Situation Awareness

User Guide

Issue 12

Date 2022-11-24

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Permissions Management

1.1 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 to 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 1-1** shows the process.

Prerequisites

Learn about the permissions supported by SA and choose policies or roles based on your requirements. For details, see **SA permissions**.

Table 1-1 lists all the system-defined roles and policies supported by SA.

Table 1-1 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:

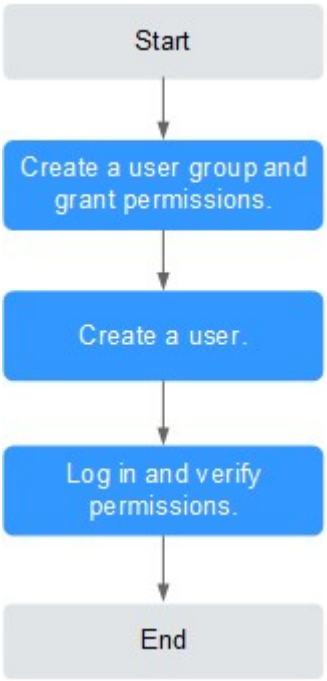
- Configure all SA permissions: **SA FullAccess** and **Tenant Guest**.

  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 1-1 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?**

1.2 SA Custom Policies

Custom policies can be created to supplement the system-defined policies of SA. For the actions that can be added to custom policies, see **SA Permissions and Supported Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For more details, see **Creating a Custom Policy**. The following section contains examples of common SA custom policies.

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:*"
         ]
      }
   ]
}
```

1.3 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.

2 Editions

2.1 Selecting a Billing Mode

2.1.1 Yearly/Monthly Pricing

Yearly/Monthly is a prepaid billing mode in which resources are billed based on the service duration. This cost-effective mode is ideal when the duration of resource usage is predictable.

Applicable Resources

SA asset quota, which is mainly the server quota.

If you want to buy yearly/monthly-billed SA, you can buy asset quotas in one order.

2.1.2 Pay-per-use Billing

In pay-per-use billing mode, a postpaid mode, your resources are billed on an hourly basis, and you can subscribe to or unsubscribe from a resource at any time. The system generates bills every hour based on the actual resource usage (how long you use the SA service) and deducts fees from your account balance.

Pay-per-use Resources

SA asset quota, which is mainly the host quota.

2.1.3 Changing the Billing Mode from Pay-per-Use to Yearly/Monthly

- **Pay-per-use** is a postpaid billing mode. In this mode, your SA is billed by usage duration, and you can enable or disable the SA service at any time.
- **Yearly/Monthly** is a prepaid billing mode. In this mode, your SA is billed based on required duration. This mode is more cost-effective than the pay-per-use mode and applicable when your resource usage period can be estimated.

If you plan to use SA for a long time, you can change the billing mode to yearly/monthly to save money.

Prerequisites

You have purchased the pay-per-use professional edition, including asset quotas.

Procedure

Step 1 Log in to the management console.

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

Step 3 Click **Professional** in the upper right corner. The edition management window is displayed.

Step 4 In the row of purchased quota billed on a pay-per-use basis, click **Change to Yearly/Monthly**.

Step 5 Confirm the resource information and select the required duration.

Step 6 Click **Pay Now** to pay the order

----End

2.2 Purchasing the Standard Edition

Overview

SA is **about to go offline**. SA capabilities have been integrated into **SecMaster**. To prevent your services from being affected, you are advised to use SecMaster. For details, see **Buying SecMaster**.

SA provides basic, standard, and professional editions for you.

- You can try the basic edition for free.

  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 your SA to the standard or professional edition.
  - The standard edition provides more types of threat detection and analysis services, including threat analysis, alarm settings, ECS vulnerability scanning, and security log management. To use the standard edition, you need to purchase a certain number of quotas based on the number of assets across your account. Each quota can protect one asset.
  - The professional edition can detect a wider range of threats and provides more analysis functions. To let SA protect all your assets, configure the total ECS quota to at least the number of assets you have.
  - For more details, see **Edition Differences**.

NOTICE

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

Prerequisites

- You have obtained credentials for logging in to the management console.

Procedure

Step 1 Log in to the management console.

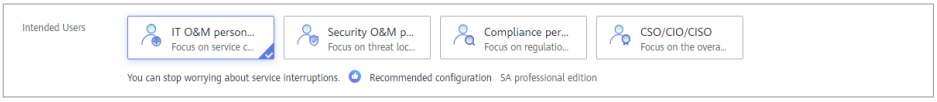
Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

Step 3 In the upper right corner of the page, click **Upgrade**.

Step 4 (Optional) 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.

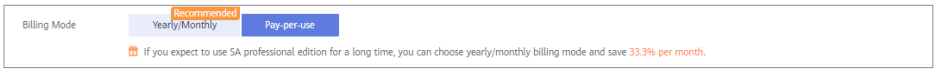
Figure 2-1 Intended Users



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

The standard edition can only be billed on a yearly or monthly basis.

Figure 2-2 Yearly/Monthly billing mode



Step 6 Select **Standard** for **Edition**.

Figure 2-3 Edition

Step 7 Configure required parameters. For details, see **Table 1 Parameter description**.

Table 2-1 Parameter description

Parameter	Description
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 8 Select the required duration.

Figure 2-4 Selecting the required duration

- Configure the required duration.

  If you select **Yearly/Monthly**, **Required Duration** must be configured.

  - You can buy SA by month or by year. The duration can be **1**, **2**, **3**, **4**, **5**, **6**, **7**, **8**, **9 months**, **1 year**, **2 years**, or **3 years**.
  - On the basis of the total price, you can enjoy a 17% discount for a one-year subscription, a 30% discount for a two-year subscription, and a 50% discount for a three-year subscription.
- Select **Auto-renew**. When you enable **Auto-renew**, your subscription will be automatically renewed in a given time before expiration. Be sure that your account balance is abundant for the renewal.

  Table 2-2 Auto-renewal period description

Required Duration	Auto-renewal Period
1, **2**, **3**, **4**, **5**, **6**, **7**, **8**, or **9 months**	1 month
1 year	1 year

NOTE

- You can also configure different required durations for different assets by referring to **Increasing Asset Quotas**.
- For details about how to modify and cancel auto renewal, see **Auto-Renewal Rules**.

Step 9 After configuration completes, click **Next**.

Step 10 On the **Details** page, confirm the order information, read the Situation Awareness Disclaimer, select "I have read and agree to the Situation Awareness Disclaimer", and click **Pay Now**.

Step 11 On the payment page, select a payment method and complete the payment.

Step 12 After the payment is complete, return to the SA console and verify that the purchase takes effect and the expiration date is correct.

----End

Follow-up Operations

Figure 2-5 Edition management window

- To change the asset quota, click **Increase Quota** and complete the purchase by referring to **Increasing Asset Quotas**.
- If the yearly/monthly edition is about to expire or has expired, you can click **Renew** to extend the validity period. For more details, see **Renewal**.
- If you no longer need the asset quota, click **Unsubscribe** or **Cancel** to unsubscribe from the corresponding SA service. For details, see **Unsubscribing**.

2.3 Purchasing the Professional Edition

Background

SA is **about to go offline**. SA capabilities have been integrated into **SecMaster**. To prevent your services from being affected, you are advised to use SecMaster. For details, see **Buying SecMaster**.

SA provides basic, standard, and professional editions for you.

- You can try the basic edition for free.

  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 your SA to the standard or professional edition.
  - The standard edition provides more types of threat detection and analysis services, including threat analysis, alarm settings, ECS vulnerability scanning, and security log management. To use the standard edition, you need to purchase a certain number of quotas based on the number of assets across your account. Each quota can protect one asset.
  - The professional edition can detect a wider range of threats and provides more analysis functions, including threat analysis, alarm settings, host and website vulnerability management, baseline inspection, log management, and large screen. To let SA protect all your assets, configure the total ECS quota to at least the number of assets you have.
  - For more details, see **Edition Differences**.

NOTICE

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

Prerequisites

- You have obtained credentials for logging in to the management console.

Yearly/Monthly Mode

Step 1 Log in to the management console.

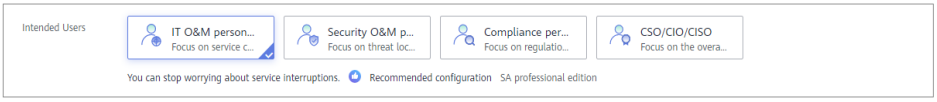
Step 2 Click in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

Step 3 In the upper right corner of the page, click **Upgrade**.

Step 4 (Optional) Select intended users.

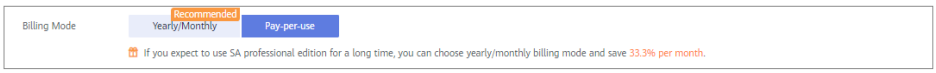
Default user: IT O&M personnel, security O&M personnel, compliance personnel, and CSO/CIO/CISO. Different configurations are recommended for different users.

Figure 2-6 Intended Users



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

Figure 2-7 Yearly/Monthly billing mode



Step 6 Select the SA edition.

The professional edition is selected by default. The professional edition is upgraded from the basic edition.

Figure 2-8 Selecting an edition

Step 7 Configure required parameters. For details, see **Table 1 Parameter description**.

Table 2-3 Parameter description

Parameter	Description
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 is as follows: • 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 host asset quantity.

Step 8 Select the required duration.

Figure 2-9 Selecting the required duration

- Configure the required duration for the asset quotas.

  If you select **Yearly/Monthly**, **Required Duration** must be configured.

  - You can buy the professional edition by month or by year. The duration can be **1**, **2**, **3**, **4**, **5**, **6**, **7**, **8**, **9 months**, **1 year**, **2 years**, or **3 years**.
  - On the basis of the total price, you can enjoy a 17% discount for a one-year subscription, a 30% discount for a two-year subscription, and a 50% discount for a three-year subscription.
- **Auto-renew**: whether to enable automatic renewal. When you enable **Auto-renew**, your subscription will be automatically renewed in a given time before expiration. Be sure that your account balance is abundant for the renewal.

  Table 2-4 Auto-renewal period description

Required Duration	Auto-renewal Period
1, **2**, **3**, **4**, **5**, **6**, **7**, **8**, or **9 months**	1 month
1 year	1 year

NOTE

- You can also configure different required durations for different assets by referring to **Increasing Asset Quotas**.
- For details about how to modify and cancel auto renewal, see **Auto-Renewal Rules**.

Step 9 After the configuration is complete, click **Next**.

Step 10 On the **Details** page, confirm the order information, read the Situation Awareness Disclaimer, select "I have read and agree to the Situation Awareness Disclaimer", and click **Pay Now**.

Step 11 On the payment page, select a payment method and complete the payment.

Step 12 After the payment is complete, return to the Situation Awareness console and verify that the purchase takes effect and the expiration date is correct.

----End

Pay-Per-Use Mode

Step 1 Log in to the management console.

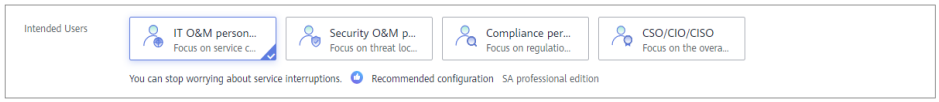
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

Step 3 In the upper right corner of the page, click **Upgrade**.

Step 4 (Optional) Select intended users.

Default user: IT O&M personnel, security O&M personnel, compliance personnel, and CSO/CIO/CISO. Different configurations are recommended for different users.

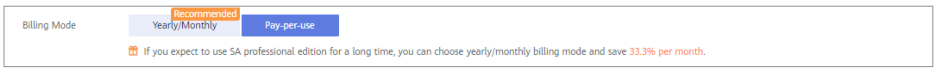
Figure 2-10 Intended Users



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.

Figure 2-11 Pay-per-use billing mode



Step 6 Select the SA edition.

The professional edition is selected by default. The professional edition is upgraded from the basic edition.

Figure 2-12 Selecting an edition

Step 7 Configure required parameters. For details, see **Table 1 Parameter description**.

Table 2-5 Parameter description

Parameter	Description
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 is as follows: • 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 host asset quantity.

Step 8 After the configuration is complete, click **Next**.

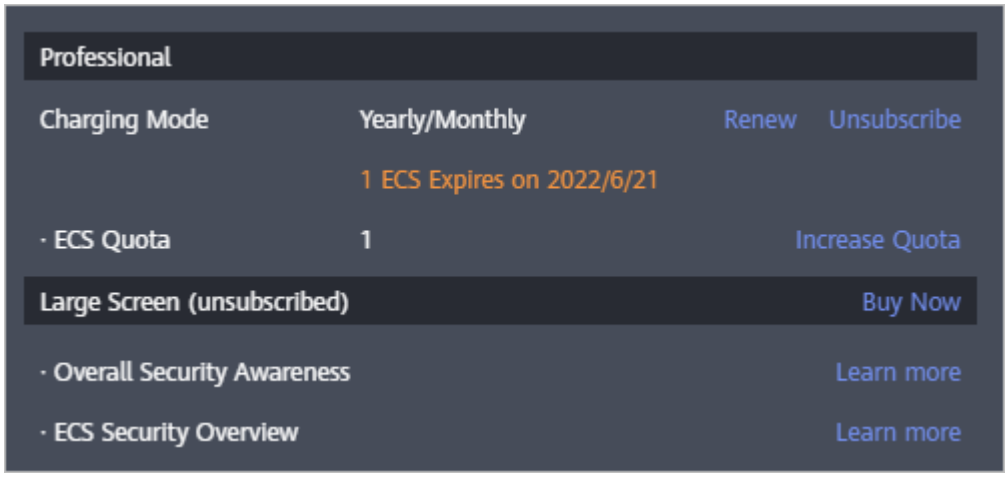
Step 9 On the **Details** page, confirm the order information, read the *Situation Awareness Disclaimer*, select "I have read and agree to the Situation Awareness Disclaimer", and click **Pay Now**.

Step 10 Return to the SA console and verify that the pay-per-use edition is enabled.

----End

Follow-up Procedure

Figure 2-13 Edition management window



- To change the asset quota, click **Increase Quota** and complete the purchase by referring to **Increasing Asset Quotas**.

- To change the SA billing mode from pay-per-use to yearly/monthly, click **Change to Yearly/Monthly** and complete the generated order by referring to **Changing Pay-per-Use to Yearly/Monthly**.
- If the yearly/monthly edition is about to expire or has expired, you can click **Renew** to extend the validity period. For more details, see **Renewal**
- If you no longer need the asset quota, click **Unsubscribe** or **Cancel** to unsubscribe from the corresponding SA service. For details, see **Unsubscribing**.

2.4 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 2-6 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.

Yearly/Monthly 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 **Yearly/Monthly** for **Billing Mode**.

Step 6 Specify **ECS Quota**. Note that you only need to increase quotas for ECSs you expect to add.

Step 7 Set **Required Duration**.

NOTE

- The required duration is set for the increased quota. This required duration does not affect the quota you purchased in the original order.
- The **Price** is calculated based on the increased quota and required duration. The existing quotas will not be charged repeatedly.
- To extend the validity period of the purchased quota in the original order, see **Renewal**.

Step 8 After the configuration is complete, click **Next**.

Step 9 On the **Details** page, confirm the order information, read the *Situation Awareness Disclaimer*, select the check box before "I have read and agree to the Situation Awareness Disclaimer", and click **Pay Now**.

Step 10 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

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

Step 9 After you complete the payment, return to the SA console. You can then start to protect the newly added hosts based on increased quota.

----End

2.5 Renewal

Renewal only extends the validity period of the original edition you have bought. Settings for **ECS Quota** cannot be changed during the renewal.

Only yearly/monthly edition can be renewed.

- Yearly/Monthly is a prepaid billing mode. If your yearly/monthly subscription is about to expire, renew it.
- For pay-per-use SA professional edition, you will be billed for what you use by the hour. When your account balance is abundant, you can use your pay-per-use edition without having to manually renew it.

Manual Renewal

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 **Standard** or **Professional** in the upper right corner. A window for you to manage SA assets will be displayed.

Step 4 Click **Renew** to go to the **Renewals** page.

Step 5 Locate the row containing the desired SA professional edition instance and click **Renew**.

Step 6 Select a renewal duration, for example, one year.

Step 7 Click **Pay** and complete the payment.

Step 8 Return to the **Renewals** page and check the SA subscription status.

----End

Enabling Auto-Renewal

Auto-renewal applies to the services billed on a yearly/monthly basis. When your account balance is abundant and auto-renewal is enabled, the total ECS quota will be automatically renewed.

For more details about auto-renewal, see **Auto-Renewal Rules**.

Step 1 Log in to the management console.

Step 2 Choose **Billing Center** > **Renewal**.

Step 3 In the **Manual Renewals** tab, select the SA professional edition instance and click **Enable Auto-Renew**.

Step 4 Specify the auto-renewal period and set the number of preset auto-renewals.

Step 5 Click **OK**.

Step 6 Return to the **Auto Renewals** tab and verify the auto-renewal status of your SA.

Your SA subscriptions will be automatically renewed based on your configurations.

----End

2.6 Unsubscribing from SA

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

- Yearly/Monthly billing mode: a prepaid mode. You can unsubscribe from a purchased cloud service and apply for a full refund unconditionally within five days of the purchase. Each account can request five-day unconditional full refund for 10 times in a year. Handling fees are required if you unsubscribe from a service over 5 days after it is purchased.
- 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.

For more details about pricing and orders, go to the **Billing Center**.

Unsubscribing from Yearly/Monthly Resources

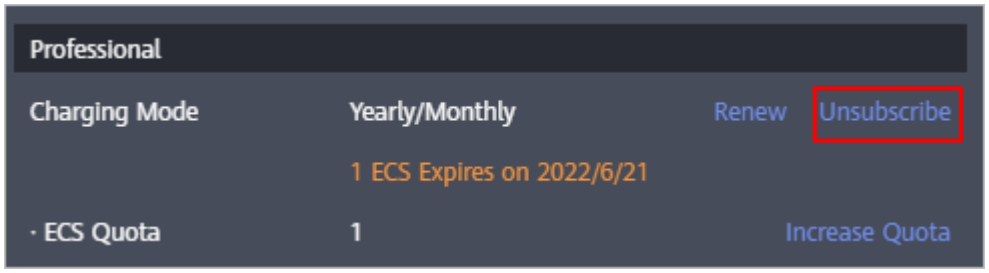
Step 1 Log in to the management console.

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

Step 3 Click **Standard** or **Professional** in the upper right corner. A window for you to manage SA assets will be displayed.

Step 4 In the row of the ECS quota billed on a yearly/monthly basis, click **Unsubscribe**.

Figure 2-14 Unsubscribing from Yearly/Monthly Resources



Step 5 Locate the row that contains the target instance, and click **Unsubscribe** in the **Operation** column.

Step 6 Confirm the information about the resource to be unsubscribed, select the unsubscription reason, and select **I understand a handling fee will be charged for this unsubscription.**

Step 7 Click **Confirm**.

Go to the edition management window and verify that the subscription to the ECS quota that is billed yearly/monthly is canceled.

----End

Canceling Pay-Per-Use SA Resources

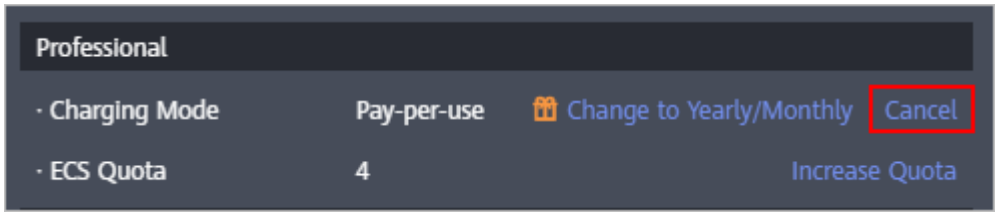
Step 1 Log in to the management console.

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.

Figure 2-15 Canceling pay-per-use 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

2.7 Upgrading SA to SecMaster

SecMaster is a next-generation cloud native platform that enables integrated and automatic security operations. You can manage cloud assets, security posture, security information, and incidents in one place and enjoy intelligent threat detection, easy security orchestration, and automatic response.

SecMaster is an upgraded version of SA. New functions and version iteration will be performed in SecMaster. If you are using SA, SecMaster is recommended for your use in the future.

Precautions

- Only the upgrade from SA to SecMaster is supported. The change from SecMaster to SA is not supported.
- During the upgrade, your SA quota will be allocated to different regions for SecMaster during the upgrade. Before the upgrade, make sure you know how you want SecMaster to take over your SA quota. Note that the SA purchase channel will be unavailable later.
- After the upgrade, SA and SecMaster share the same lifecycle. However, as for you pay-per-use SA subscriptions, you still need to go to the SA console for cancelling or renewing the subscription.
- After the upgrade, change operations cannot be performed in SecMaster. If you need to perform operations such as version upgrade or quota increase, perform the operations in SA.

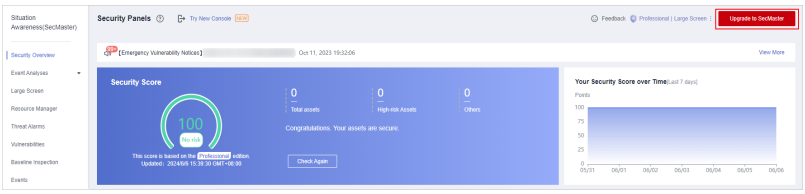
Upgrading SA to SecMaster

Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, click and choose **Security & Compliance** > **Situation Awareness**.

Step 3 In the upper right corner of the page displayed, click **Upgrade to SecMaster**.

Figure 2-16 Upgrade to SecMaster



Step 4 On the **Upgrade to SecMaster** page, configure parameters.

- **Edition Mapping**: The system has automatically synchronized the edition mappings between SA and SecMaster (edition, billing mode, or large screen). No manual configuration is required.
- **Allocate Quota**: Allocate all SA quotas to SecMaster based on your needs.

Step 5 Click **Upgrade Now**.

After the upgrade is complete, you can use SecMaster. Go to SecMaster: Click in the upper left corner of the page and choose **Security & Compliance** > **SecMaster**. For more details, see **SecMaster Introduction**.

----End

3 Security Overview

3.1 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.

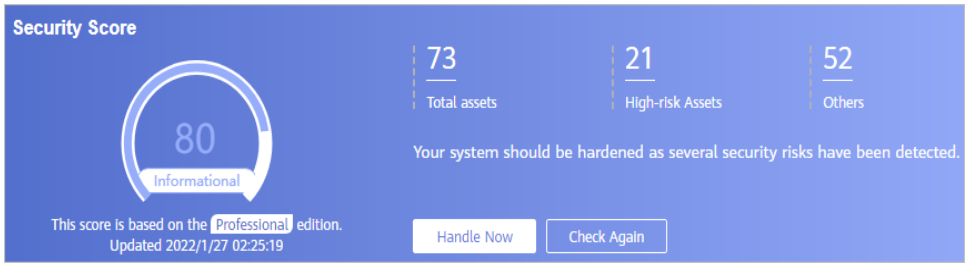
On the **Security Overview** page, you can view the overall security posture of your assets and take actions accordingly. The **Security Overview** page consists of the following parts:

- **Security Score**
- **Security Monitoring**
- **Your Security Score over Time**
- **Threat Detection**

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 3-1** shows an example.

Figure 3-1 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**, **Vulnerabilities**, 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**, **Vulnerabilities**, and **Compliance Check**, which sort risks that have not been handled.

Figure 3-2 Security Monitoring

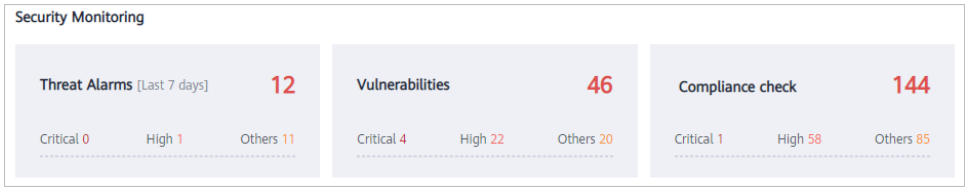
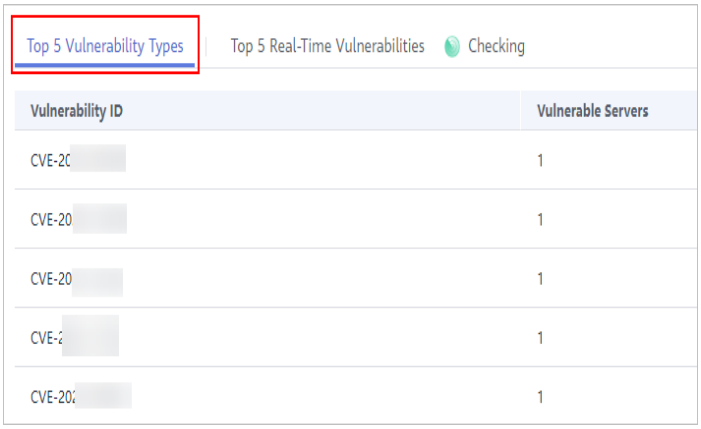
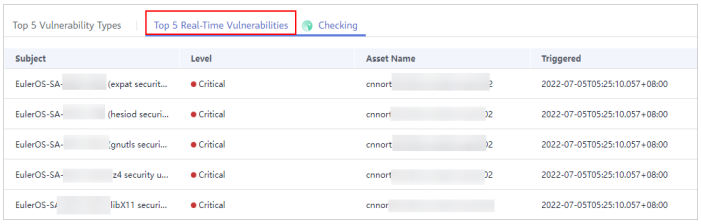
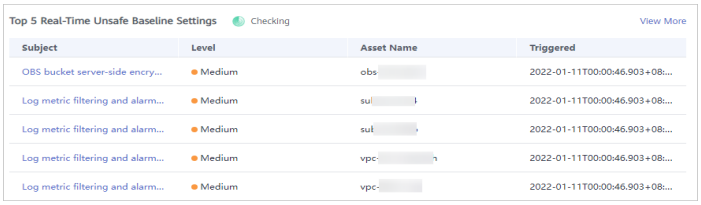


Table 3-1 Security Monitoring parameters

Parameter	Description
Threat Alarms	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. • Risk severity levels: – **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. **Figure 3-3** shows an example. – 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. For details about how to view threat alarms, see **Threat Alarms Overview**. **Figure 3-3** Viewing real-time alarms 

Parameter	Description
Vulnerabilities	This panel displays the top five vulnerability types and the total number of unfixed vulnerabilities in your assets detected in the last 24 hours. You can quickly learn of the total number of unfixed vulnerabilities and the number of vulnerabilities at each severity level. • Risk severity levels: – **Critical**: There are vulnerabilities in your workloads, and you should view vulnerability details and handle the vulnerability in a timely manner. – **High**: There are abnormal events on your workloads, and you should view vulnerability details and handle the vulnerability in a timely manner. – **Others**: There are risky events that are marked as medium-risk, low-risk, and informational alarms detected in your systems. You can view vulnerability details to learn what actions need to be taken. • When you click the **Top 5 Vulnerability Types** tab, the system displays the top 5 vulnerability types. – Vulnerability rankings are based on the number of hosts a vulnerability affects. The vulnerability that affects the most hosts ranked the first. – The data is only displayed in **Top 5 Vulnerability Types** if the hosts have Host Security Service (HSS) Agent version 2.0 installed. If no data is displayed or you want to view the top 5 vulnerability types, upgrade Agent from 1.0 to 2.0. **Figure 3-4** Top 5 Vulnerability Types  • Click **Top 5 Real-Time Vulnerabilities** tab. The system displays the top 5 vulnerability events detected in the last 24 hours. You can quickly view vulnerability details. **Figure 3-5** shows an example. – You can view details such as the vulnerability name, severity, asset name, and discovery time.

Parameter	Description
	– If there is no data available, no vulnerabilities were detected on the current day. – You can click **View More** to go to the **Events** tab and view more vulnerabilities. You can apply custom search filters to query vulnerability information. **Figure 3-5** Viewing real-time vulnerabilities 

Parameter	Description
Compliance Check	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. • Risk severity levels: – **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. **Figure 3-6** shows an example. – 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. For details, see **Cloud Service Baseline Overview**. **Figure 3-6** Viewing compliance risks 

Your Security Score over Time

SA displays your security scores for the last 7 days.

Figure 3-7 Your Security Score over Time

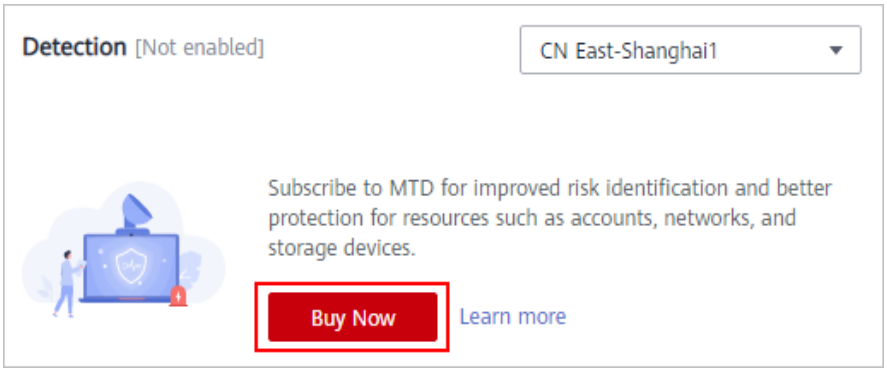
Threat Detection

The **Threat Detection** area displays the number and types of alarms detected on your assets in the last seven days.

Managed Threat Detection (MTD) continuously scans for malicious activities and unauthorized behavior to protect your accounts and workloads. It integrates detection models, such as an AI detection engine, threat intelligence, and detection policies, to identify threats and generate detection reports. By analyzing the detection results, MTD improves the accuracy of alarm notifications and threat detection, and simplifies O&M.

If you want to use MTD to monitor access behavior and potential threats using access logs, to generate alarms, and output alarm results, subscribe to MTD. If MTD is not enabled, click **Buy Now**.

Figure 3-8 Enabling MTD



3.2 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 3-2 Security score table

Severity	Security Score	Description
Secure	100	Congratulations. Your assets are secure.
Informational	80 ≤ Security Score < 100	Your system should be hardened as several risks have been detected.
Low	60 ≤ Security Score < 80	Your system should be hardened in a timely manner as numerous risks have been detected.
Medium	40 ≤ Security Score < 60	Your system should be hardened ASAP. Your assets are vulnerable to attacks.
High	20 ≤ Security Score < 40	Detected risks should be handled ASAP. Your assets are vulnerable to attacks.
Critical	0≤ Security Score <20	Detected risks should be handled immediately. Your assets are likely to be attacked.

Unscored Check Items

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

Table 3-3 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		
Vulnerabilities	Critical vulnerabilities not fixed	10	Fix vulnerabilities by referring to corresponding suggestions and start a new scan. The security score will be updated.	20
	High-risk vulnerabilities not fixed	5		
	Medium-risk vulnerabilities not fixed	2		
	Low-risk vulnerabilities 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		

4 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, region, and security status. This helps you quickly locate security risks and find solutions.

You can view the security status of the following resources:

Elastic Cloud Server (ECS), Virtual Private Cloud (VPC), Object Storage Service (OBS), Elastic IP (EIP), Domain Name Service (DNS), Elastic Load Balance (ELB), Relational Database Service (RDS), Bare Metal Server (BMS), Cloud Container Engine (CCE), Cloud Container Instance (CCI), Web Application Firewall (WAF), SSL Certificate Manager (SCM), and Elastic Volume Service (EVS)

Prerequisites

- You have purchased the SA standard or professional edition.
- 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 **How Do I Configure Permissions for Resource Manager?**

Procedure

Step 1 Log in to the management console.

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

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

Step 4 View the security status of all resources. **Table 4-1** describes related parameters.

Figure 4-1 Resource Manager

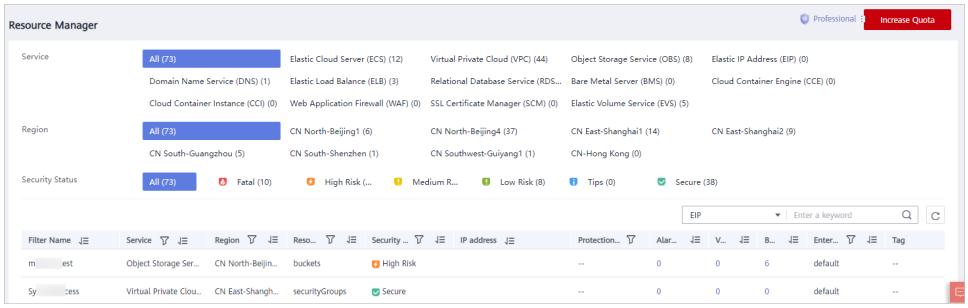


Table 4-1 Parameters for resource security status

Parameter	Description
Resource Name	Resource name.
Service	Service the resource belongs to.
Region	Region where the resource locates
Resource Type	Type of the resource. For example, cloud servers, disks, and instances.
Security Status	Risk severity of the resource. • 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	The total number of threat alarms for the resource in the last 7 days. 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.

Parameter	Description
Vulnerabilities	The total number of vulnerabilities that have not been fixed within the last 24 hours. • 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.
Baseline	The total number of baseline risks for a resource in the last 30 days. • 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	Tags added to the resource. If a tag is added to a resource on the current day, the tag will be displayed in this column the next day.

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

5 Event Analyses

SA works with other cloud security services to centrally display the security status and risks of your cloud assets in real time.

Overview

- HSS analysis

  Host Security Service (HSS) helps you identify and manage the assets on your servers; manage programs, file integrity, security operations, and vulnerabilities; check for unsafe settings; and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

  On the HSS page of SA, you can learn about the security status of your ECSs in real time, including the protection status, risk statistics for the last 24 hours, risks for the last 7 or 30 days, and intrusion statistics of protected ECSs.

- WAF analysis

  Web Application Firewall (WAF) keeps your web applications and websites secure and stable. Powered by machine learning, WAF intelligently examines website traffic and defends against malicious requests and unknown threats.

  On the WAF page of SA, you can view the protection logs of all protected websites or instances for a specified time range, including yesterday, today, past 3 days, past 7 days, or past 30 days. On this page, event logs are displayed by different dimensions, including the number of requests and attack types, QPS, response code, event distribution, top 10 attacked domain names, top 10 attack source IP addresses, top 10 attacked URLs, top 10 attack source locations, and top 10 error pages.

  Statistics on this page are updated every two minutes.

- DBSS analysis

  Database Security Service (DBSS) is an intelligent database security service powered by the machine learning and big data analytics technologies. It can audit your databases, detect SQL injection attacks, and identify high-risk operations.

  On the DBSS page of SA, you can view the overall audit status, risk distribution, session statistics, and SQL distribution of your databases for the last 30 minutes, last hour, last 24 hours, last 7 days, or last 30 days.

Prerequisites

You have enabled linked services in the required region. For example, if you want to view the analyses of ECSs in the **CN-Hong Kong** region, then enable HSS in this region.

Procedure

Step 1 Log in to the management console.

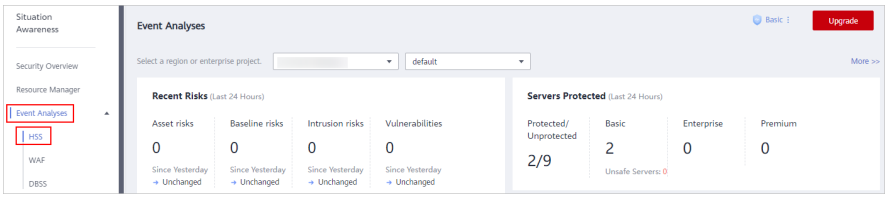
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

Step 3 Select a security service.

- HSS

  In the navigation pane on the left, choose **Event Analyses** > **HSS** to go to the HSS analysis page.

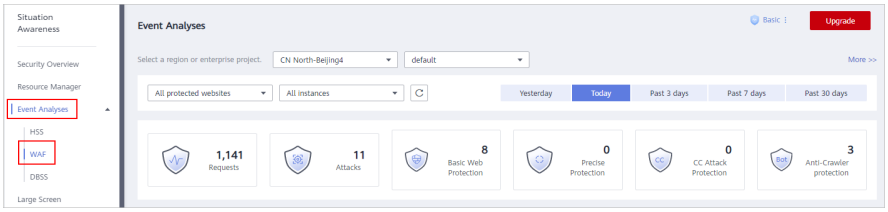
  Figure 5-1 HSS analysis

- WAF

  In the navigation pane on the left, choose **Event Analyses** > **WAF** to go to the WAF analysis page.

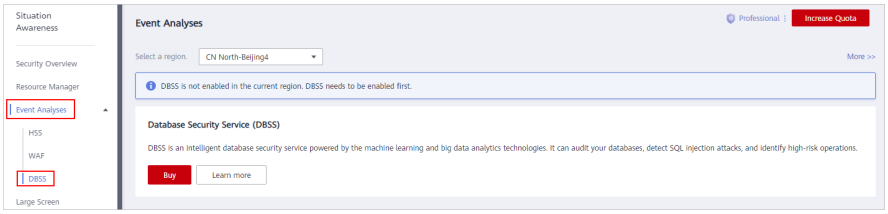
  Figure 5-2 WAF analysis

- DBSS

  In the navigation pane on the left, choose **Event Analyses** > **DBSS** to go to the DBSS analysis page.

  Figure 5-3 DBSS analysis

Step 4 View the analysis results.

- HSS dashboard

  On the HSS page in SA, you can learn about the security status of your ECSs in real time, including the protection status, risk statistics for the last 24 hours, risks for the last 7 or 30 days, and intrusion statistics of protected ECSs.

  For details, see **HSS Analysis**.

- WAF dashboard

  On the WAF page in SA, you can view the protection logs of all protected websites or instances for a specified time range, including yesterday, today, the past 3 days, past 7 days, or past 30 days. On this page, different aspects of event logs are displayed. You can view the number of requests and attack types, QPS, response code, event distribution, top 10 attacked domain names, top 10 attack source IP addresses, top 10 attacked URLs, top 10 attack source locations, and top 10 error pages.

  For details, see **WAF Analysis**.

- DBSS dashboard

  On the DBSS page in SA, you can view the overall audit status, risk distribution, session statistics, and SQL distribution of your databases for the last 30 minutes, last hour, last 24 hours, last 7 days, or last 30 days.

  For details, see **DBSS Analysis**.

----End

6 Threat Alarms

6.1 Threat Alarms Overview

Overview

SA can aggregate alarms reported by other Huawei Cloud 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, Anti-DDoS, 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 Notifications**

  Allows you to customize threat alarm notifications. You can set scheduled daily alarm notifications and real-time alarm notifications to learn about threat risks in a timely manner.
- **Alarm Monitoring**

  Allows you to customize the threat list, alarm type, and risk severity to view only the threat alarms you are concerned with.

Alarm Types

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

NOTE

The basic edition can detect only some threats and attacks. To better protect your assets on the cloud, we recommend the professional edition.

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

6.2 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 standard and professional editions.
- 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.

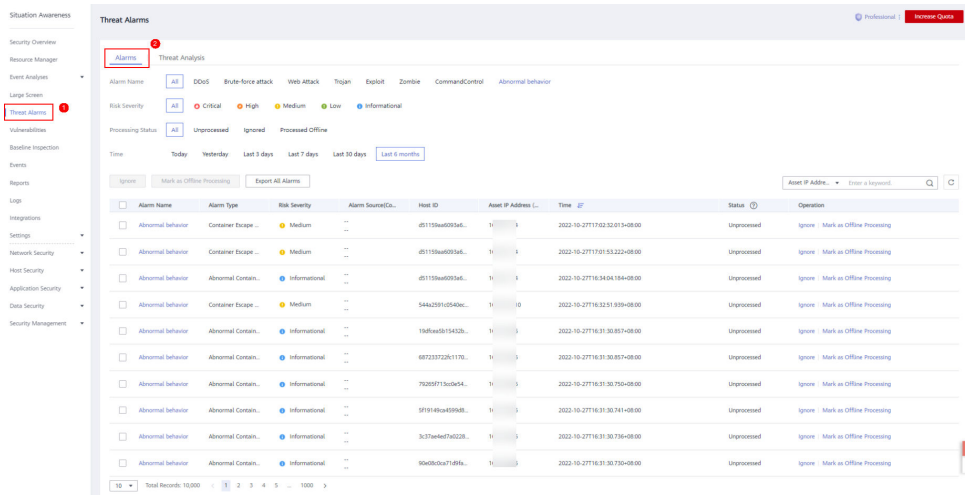
Viewing Alarm Details

Step 1 Log in to the management console.

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

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

Figure 6-1 Viewing 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.

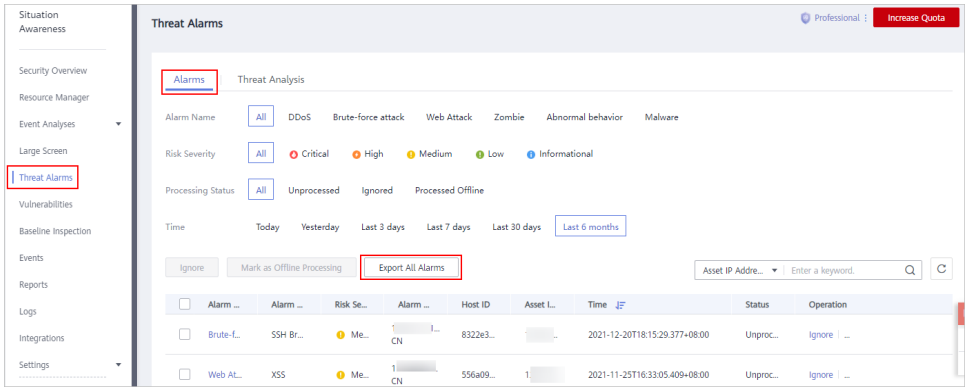
To change the processing status of an alarm, locate the target row and click **Unignore** or **Unmark** in the **Operation** column to restore the alarm to the **Unhandled** status and then re-mark the alarm processing status.

----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.

Figure 6-2 Exporting alarm events



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.

6.3 Viewing Threat Analysis

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

Prerequisites

The standard or professional edition 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 & Compliance** > **Situation Awareness**.

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

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

6.4 Handling Alarms and Events

6.4.1 DDoS

Overview

In a DDoS attack, an attacker uses compromised computers on the Internet to launch DoS attacks on the target. DoS attacks, also called flood attacks, are intended to exhaust the network or system resources on the target computer, causing services to be interrupted or suspended, so legitimate users are unable to access network services.

The basic, standard, and professional editions can detect more than 100 types of DDoS attacks.

Suggestion

If SA detects that an application system is experiencing a DDoS attack, SA will report an **Informational** alarm. You are advised to purchase an **AAD** instance for better protection.

6.4.2 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.

As long as **Host Security Service (HSS)** is enabled, the professional edition SA can detect 22 types of brute-force attacks. If HSS is not enabled, the professional edition can detect 14, and the standard edition can detect 8. The basic edition does not support this feature.

Suggestion

If a brute force attack threat is detected, handle the threat by following the instructions in **Table 6-1**.

Table 6-1 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.	The SSH port is open to the public network. You are advised to perform the following operations: 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.	The RDP port is open to the public network. You are advised to perform the following operations: 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.

Threat Alarm	Severity	Threat Description	Suggestion
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).	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: 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.
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: 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: 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.

Threat Alarm	Severity	Threat Description	Suggestion
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.

6.4.3 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.

As long as **Web Application Firewall (WAF)** to detect 14 of them and **Host Security Service (HSS)** are both enabled, SA professional edition can detect 38 types of web attacks. HSS is required for 3 of them, and WAF is required for 14 of them. The standard edition can detect 19 types of web attacks, and the basic edition does not support web attack detection.

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.

6.4.4 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.

SA can detect 5 types of Trojans. The professional edition can detect them all. The standard edition can detect one type of Trojan. The standard edition cannot detect Trojans.

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.

6.4.5 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.

SA can detect two types of exploits. The professional edition can detect them all. The basic and standard editions do not support exploit detection.

Suggestion

If an exploit is detected, handle the threat by following the instructions in **Table 6-2**.

Table 6-2 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: 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: 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.

6.4.6 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.

SA can detect seven types of zombie threats. The professional edition can detect all types of zombie threats. The standard edition can detect five of them. The basic edition does not support zombie detection.

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.

6.4.7 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.

SA can detect three types of C&C attack threats. The professional edition can detect them all. The basic and standard editions do not support C&C attack detection.

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.

6.4.8 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 unexpected, 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).

SA can detect 21 types of abnormal behavior threats. The professional edition can detect them all. Note that you need to buy **Web Application Firewall (WAF)** to

detect 7 types of them and buy **Host Security Service (HSS)** to detect 11 types of them. The basic edition does not support abnormal behavior detection.

Suggestion

If an abnormal behavior threat is detected, handle the threat by following the instructions in **Table 6-3**.

Table 6-3 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.

7 Baseline Inspection

7.1 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.

SA can check key cloud service configurations for your workloads on the cloud based on security standards **Cloud Security Compliance Check 1.0** and **Network Security**.

Limitations and Constraints

- The SA basic edition does not support baseline inspection. The basic edition does not support viewing of cloud service baseline details. 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**.
- The baseline inspection is a regional function. You can go to the SA console to see which regions support the function.

7.2 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**.

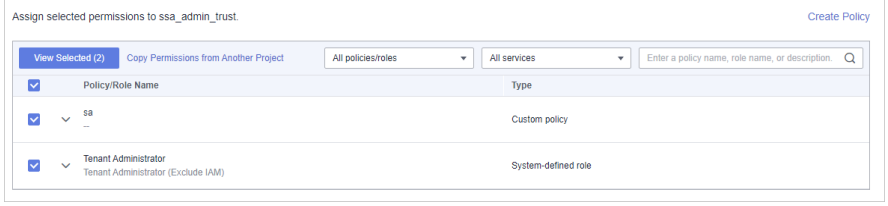
Step 4 In the navigation pane one the left, choose **Agencies**.

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 7-1 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

7.3 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

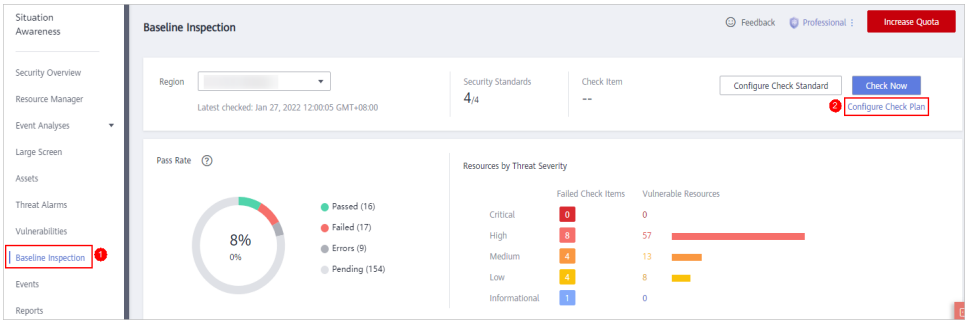
Step 1 Log in to the management console.

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

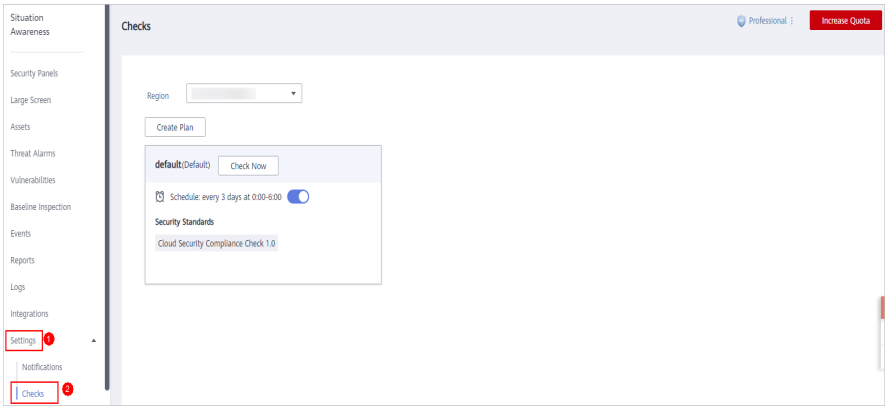
  Figure 7-2 Accessing the page for configuring check plans



- Method 2

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

Figure 7-3 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 7-1**.

   Table 7-1 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. – 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 & Compliance** > **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**.

7.4 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

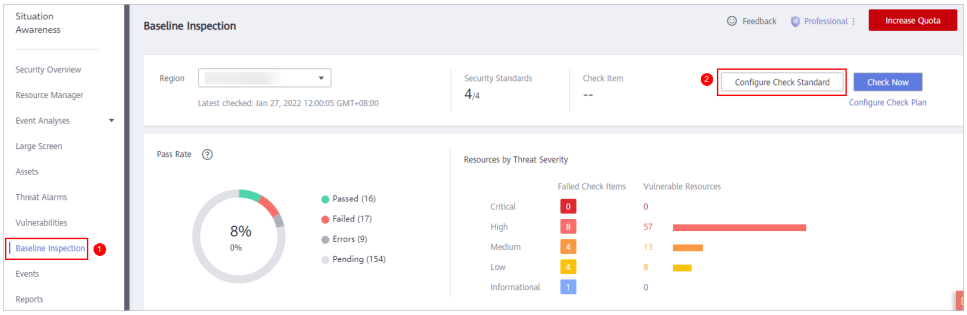
SA will immediately execute check plan you configured.

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **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 7-4 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.

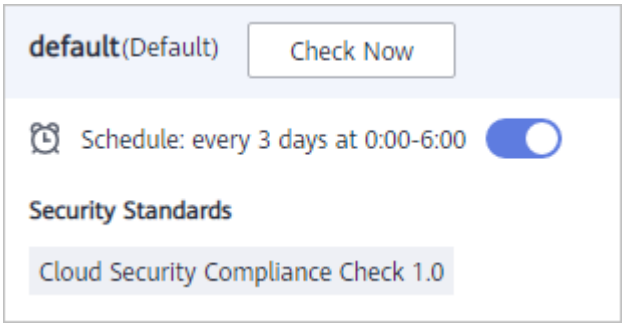
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

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 7-5 Executing a specific check plan



SA immediately executes the selected baseline check plan.

----End

7.5 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.

For all check items in **DJCP 2.0 Level 3 Requirements** and some check items in **Cloud Security Compliance Check 1.0** and **Network Security**, they must be manually checked first. Then, you need to report the check results to SA so that they can be counted when the pass rate is calculated.

Prerequisites

- Your professional edition SA is available.
- 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 & Compliance** > **Situation Awareness**.

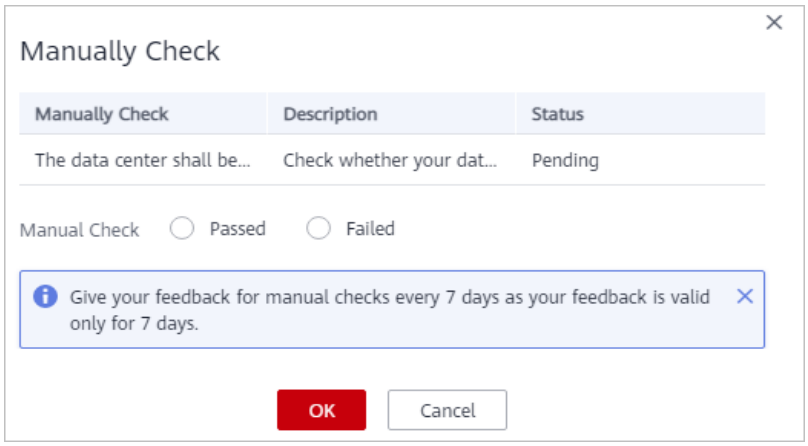
Step 3 In the navigation pane on the left, choose **Baseline Inspection**.

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 7-6 Manually Check



NOTE

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

----End

7.6 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

- Your professional edition SA is available.
- 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.

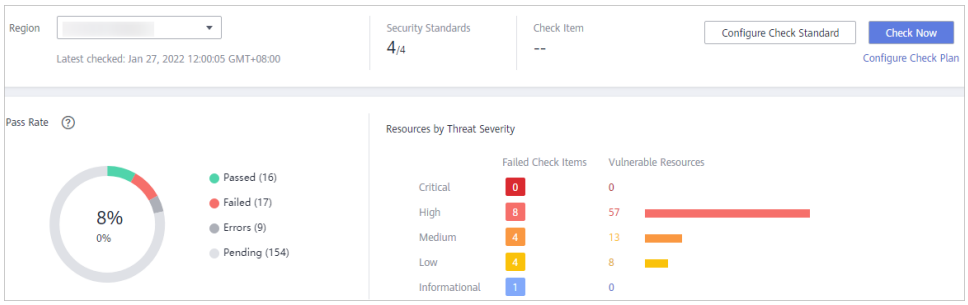
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

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 7-7 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 & Compliance** > **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

NOTE

The SA basic and standard editions do not support viewing of cloud service baseline details. With the **professional edition**, you can view details about **Vulnerable Resources** and **Fix Method**.

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 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.

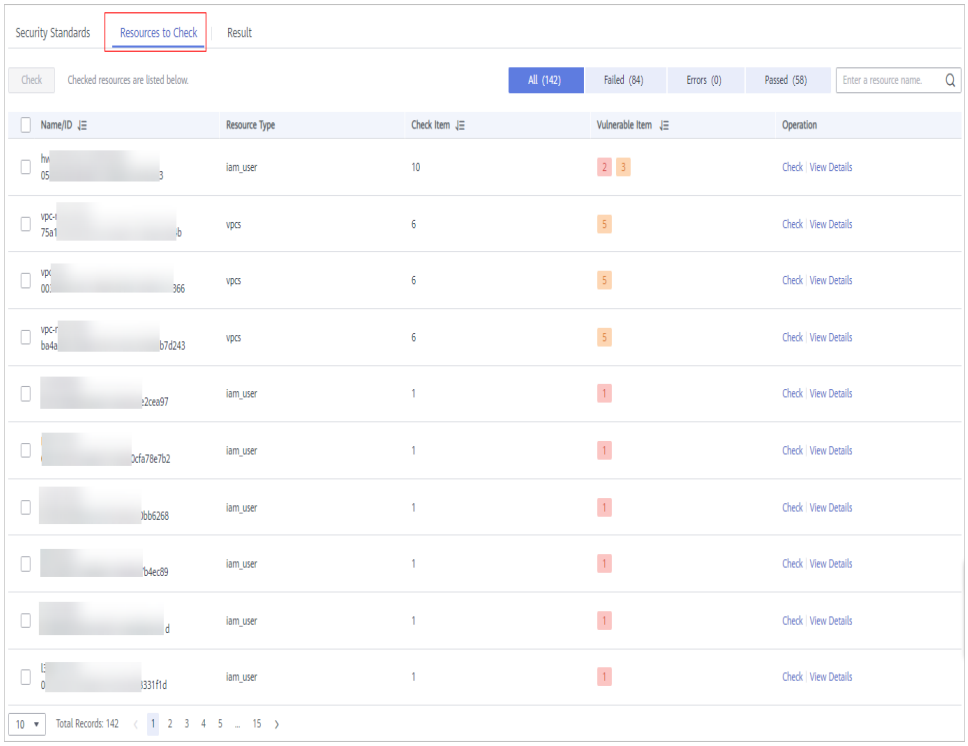
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

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 7-8** shows an example.

Figure 7-8 All resources to check



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

NOTE

The SA basic and standard editions do not support viewing of cloud service baseline inspection details. With the **professional SA**, you can view details about **Vulnerable Resources** and **Fix Method**.

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

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

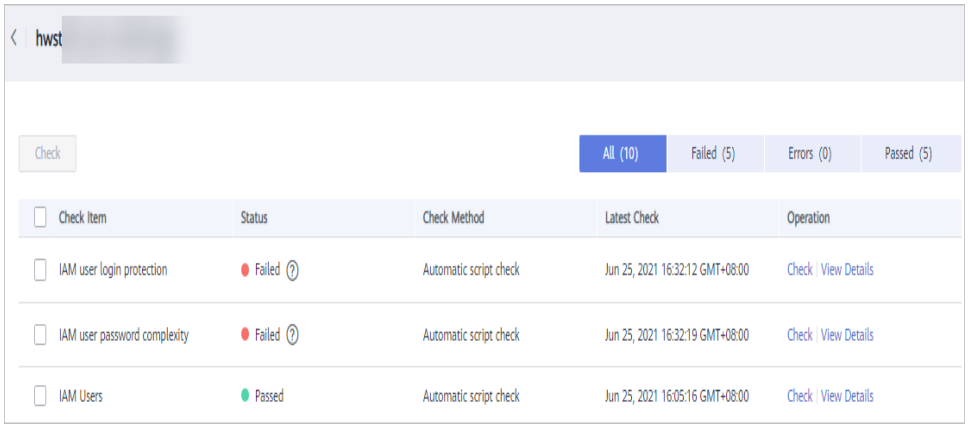
Step 5 In the checked resource list, locate the resource you want and click **View Details** in the **Operation** column.

Figure 7-9 Resources to Check

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

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

Figure 7-10 Details page of a check resource



----End

Viewing Check Results

NOTE

The SA basic and standard edition do not support viewing of cloud service baseline inspection results. To learn about the cloud service configuration status and ensure that cloud service configuration is appropriate, the professional edition is recommended. For details, see **Purchasing the Professional Edition**.

Step 1 Log in to the management console.

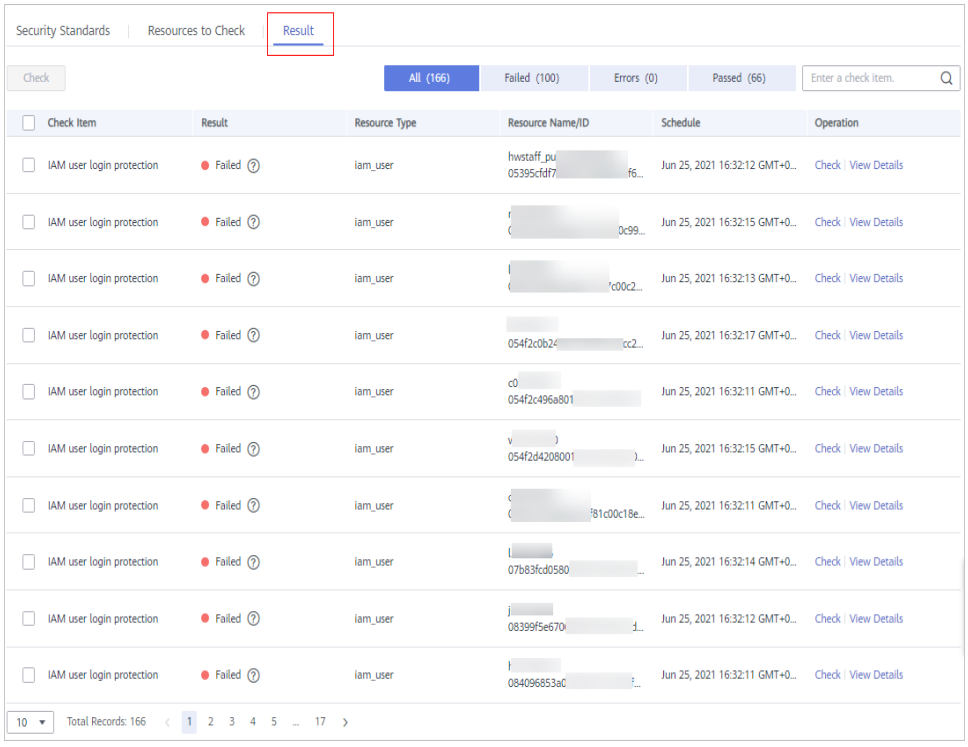
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

Step 3 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 7-11** shows an example.

Figure 7-11 All check results



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

7.7 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

- Your professional edition SA is available.
- The cloud service baseline has been scanned.

Handling Unsafe Settings

The following describes how to fix unsafe settings discovered by check item **IAM user login protection**.

Step 1 Log in to the management console.

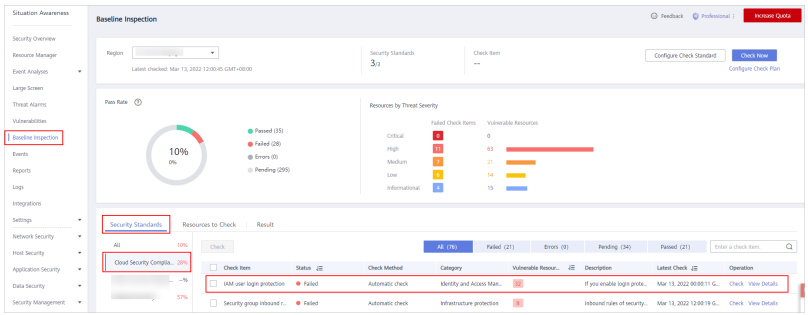
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Situation Awareness**.

Step 3 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, choose **Cloud Security Compliance Standard 1.0**, and view the risk status of check items.

Figure 7-12 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 row containing the **IAM user login protection** check, click **View Details** in the **Operation** column.

Step 7 View the risk details and fix the unsafe settings by referring to **Result** and **Reference**.

Table 7-2 Check item description

Parameter	Description
Status	Displays the check status of the current check item. • 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.
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**. • 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 & Compliance** > **Situation Awareness**.

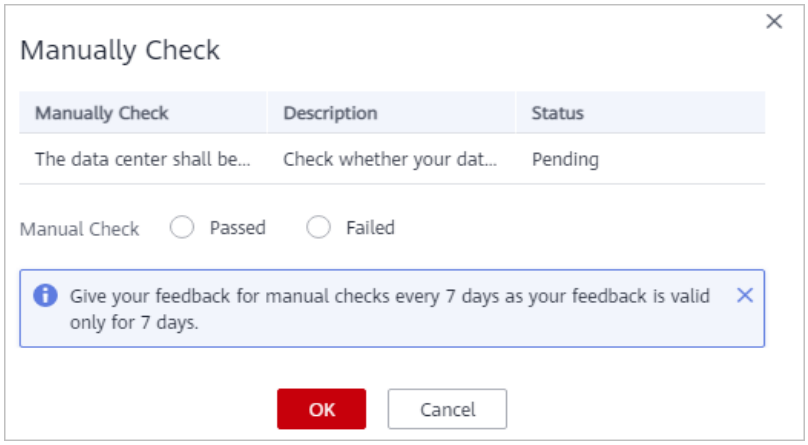
Step 3 In the navigation pane on the left, choose **Baseline Inspection**.

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 7-13 Manually Check



NOTE

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

----End

Ignoring a Check Item

If you have custom requirements for a check item, ignore the check item. For example, SA checks whether the session timeout duration is set to 15 minutes, while you need to set it to 20 minutes. In this situation, ignore this check item so that SA no longer executes this check.

An ignored check item will be no longer executed. It will not be counted when the **Pass Rate** is calculated.

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

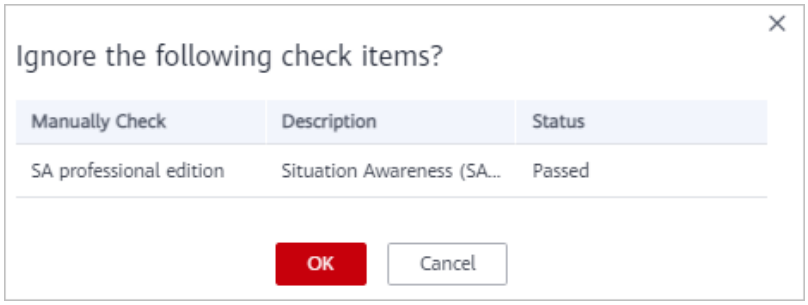
Step 4 Select the region where the check result to be viewed is located.

Step 5 On the **Security Standards** tab, locate the row containing the check item you want to ignore, click **Ignore** in the **Operation** column.

To ignore more than one check item at a time, select all the check items you want to ignore, and click **Ignore** in the upper left corner of the check item list.

Step 6 In the displayed dialog box, click **OK**.

Figure 7-14 Ignore the following check items?



NOTE

- Ignored check items will be not executed. They will not be counted when the **Pass Rate** is calculated.
- To resume an ignored check item, locate the row containing the ignored check item, and click **Unignore** in the **Operation** column. Then, in the displayed dialog box, click **OK**.

----End

8 Events

8.1 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.

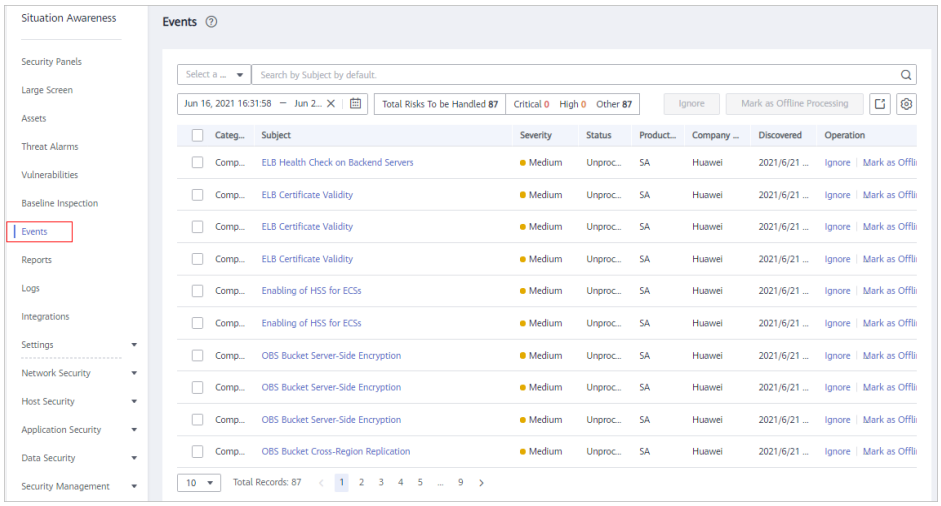
Procedure

Step 1 Log in to the management console.

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

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

Figure 8-1 Viewing the event list



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**.

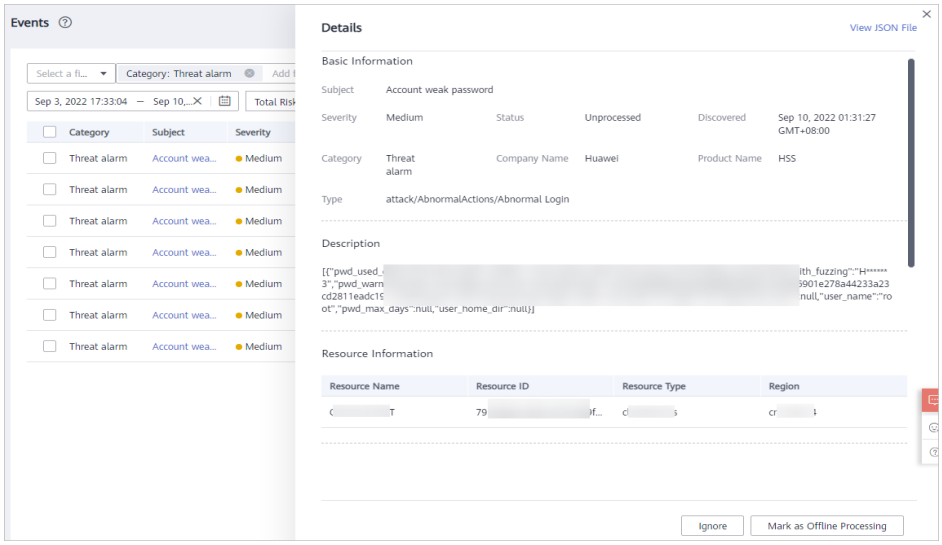
Step 5 View the event list.

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 8-2 Details



2. On this pane, the **Basic Information**, **Description**, **Resource Information**, **Attack Information**, and **Tenant Information** are listed. For more details, see **Table 8-1**.

Table 8-1 Parameters on the event details page

Parameter	Description
Basic Information	Basic information about an event, including the subject, severity, status, discovery time, category, company name, product name, and type.
Description	Brief description of an event.
Resource Information	Information about affected resources, including the resource name, resource ID, resource type, and the region where the affected resource locates.
Tenant Information	Information about affected users, including the tenant ID, project name, project ID, and region where the user account is registered.
Attack Source Information	Attack source information, including the IP address, port, and longitude from where an attack originates.
Attacked Resource Details	Information about the attacked resource, including the attacked IP address and port.
Check Results	Information about the associated detection results, including the associated resource name and result source.

Parameter	Description
Vulnerability Information	Vulnerability result information, including the vulnerability ID, CVSS score, CVSS version, and provider.
Affected Products	Vulnerability impact scope information, including affected resource versions and security product versions.
Compliance Information	Basic information about compliance check, including check items and check results.
Involved CVE	CVE ID of the vulnerability.
References:	Related reference links.
Repair/ Handling Suggestion	Details of risk repair or handling suggestions.

3. On the **Details** pane, Click **View JSON File** in the upper right corner to view the event details in a JSON file.

----End

8.2 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.

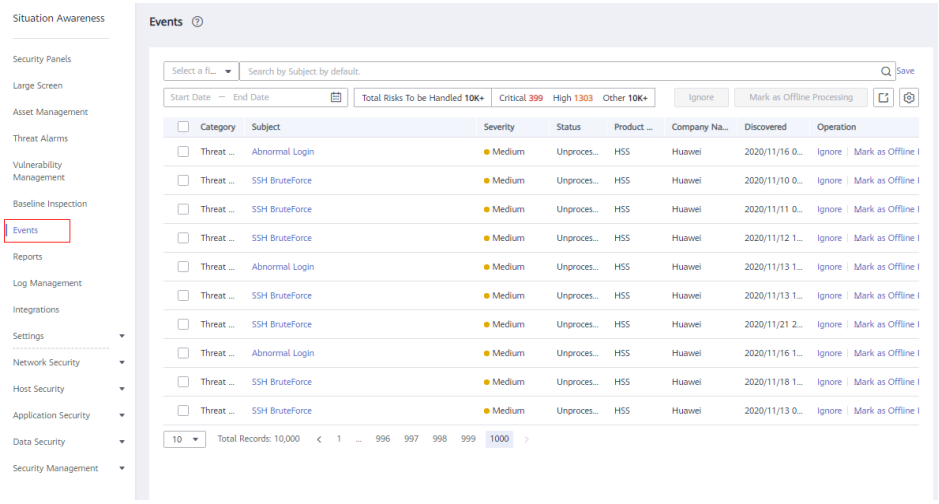
Procedure

Step 1 Log in to the management console.

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

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

Figure 8-3 Processing events



Step 4 Filter events.

Step 5 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 6 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

8.3 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.

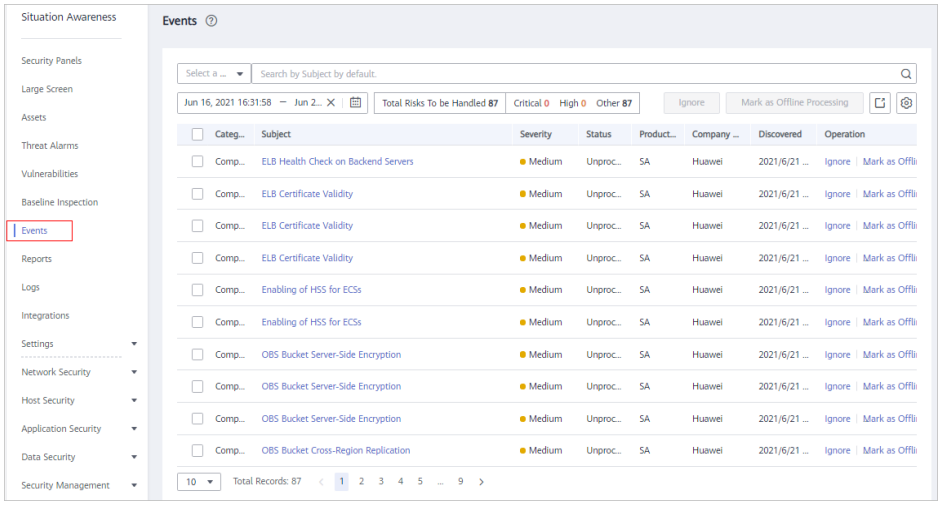
Procedure

Step 1 Log in to the management console.

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

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

Figure 8-4 Exporting events



Step 4 Filter events.

Step 5 Click ⬈ to export the filtered events to a .csv file and save it locally.

You can then view them offline.

----End

8.4 Customizing the Event List

You can customize the event list.

Prerequisites

- SA has received the events from other security products.

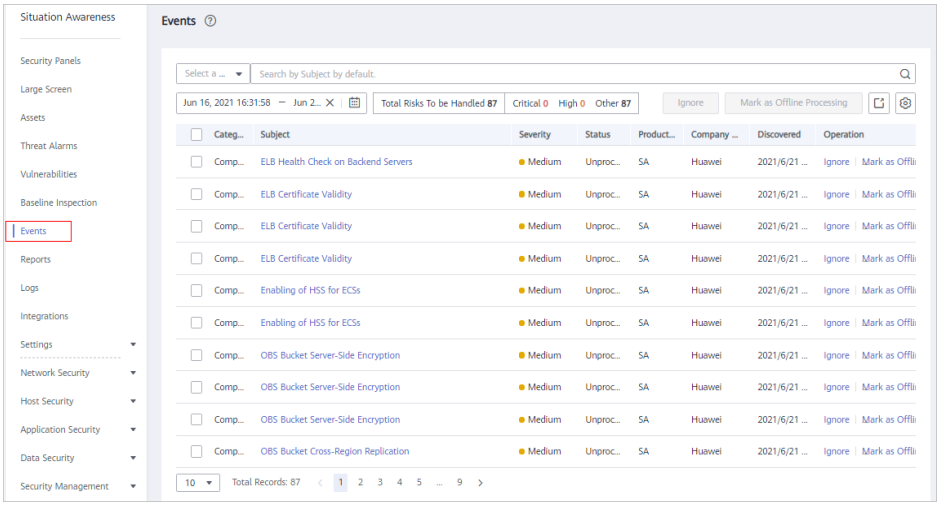
Procedure

Step 1 Log in to the management console.

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

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

Figure 8-5 Customizing the event list



Step 4 Click ⚙ to expand all column options of the event list.

Step 5 Select the columns you want to display.

Step 6 Refresh the event list.

----End

8.5 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**

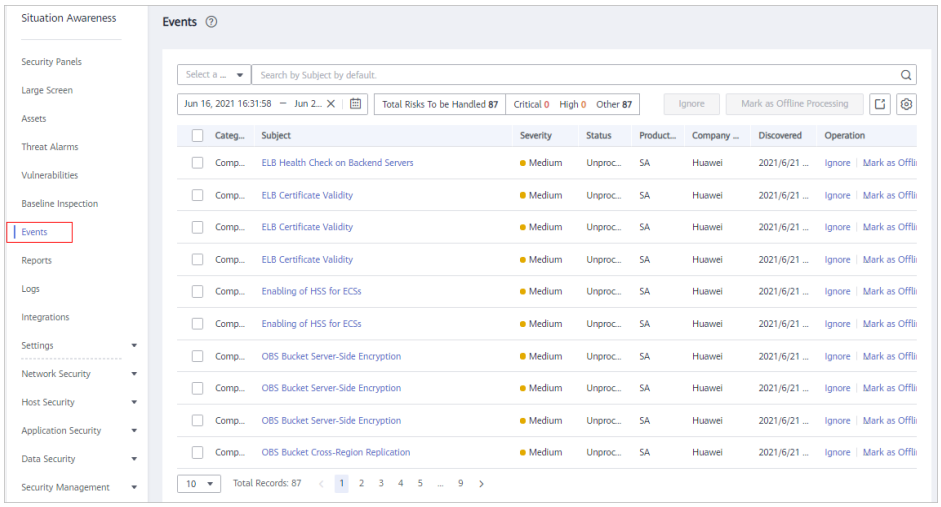
Creating a Filter

Step 1 Log in to the management console.

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

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

Figure 8-6 Events



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 & Compliance** > **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 & Compliance** > **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

9 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.

For SA log disaster recovery, you can use Data Ingestion Service (DIS) to transmit the logs dumped to OBS buckets to your offline security information and event management (SIEM) system. You can also upload logs in the offline SIEM system to the cloud through DIS for analysis and storage.

NOTE

- With DIS, you can use a wide range of data transmission tools, such as Kafka Adapter, DIS Agent, DIS Flume Plugin, DIS Flink Connector, DIS Spark Streaming, and DIS Logstash Plugin. For details, see **Using DIS**.
- Uploading logs to an OBS bucket may be unavailable in some regions.
- OBS is billed separately. You can learn more pricing details in the OBS service.

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, see **How Do I Assign Operation Permissions to an Account?**

Creating an OBS Bucket for Storing Logs

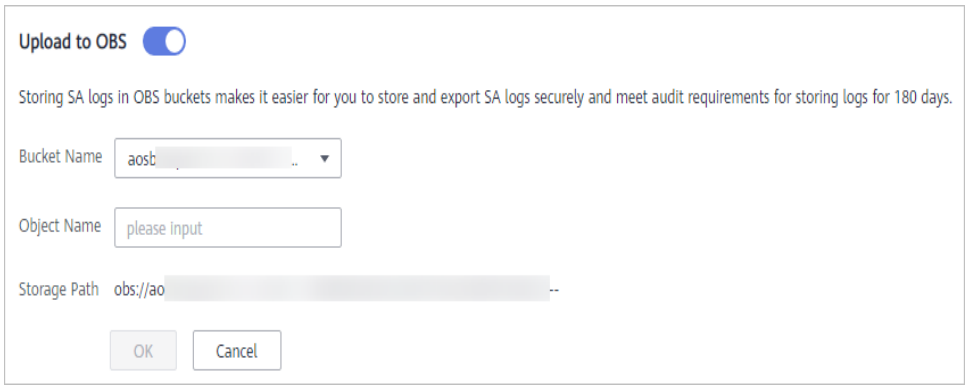
To meet the security audit requirements for storing logs for at least 180 days, you can transfer logs to an OBS bucket for long-term storage. You can also download transferred logs on the OBS console.

Step 1 Log in to the management console.

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

Step 3 In the **Upload to OBS** area, click  to enable OBS. **Figure 9-1** shows an example.

Figure 9-1 Upload to OBS



Step 4 Configure related parameters. **Table 9-1** describes the parameters.

Table 9-1 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** • 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**.

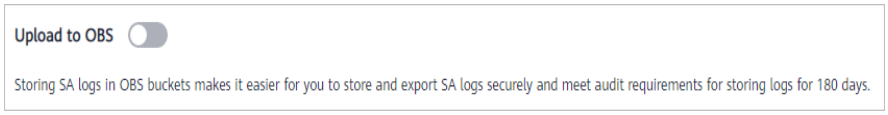
It takes about 10 minutes for the service to upload logs to the bucket.

----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.

Figure 9-2 Disabling uploading logs to an OBS bucket



10 Integrations

10.1 Managing Integrations

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

By default, SA integrates the events from the following cloud services:

- Anti-DDoS
- Web Application Firewall (WAF)

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.

Constraints

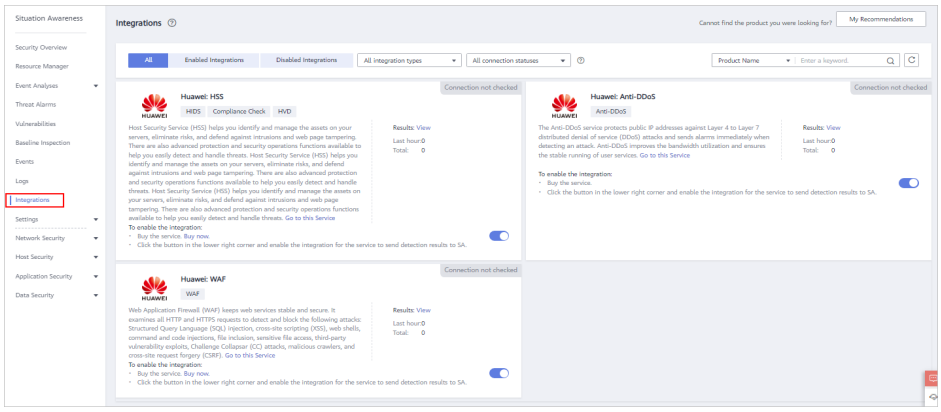
- An integration can only be enabled or disabled by region.
- The account you want to use to enable integrations must have the **Tenant Administrator** role assigned.

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 & Compliance** > **Situation Awareness** > **Integrations**.

Figure 10-1 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.

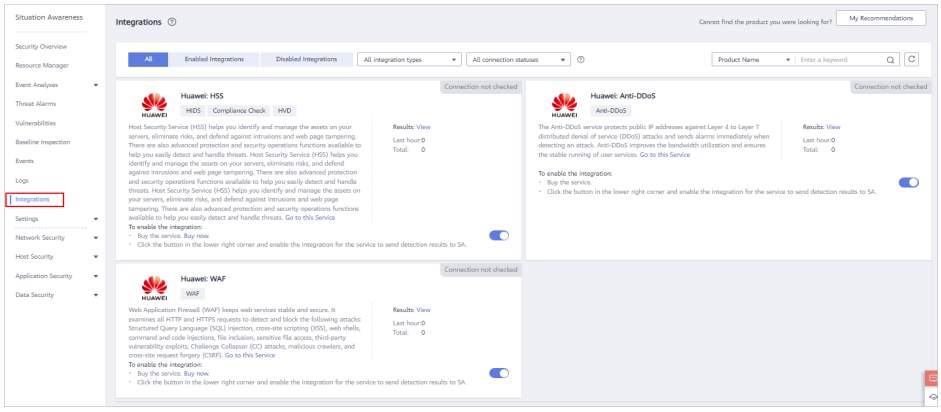
----End

Disabling an Integration

Step 1 Log in to the management console.

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

Figure 10-2 Integrations



Step 3 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 4 Stop to receive results.

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

----End

10.2 Viewing Integrations

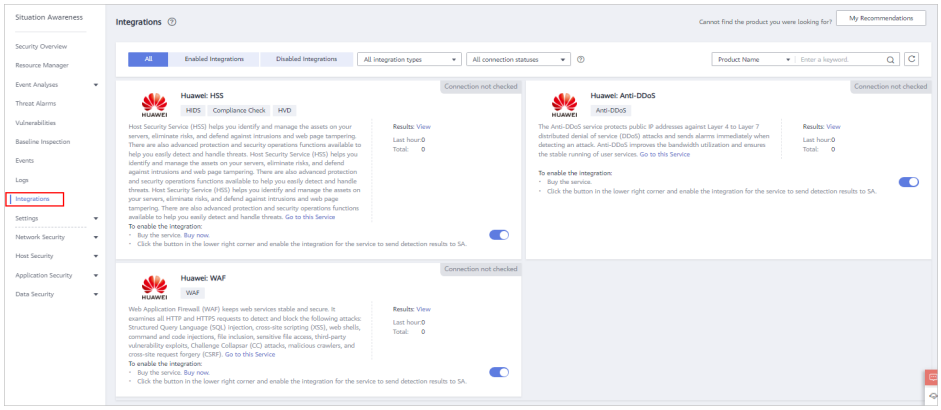
You can manage all integrations and view the number of statistics results received from other products.

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 & Compliance** > **Situation Awareness** > **Integrations**.

Figure 10-3 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.

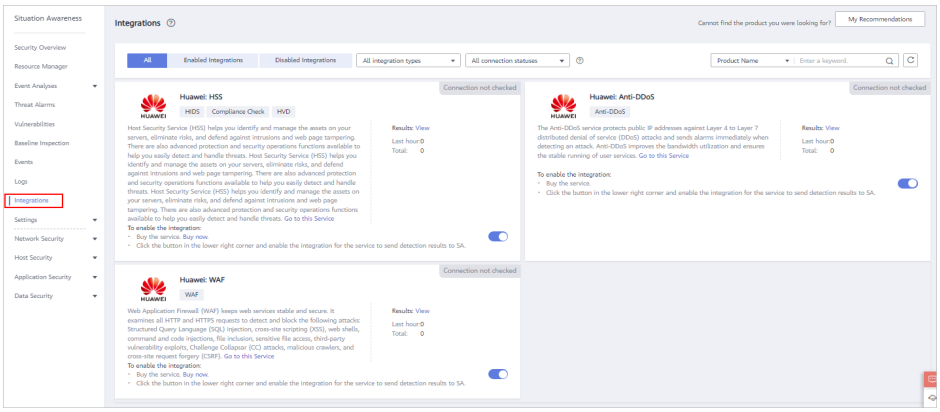
----End

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 & Compliance** > **Situation Awareness** > **Integrations**.

Figure 10-4 Integrations



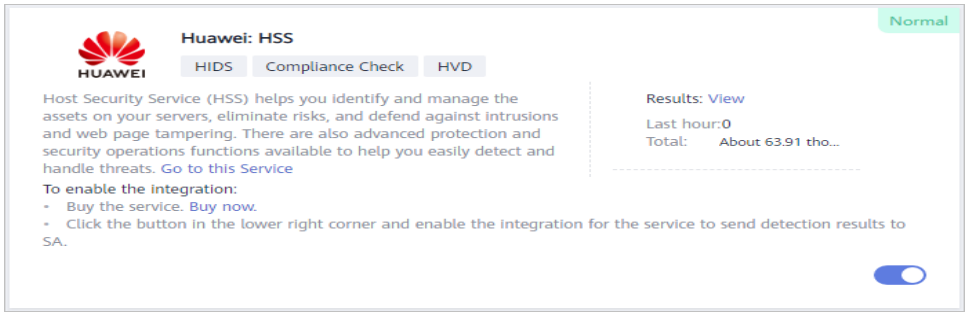
Step 3 Query the security products that have been aggregated in SA.

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**.

Figure 10-5 Viewing data from other security products



----End

10.3 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 10-1 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.
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

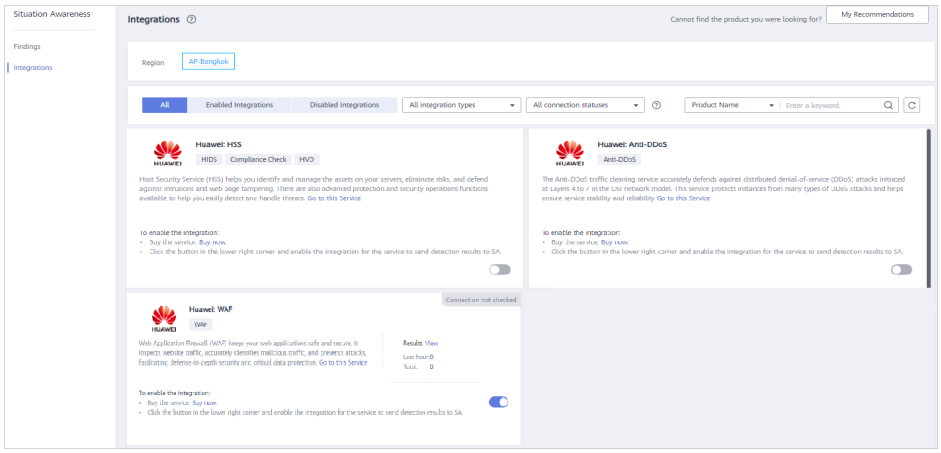
The connection status of an integration is determined by how many times the integration calls the data reporting API. An integration can call the data reporting API every 5 minutes to check the connectivity.

Procedure

Step 1 Log in to the management console.

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

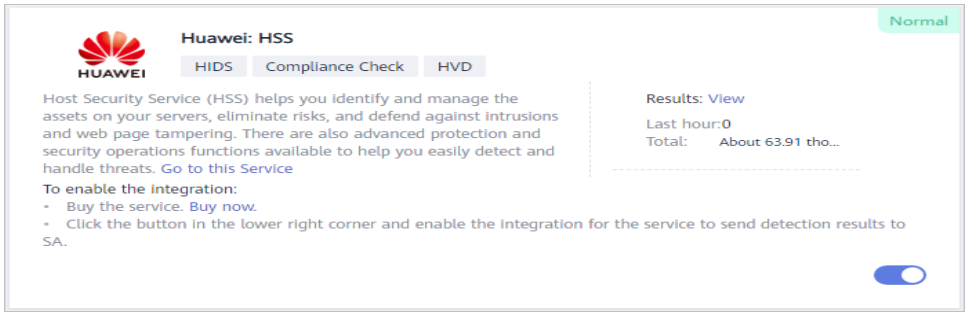
Figure 10-6 Viewing heartbeat statuses of integrations



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.

Figure 10-7 Viewing data from other security products



----End

11 Settings

11.1 Alarm Settings

11.1.1 Configuring Alarm Notifications

After the alarm notification function is enabled, SA notifies you of threat alarms by email or SMS message.

Prerequisites

Your standard or 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 & Compliance** > **Situation Awareness**.

Step 3 In the navigation pane on the left, choose **Settings** > **Notifications**. On the displayed page, choose **Alarm Settings** > **Alarm Notifications**.

Step 4 Select required notification items and risk severity options.

- **Daily Alarm Notification**

  Alarm notifications are sent to you at 10:00 every day.

  You can select notification items and risk severity as needed. The daily alarm notification takes effect only when you select at least one item for both **Notification Item** and **Risk Severity**.

- **Real-Time Alarm Notification**

  Real-time alarm notifications are sent on the hour after a threat alarm occurs.

  You can select notification items and risk severity as needed. The settings of real-time alarm notification take effect only when you set both **Notification Item** and **Risk Severity**.

To avoid disturbing, you can select **24 hours** or a specified time period in the **Notification Time** column. Then you will receive notifications only in the specified period.

Step 5 Select an SMN notification topic.

- Select an existing topic from the drop-down list or click **View** to create a topic. For details, see **Creating a Topic**.
- You can add multiple subscriptions to a topic and select multiple subscription endpoints (such as SMS messages and emails). For details, see **Adding a Subscription**.

  NOTE

  Before selecting a topic, ensure that the subscription status of the topic is **Confirmed**. Otherwise, alarm notifications may not be received.

For details about topics and subscription, see the *Simple Message Notification User Guide*.

Step 6 Click **Apply** to enable alarm notification.

Now, you will be notified by SMS message or email if an event that falls to the notification items you select is found.

----End

11.1.2 Configuring Alarm Monitoring

You can configure alarm types you want to monitor under the **Alarm Monitoring Settings** tab. After you complete the configuration, SA detects and pushes only alarms of configured types.

- Currently, you can configure alarm monitoring information in the **List Settings**, **Type and Level Settings**, and **Alarm Source Settings** areas.
  - **List Settings**: You can set a maximum of 50 pieces of information. The information must be IP addresses, IP addresses with port numbers, IP addresses with masks, or IP address ranges. Each piece of information must be different from others. Every two pieces of information must be separated with a line break.
  - **Type and Level Settings**: You can select **Brute-force attack**, **Web Attack**, **Exploit**, **Abnormal behavior**, and/or **Zombie** and specify risk severity, including **Critical**, **High**, **Medium**, **Low**, and **Informational**.
  - **Alarm Source Settings**: You can select **IDS**, **IPS**, **DDoS**, **HSS**, and **WAF** as your alarm sources.
- After alarm monitoring settings are completed, only the alarms that meet the configured conditions are listed on the **Threat Alarms** page. The alarm monitoring settings take effect only for alarms generated after the settings are completed.
- By default, no alarm monitoring settings are configured, so SA monitors attacks on all ports and IP addresses of assets and displays threat alarms of all assets across your account.

Constraints

- Select at least one alarm type and one alarm risk severity for each alarm type. Otherwise, the alarm monitoring settings will not work.
- Select at least one alarm source. Otherwise, the alarm monitoring settings will not work.

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 & Compliance** > **Situation Awareness**.

Step 3 In the navigation pane on the left, choose **Settings** > **Notifications**. On the displayed page, choose **Alarm Settings** > **Alarm Monitoring Settings**.

Step 4 Configure an alarm monitoring list.

In the **List Settings** area, click **Configure** in the **Operation** column and complete configuration in the displayed dialog box.

To set the alarm monitoring source list, perform the following steps:

1. Import a monitoring list.

   Click **Select File** and select the target file in TXT format. The selected file is displayed in the text box.

2. Enter required IP addresses, IP addresses with port numbers, IP addresses with masks, or IP address ranges in the text box.

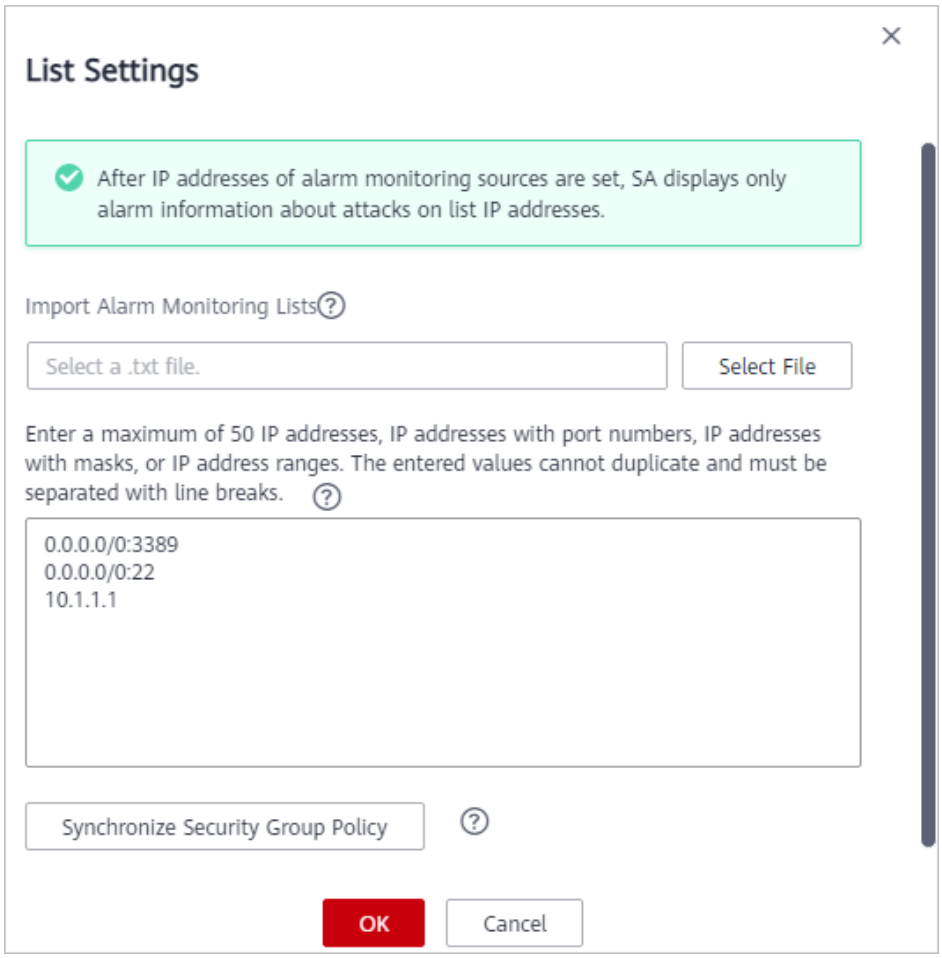
   If you enter **0.0.0.0/0:3389**, **0.0.0.0/0:22**, and **10.1.1.1** in the text box, SA only displays the alarm information of attacks to these objects. **Figure 11-1** shows an example.

3. Synchronize security group policies.

   Click **Synchronize Security Group Policy** to synchronize security group policies into the text box of **List Settings**. After the synchronization is complete, the objects to be monitored are automatically displayed in the text box.

4. Click **OK**.

Figure 11-1 Alarm monitoring list

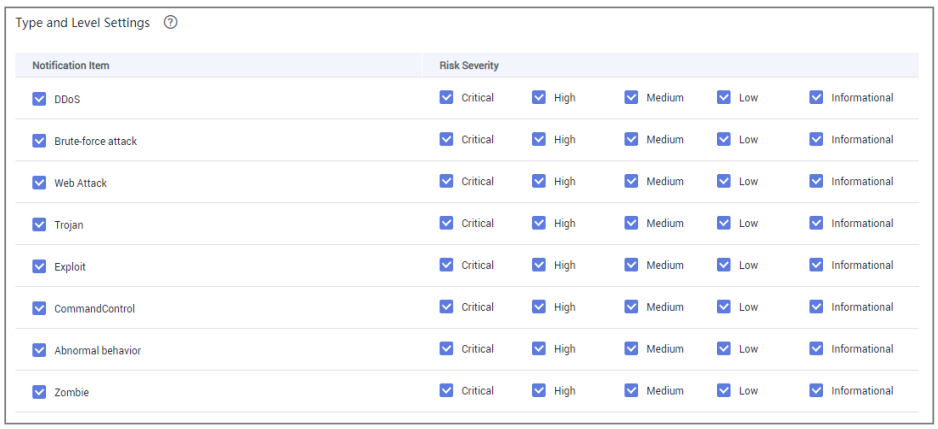


Step 5 Select the alarm monitoring type and risk severity.

In the **Type and Level Settings** area, select the notification items and alarm risk severity options of the alarm types you want to monitor. For unselected **Notification Item** and **Risk Severity**, SA will stop monitoring related alarm types.

SA then monitors the alarm information of the selected threat types and risk severity options.

Figure 11-2 Selecting the notification items and alarm risk severity options

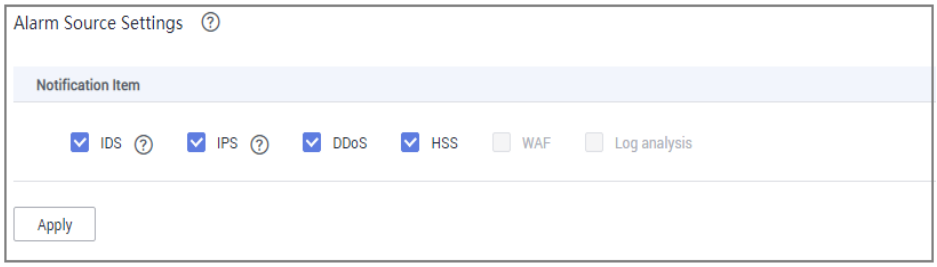


Step 6 Set the alarm sources.

In the **Alarm Source Settings** area, select the **Notification Items**.

SA then monitors the alarm information from the selected options.

Figure 11-3 Selecting notification items



Step 7 Click **Apply**. It takes 3 to 5 minutes for the alarm monitoring settings to take effect.

----End

11.2 Check Settings

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

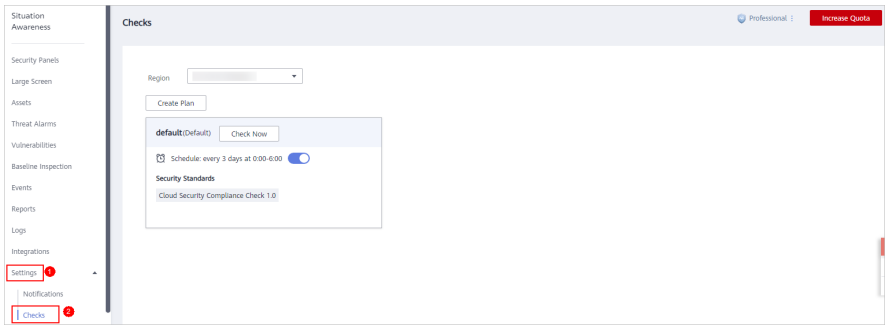
Procedure

Step 1 Log in to the management console.

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

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

Figure 11-4 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 11-1**.

Table 11-1 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. – 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 & Compliance > Situation Awareness > Baseline Inspection**.

----End

