAccess**, and **Tenant Administrator** permissions.

For details about **Tenant Administrator**, see sa_01_0016.html#section753419154403

Creating an OBS Bucket for Storing Logs

To meet the security audit requirements for storing logs for at least 180 days, you can transfer logs to an OBS bucket for long-term storage. You can also download transferred logs on the OBS console.

Step 1 Log in to the management console.

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

Step 3 In the **Upload to OBS** area, click  to enable OBS.

Figure 10-1 Upload to OBS

Step 4 Configure related parameters. [Table 10-1](#) describes the parameters.

Table 10-1 Log storage parameters


Parameter	Description
Bucket Name	Select an OBS bucket. If no OBS bucket is available, go to the OBS console and create one. NOTE <ul style="list-style-type: none"> Only OBS buckets in the region where the current account is located can be selected. Only Standard and Infrequent Access OBS buckets can be used for LTS.
Object Name	Name you want to use for the object.
Storage Path	Storage path generated based on the bucket name and object name.

Step 5 Click **OK**.

It takes about 10 minutes for the service to upload logs to the bucket.

----End

Other Operations

If you no longer want to store logs in an OBS bucket, in the **Upload to OBS** area, click  to disable the function. This does not delete the logs you have uploaded to the OBS bucket.

11 Integrations

11.1 Managing Integrations

SA integrates a variety of security products to aggregate their detection data and manage all findings in one place.

NOTE

If you want to aggregate events from other products, click **My Recommendations** in the upper right corner of the **Integrations** page and provide details about the product.

This topic walks you through how to manage security product integrations, including enabling and disabling a product integration.

Enabling an Integration

Step 1 Log in to the management console.


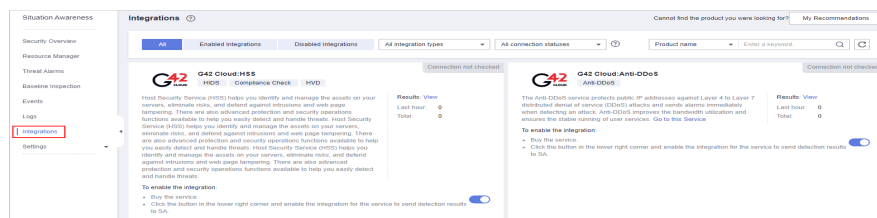
Step 2 Click  in the upper left corner of the page and choose **Security > Situation Awareness > Integrations**.

Figure 11-1 Integrations



Step 3 Query the security products you want to aggregate in SA.

Select the **Disabled Integrations** tab and search for security products you want to enable. For more query methods, see [Viewing Integrations](#).

Step 4 Start to receive events.

Locate the product whose detection data you want to receive in SA and enable the integration.

About 5 minutes after you enable an integration, you will receive the detection data reported by the product.

NOTE

To let SA receive the product events properly, ensure that the corresponding protection of the product has been enabled.

----End

Disabling an Integration

Step 1 Query the security products that have been aggregated in SA.

Select the **Enabled Integrations** tab and search for security products you want. For more query methods, see [Viewing the Integration List](#).

Step 2 Stop to receive results.

Locate the product whose detection data you no longer want to receive in SA and disable the integration.

----End

11.2 Viewing Integrations

You can manage all integrations and view the number of statistics results received from other products.

Viewing the Integration List

Step 1 Log in to the management console.


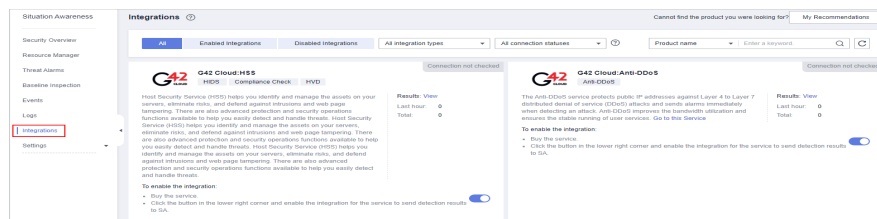
Step 2 Click  in the upper left corner of the page and choose **Security > Situation Awareness > Integrations**.

Figure 11-2 Integrations




Step 3 Select an integration type from the **All integration types** drop-down list and a connection status from **All connection statuses**.

There are two types of integrations: **Detection integrations** and **Analysis integrations**.

Options for connection statuses: **Connected**, **Disconnected**, **Connection not checked**, and **Connection check stopped**.

Step 4 Select **Product Name**, **Product Category**, or **Company Name** to query security products whose detection data can be aggregated in SA.

Step 5 Enter a keyword in the search box and click  to view the products that meet the search criteria.

----End

Viewing Enabled Integrations

Step 1 Log in to the management console.


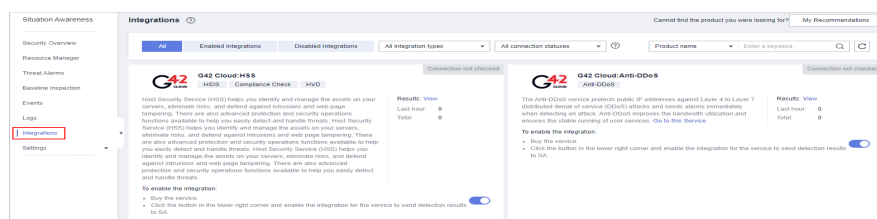
Step 2 Click  in the upper left corner of the page and choose **Security > Situation Awareness > Integrations**.

Figure 11-3 Integrations



Step 3 Query the security products that have been aggregated in SA.

Select the **Enabled integrations** tab, specify the integration type, and select the connection status you want to search for products that meet the search criteria. For more query methods, see [Viewing the Integration List](#).

Step 4 Check the statistics on received events.

- In the column of a specific product, you can view the total number of events received from the product and the number of results received in the last hour.
- Click **View** to go to the **Events** page and view the event list of the product. For more details, see [Viewing All Events](#).

----End

11.3 Checking the Connection Status of an Integration

The connection status reflects the status of reporting detection data of other security products to SA. This function is used to check whether an integration can report data to SA.

Table 11-1 Connection status description

Status	Description
Connected	The data API is called not less than 8 times within one hour. This means the API connectivity is normal, and the integration will properly report detection data to SA. By default, the connection status of an integration is healthy within one hour after the integration is enabled.

Status	Description
Disconnected	The data API is called less than 8 times within one hour. This means the API connectivity is abnormal, and the integration cannot report detection data to SA.
Connection check stopped	The integration no longer reports detection data to SA.
Connection not checked	The integration never reports detection data to SA.

NOTE

The connection status of an integration is determined by how many times the integration calls the data reporting API. An integration can call the data reporting API every 5 minutes to check the connectivity.

Procedure

Step 1 Log in to the management console.


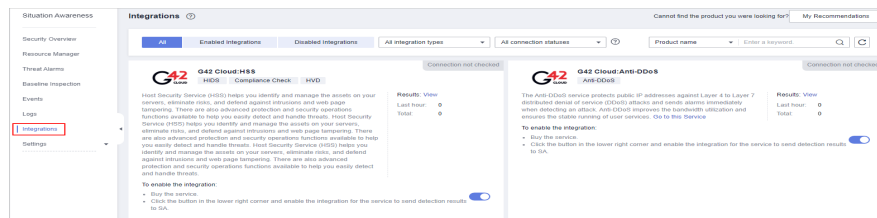
Step 2 Click  in the upper left corner of the page and choose **Security > Situation Awareness > Integrations**.

Figure 11-4 Integrations



Step 3 In the connection status drop-down list, select a status. All integrations in the selected status will be displayed.

Step 4 In the panel for a specific integration, view the data volume received from and the connection status of the integration.

----End

12 Settings

12.1 Check Settings

This topic describes how to create baseline check plans. To use cloud service baseline inspection, create your check plans first.

Procedure


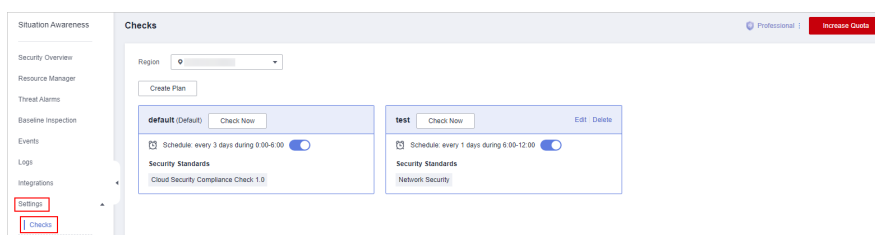
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Security > Situation Awareness**.
- Step 3** In the navigation pane on the left, choose **Settings > Checks**.

Figure 12-1 Configuring checks



- Step 4** On the **Checks** page, select a region for the plan and click **Create Plan**. The pane for creating a check plan is displayed on the right.
- Step 5** Configure the check plan.
 1. Enter the basic information by referring to [Table 12-1](#).

Table 12-1 Basic information about a check plan

Parameter	Description
Name	Name you specify for the check plan.

Parameter	Description
Schedule	Select how often and when the check plan is executed. <ul style="list-style-type: none"> - Schedule: every day, every 3 days, every 7 days, every 15 days, or every 30 days - Check triggering time: 00:00-06:00, 06:00-12:00, 12:00-18:00, and 18:00-24:00

2. Select a security standard for the plan.
Select the baseline check items to be checked. For details, see [Cloud Service Baseline Overview](#).
3. Click **OK**.

Step 6 The check plan is created.

SA will execute the cloud service baseline inspection at the specified time. To view the check result, choose **Security > Situation Awareness > Baseline Inspection**.

----End

13 FAQs

13.1 Product Consulting

13.1.1 What Does SA Do?

Situation Awareness (SA) is a visualized threat detection and analysis platform. SA 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.

13.1.2 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.

13.1.3 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). 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.


13.1.4 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 professional SA, you can view vulnerable assets on the **Resource Manager** page. This function is not included in the basic edition.

Procedure

Step 1 Log in to the management console.

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

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

----End

13.1.5 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 13-1 summarizes SA and other security services.

Table 13-1 Differences between SA and other services

Service Name	Service Category	Dependency and Difference	Protected Object
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
Anti-DDoS	Network security	Anti-DDoS detects and defends against DDoS attacks. It synchronizes attack logs and protection data to SA.	Service stability
HSS	Host security	HSS detects server risks and protects servers with protection policies. It synchronizes alarms and protection data to SA.	Servers
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
DBSS	Data security	DBSS protects and audits database access behavior. It synchronizes audit logs and alarm data to SA.	Cloud databases

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

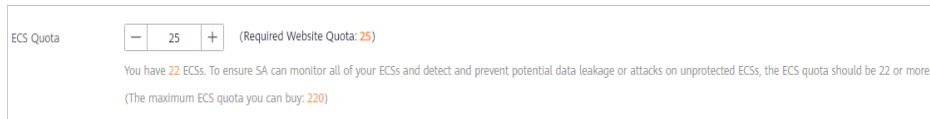
The total ECS quota is the total number of hosts that are authorized to receive detections. When buying SA, ensure that the total ECS quota is greater than or equal to the total number of hosts under the current account. If the total ECS quota is less than the number of hosts, the following impact may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

Figure 13-1 Total ECS Quota

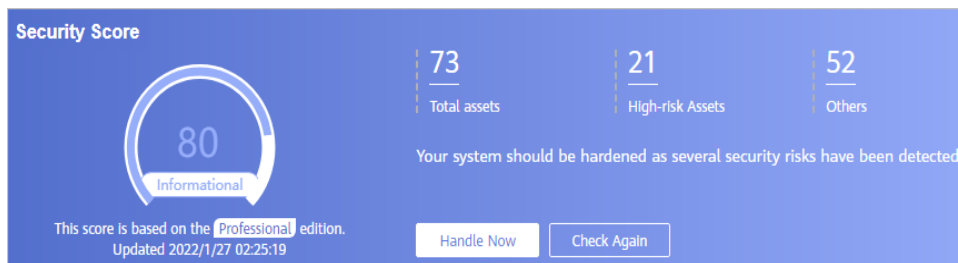


13.1.7 How Do I Update My Security Score?

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 13-2 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 > 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

13.1.8 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.

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 > 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

13.1.9 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": [
    {
      "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**.

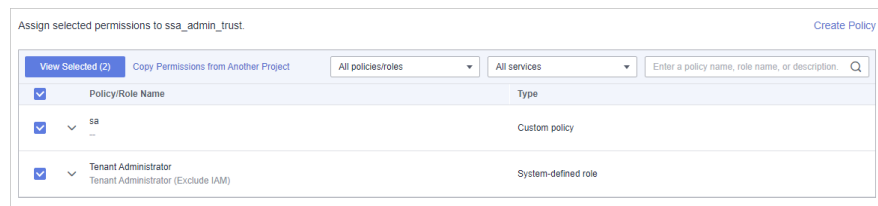
Step 4 In the navigation pane on the left, choose **Agencies**.

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 13-3 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**.

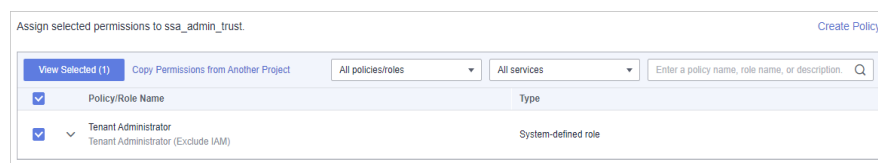
Step 3 In the navigation pane on the left, choose **Agencies**.

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 13-4 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

13.1.10 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.

13.2 Purchase Consulting

13.2.1 How Do I Change the SA Specifications?

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

----End

13.2.2 How Is SA Billed?

SA is billed on a pay-per-use basis. You are billed for usage duration by the hour. This billing mode allows you to enable or disable the SA service at any time.

13.2.3 How Do I Cancel My Subscription to SA?

If you no longer need SA, unsubscribe from it or cancel it in just a few clicks.


- Pay-per-use billing mode: pay for what you use by the hour. This mode allows you to enable or disable resources at any time.

 **NOTE**

The free edition does not support unsubscription.

Unsubscribing from the Pay-per-use Professional Edition 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 **Professional** in the upper right corner. The edition management window is displayed.

Step 4 In the row of the SA edition purchased in pay-per-use billing mode, click **Cancel** to release the purchased SA resources.

Go to the edition management window and verify that the subscription to resources billed on a pay-per-use basis is canceled.

----End

13.2.4 Can I Use SA for Free?

Yes.

SA provides the basic and professional editions.

- You can use the basic edition for free for a long time.
- The professional edition is billed on a pay-per-use basis.

For details about function differences, see [Features](#).

A Change History

Released On	Description
2023-04-24	<p>This issue is the second official release.</p> <ul style="list-style-type: none"> Added Creating a User and Granting Permissions, Increasing Asset Quotas, Unsubscribing from SA, Handling Alarms and Events, How Do I Get Information About the Most Vulnerable Assets?, What Are the Dependencies and Differences Between SA and Other Security Services?, Why Cannot the Total ECS Quota Be Less Than the Number of Existing ECSs? and Why Is the Event Data in SA Inconsistent with That in WAF and HSS? Updated the content and figures in Resource Manager, Baseline Inspection, Events and Integrations.
2023-01-10	<p>This issue is the first official release.</p>