Alibaba Cloud
Apsara Stack Enterprise

Security Administrator Guide (Advanced Edition)

Version: 1807

Issue: 20180731

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade

secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructio ns, best practices, tips, and other contents.	 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
`Italics`	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`switch` *`{stand | slave}`*

Contents

1 Overview

Apsara Stack Security Advanced Edition is an Internet protection system suitable for the protection of core business applications. It provides real-time protection capabilities, including DDoS detection/prevention, web-layer attack detection/prevention, web vulnerability discovery /repair, host vulnerability discovery/repair, and protection against host intrusion. Using a wide range of local security data derived from your existing network and cloud-based intelligence, this product performs centralized big data analysis in the security data analysis engine cluster and presents security administrators with overall security trends and allows them to trace intrusion events back to their sources. For example, it provides targeted attack detection, employee intelligence leak alerts, and intrusion cause analysis. Based on the core security information, security administrators not only can understand the security status, but can also use the custom analysis interface provided by the security data analysis engine to perform tailored analyses on existing security data. This allows you to flexibly customize your security analysis capabilities.

2 Configuration requirements

To log on to the Apsara Stack Security Center console, you must first configure your computer to meet the requirements listed in *Table 2-1: Configuration requirements*.

Table 2-1: Configuration requirements

Item	Requirement
Browser	• Internet Explorer: version 11 or later • Google Chrome (recommended): version 42.0.0 or later • Mozilla Firefox: version 30 or later • Safari: version 9.0.2 or later
Operating system	• Windows XP, Windows 7, or a later versions of Windows • macOS

3 Logon and logout

3.1 Roles for Apsara Stack Security Center

Before login on the Apsara Stack Security Center, you need create an account for Apsara Stack Security Center, and assign this user a role with permissions for the Apsara Stack Security Center.

The Apsara Stack Security Center has preset roles. You cannot add custom roles. For information on how to create users and assign them roles and permissions, see *Create a user* in the *Cite LeftAdministrator guideCite Right*.

Table 3-1: Roles for Apsara Stack Security Center

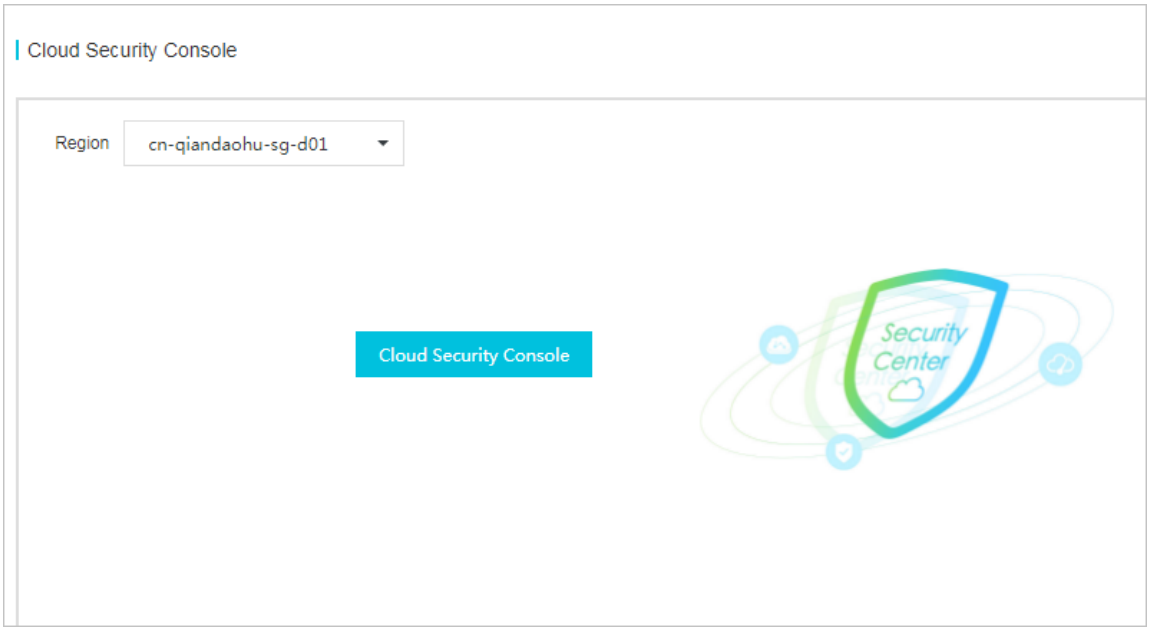
Role	Description
Cloud Security Center System Administrators	Responsible for the Apsara Stack Security Center system management and configuration. They have permissions for managing Alibaba Cloud accounts, setting alerts, and setting global parameters, but cannot perform intelligence synchroniz ation.
Cloud Security Center Security Administrators	Responsible for the security of Apsara Stack and the security policies of the Apsara Stack functional modules. They have permissions for accessing Situation Awareness, DDoS detection, server security, and all functional nodes in the asset management directories. In addition, they can set security alerts in the system management directory.
Department Security Administrators	Responsible for the security of the cloud products and resources and the security policies of the Apsara Stack functional modules for the departments that they are in. They have permissions for accessing Situation Awareness, DDoS detection, server security, and all functional nodes in the asset management directories.
Cloud Security Center Security Auditors	Responsible for the security auditing of Apsara Stack. They have permissions for viewing audit logs, setting audit policies , and accessing all the functional nodes in the security audit directory.

3.2 Log on to the Apsara Stack Security

You can log on to the Apsara Stack console and navigate to Apsara Stack Security, or log on to the Apsara Stack Security Center console directly.

- Log on to the Apsara Stack console, and go to the Apsara Stack Security console.
  a) Start Chrome.
  b) In the address bar, enter the web address of the Apsara Stack console (for example, *http://ydconsole.aliyun.com*), and press **Enter** to go to the Apsara Stack logon page.
  c) On the Apsara Stack logon page, enter the user name, password, and verification code of an existing Apsara Stack Security account.
  d) Click **Log On**.
  e) In the Apsara Stack console, choose **Console** > **Compute, Storage & Networking** > **Apsara Stack Security Center Console**.
  f) Select **Region** and click **Cloud Security Console** to go to the Security Center page, as shown in *Figure 3-1: Security Center*.

  Figure 3-1: Security Center



- Directly log on to the Security Center with the website address of the Apsara Stack console.

  Note:
  You can ask for the URL from the on-premises engineers.

a) Start Chrome.

b) In the address bar, enter the website address of the Apsara Stack Security Center (for example, http://*DTCSC address*), and press **Enter**.

c) Then, enter the user name, password, and verification code of an existing account on the Security Center.

d) Click **Log On**.

3.3 Log out of the Apsara Stack Security Center console

- Click **Exit** in the upper-right corner of the **Security Center** page to log out.

4 Apsara Stack Security Advanced Edition security center interface

The Apsara Stack Security Advanced Edition security center interface is divided into three main areas, as shown in *Figure 4-1: Apsara Stack Security Advanced Edition security center page*.

Figure 4-1: Apsara Stack Security Advanced Edition security center page

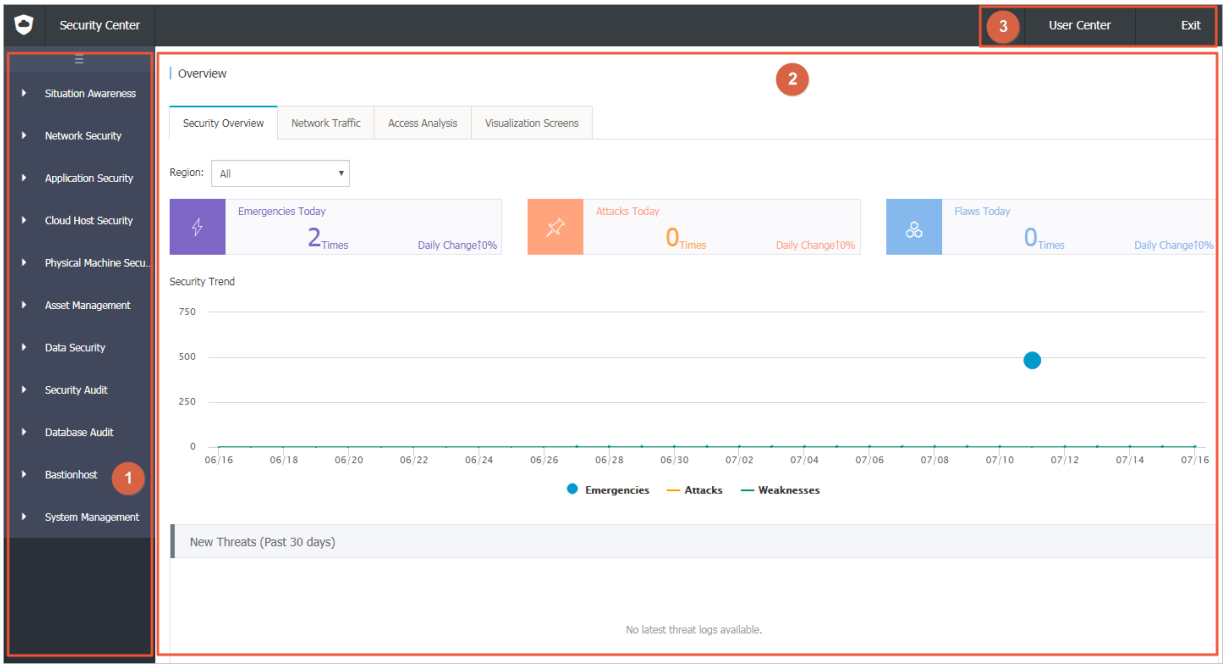


Table 4-1: Functional area descriptions describes functional areas on the webpage:

Table 4-1: Functional area descriptions

NO.	Region	Description
1	Menu navigation tree	The Apsara Stack Security Advanced Edition security center console provides six main parts: Situation Awareness, security capabilities, server security, asset management, security audits, and system management. Their functions are as follow: • **Situation Awareness**: This function detects and analyzes cybersecurity trends, performs associated tracing and big data analysis on threats, and presents the risks of potential security events. • **Network Security**: This function prevents and detects attack behavior, allowing administrators to better analyze and handle attacks.

NO.	Region	Description
		• **Server security**: This function provides host protection and intrusion detection to ensure the security of your servers. • **Asset management**: This function uses charts to present your current total assets, their increase/decrease frequency, regional distribution, and other statistical information. This allows administrators to query and view asset information by group or type, increasing their understanding of the asset situation for better asset management. • **Security auditing**: This function presents and audits cloud service operation logs. This allows auditors to promptly discover and eliminate security risks. • **System management**: Allows system administrators to configure settings of Apsara Stack Secutiry, such as alert, sychronization, and global settings.
2	Operation view area	After a menu item is selected, its function configuration interface is displayed in the right-side operation view area.
3	Operation button area	• **User Center**: Click this button to modify your profile page. • **Exit**: Click this button to log out.

5 Situation Awareness

Situation Awareness incorporates a full range of capabilities to monitor enterprise vulnerability , hacker intrusion, web attacks, DDoS attacks, threat intelligence, enterprise security reputation , and other security trends. Through modeling and analysis, this function is designed to obtain key information, including traffic features, host behavior, and host operation logs. This allows the system to detect intrusions that cannot be found only through traffic detection and file scans . By combining the output from cloud-based analysis models with intelligence data, the function identifies attack threat sources and behaviors, and assesses the level of threat.

Situation Awareness contains five main parts:

- **Overview**: Shows overall security trends, network traffic conditions, and dashboard information.
- **Emergencies**: Shows security events and development trends discovered in the business system.
- **Threat Analysis**: Shows the current security risks and threat sources facing the business system.
- **Vulnerability Analysis**: Shows existing security risks in the business system.
- **Intelligence Analysis**: Shows important self-disclosed information and the latest cybersecurity intelligence.

5.1 Overview

The **Overview** page provides an overview of situational awareness. The page represents several types of information: emergencies, threats, vulnerabilities, intelligence, network traffic, access analysis, and visualization dashboard. This gives you an overall picture of your security situation.

The Overview page mainly includes the following:

- **Security Overview**: This area presents a general overview of your current security threats, system vulnerabilities and defects, and current security intelligence from across the Internet.
- **Emergencies**: Emergencies are events that have already occurred in your system. An emergency indicates you have suffered or are suffering a security attack and you must quickly take appropriate measures to defend against the attack.
- **Threats**: Threats are events that have not yet occurred, but that may possibly threaten your system. Alibaba Cloud Security identifies threats using big data analysis and information collected from scanners. To prevent threats, you must increase your security vigilance.

- **Vulnerabilities**: This function scans and analyzes your system for vulnerabilities and defects. Vulnerabilities that hackers can use to exploit your system are displayed. You must promptly repair them to increase your system security.
- **Intelligence**: This refers to threat intelligence synced from Alibaba Cloud. In the age of cloud security, an individual system provides limited security awareness. However, by filtering, collecting, and effectively analyzing security information from across the Internet, we can identity Internet security trends and provide guidance on defensive measures for individual systems.
- **Network Traffic**: This function analyzes outgoing/incoming network traffic and QPS information and displays your high and low traffic times, speeds, and source region distribution.
- **Access Analysis**: This function identifies visitors and shows their information and the webpages they visit.
- **Visualization Dashboard**: This function provides an intuitive display of security trends and current threats, and serves as an important reference for security decisions.

5.1.1 View security overview information

Context

The **Security Overview** page includes security trends, the latest threats, latest intelligence, and information on the overall asset situation. This page presents you with a comprehensive picture of your system's security situation.

Procedure

Select **Situation Awareness** > **Overview**. On this page, you can view your system's overall security situation, as shown in *Figure 5-1: Overview page*.

Figure 5-1: Overview page

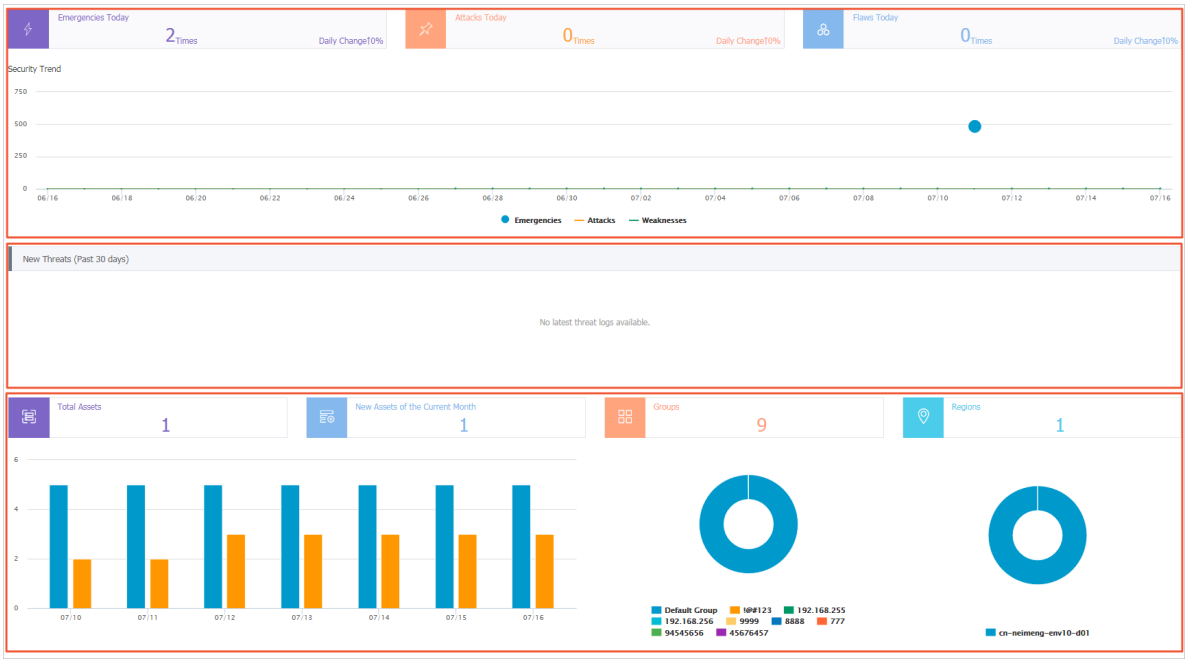


Table 5-1: Security overview page area descriptions

Page area	Description
Security trends	The security trends area displays the security events and attacks that have occurred in the current system, vulnerabilities and defects discovered in the system, and system security trends over time.
Latest threats	The latest threats area displays the security threats currently facing your system. These are threats that require your urgent attention. **Note:** These threats are identified by Apsara Stack Security's core scanner function and special Apsara Stack big data analysis models.
Asset overview	This area displays information on your most important assets, allowing you to keep informed about your assets in real time.

5.1.2 View network traffic information

Context

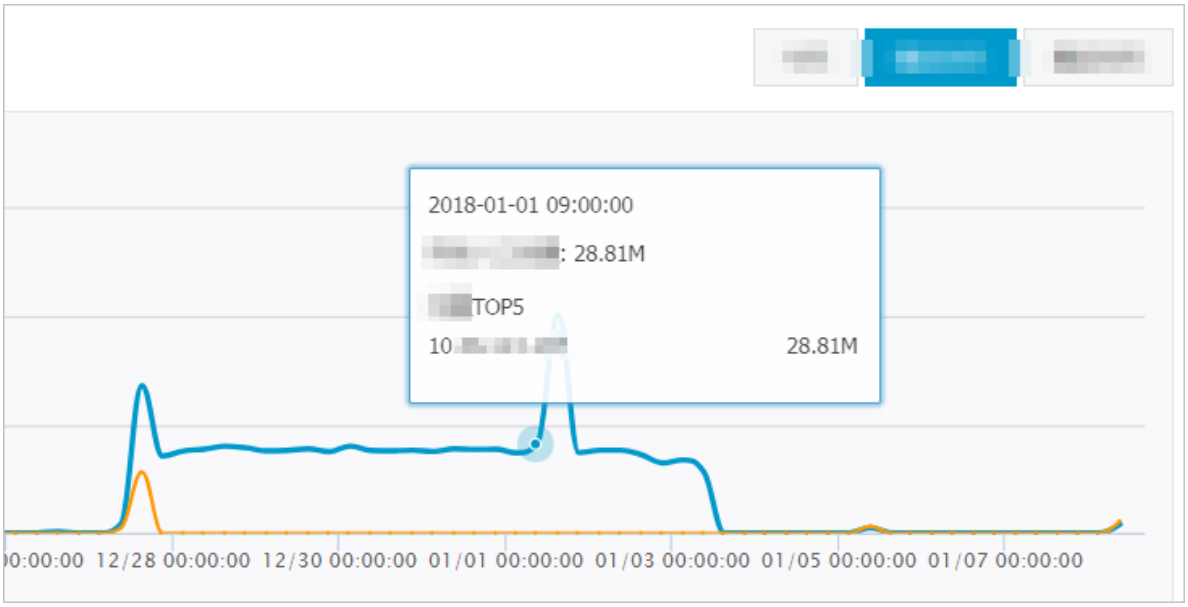
The Network Traffic page uses line graphs to show traffic information for a past time period. By viewing the traffic conditions for different periods, regions, or a single IP address, you can identify your high and low traffic periods and view traffic speed and region distributions. This page also

shows the five IP addresses that generate the most traffic, so you can effectively block access by malicious IP addresses.

Procedure

1. Click**Overview** > **Network Traffic** to display the traffic viewing page.
2. On the page, click the **Today**, **Last 30 Days**, or **Last 90 Days** buttons to view traffic information for the selected period.
3. In the **Region** area, you can select a region and enter an IP address in the search box to query traffic information by region and IP address.
4. Move your cursor over the traffic graph to display the five IP addresses that generate the most traffic, as shown in *Figure 5-2: View top five IP addresses by traffic*.

Figure 5-2: View top five IP addresses by traffic



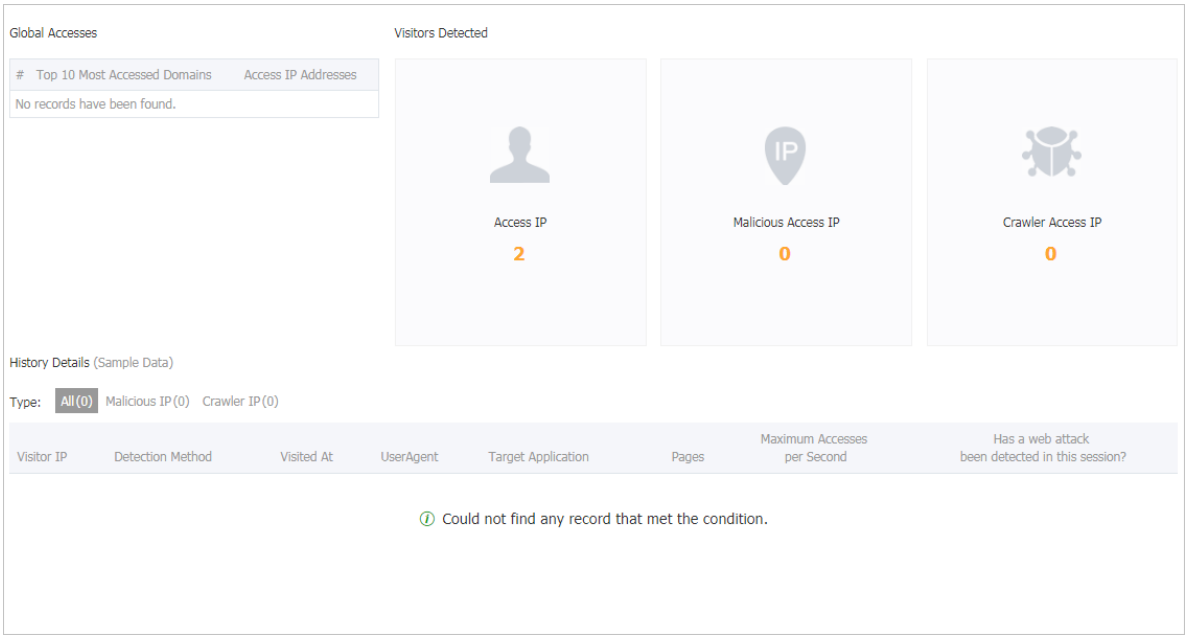
5.1.3 View access analysis results

Context

The Access Analysis page analyzes and screens access results from different sources. Using big data analysis, the system classifies access as normal access, malicious access, and crawler access. This allows you to effectively understand the security risks facing your system due to malicious and crawler access and identify the sources of such access traffic.

- Select**Overview** > **Access Analysis**to display the access analysis page, as shown in *Figure 5-3: Access analysis page*.

Figure 5-3: Access analysis page



5.1.4 View Visualization Dashboard

Context

The Visualization Dashboard uses animations to present key security event metrics. This gives you a general picture of your security situation and provides effective support for security decisions.

The Visualization Dashboard currently supports access traffic dashboard and security monitoring dashboard.

Procedure

1. Select**Overview** > **Visualization Dashboard**to display the Visualization Dashboard portal.

   Click **Modify** at the top of the page to modify the display scale of the access traffic dashboard.
2. Click the screen shown on the page to go to the Dashboard page.

   - **Access traffic dashboard**

     Powerd by the access and traffic monitoring and reporting capabilities of the Apsara Stack Security traffic security monitoring module, the access traffic dashboard provides statistics on the source regions and quantities of current requests and attacks. It also displays the system's overall traffic situation and lists the top five request and attack source regions. This gives you an accurate picture of the regional distribution of requests and attacks.

The access traffic dashboard traffic information sources and implementation mechanisms are shown in *Table 5-2: Access traffic data source table*.

Table 5-2: Access traffic data source table

Type	Implementation mechanism
Request analysis	The system pushes the assets that interest you to the traffic security monitoring module, which reports access information for these assets.
Attack analysis	Apsara Stack Security's traffic security monitoring module detects, reports and displays events similar to web attacks.
Traffic display	The traffic security monitoring module collects and reports traffic information to the console for the record.

- **Security monitoring dashboard**

  The security monitoring dashboard shows detailed information about the security events currently facing your system. By analyzing system vulnerabilities and defects and the assets that have been attacked or drawn the particular interest of hackers, this dashboard evaluates your system's security situation and displays its current security grade.

  The data shown on this dashboard is derived mainly from reports and scans by modules such as Apsara Stack Security traffic security monitoring, Server Guard, and vulnerability analysis. The top five assets that interest hackers most are determined by modeling and analysis performed by the big data engine.

5.2 Emergencies

Emergencies are security events that have occurred or are currently occurring in the system. Emergencies are discovered and reported through scans performed by Alibaba Cloud Security modules, such as traffic security monitoring, Server Guard, and vulnerability analysis. Emergencies require you to pay immediate attention and take appropriate security measures.

For information on emergency event types and definitions, see *Table 5-3: Emergency event type table*.

Table 5-3: Emergency event type table

Emergency event type	Description
Backdoor	The Server Guard client detects Webshell backdoors in your system. The big data analysis module imports traffic analysis information from the traffic security monitoring module to detect single-statement and multi-functional trojans.
Successful brute-force attack	When a brute-force password cracking attack succeeds, the Server Guard client reports the relevant information. This event is shown in the emergency list and requires your immediate attention.
Unauthorized download	Distinctive responses within a specified quantity range (greater than 1, less than 20) are selected from the output traffic of the traffic security monitoring module. This allows the big data analysis module to detect unauthorized downloads.
Bot behavior	A host is controlled by hackers and used as a bot to launch external attacks.
Page tampering	The vulnerability analysis module scans accessible webpages and reports page tampering. This mainly targets hidden-chain attacks.

5.2.1 View Event Analysis

Procedure

1. Select **Situation Awareness** > **Event Analysis** to go to the Event Analysis page.
2. You can enter keywords in the **Type** field to search for emergencies of the specified type.

5.3 Threats

The threat page has two parts: threat analysis and attacks.

Threat analysis

The unique Apsara Stack big data model analyzes traffic information to discover attack features and integrate information by attack type. This provides information on the security risks currently facing your system.

Threat analysis mainly covers the following information:

- This shows normal attack and targeted attack trends for the last seven days and attack analysis information for the last 30 days.

- Top five assets that interest hackers most: This section analyzes traffic using the big data model and rates the threats facing each asset. The five most risky assets are displayed for your protection.
- Targeted attack analysis: This section uses the big data model to analyze the traffic information provided by the traffic security monitoring module, so as to analyze and detect targeted attacks.

  Current targeted attack types are shown in *Table 5-4: Targeted attack type descriptions*.

  Table 5-4: Targeted attack type descriptions

Targeted attack type	Description
Targeted host password cracking	Targeted host brute-force password cracking attacks attempt to crack users' logon passwords. Hackers generally launch untargeted cracking attacks on host passwords. A targeted attack generally implies that hackers are interested in specific assets.
Credential stuffing attacks	The system analyzes abnormal logon behavior to detect behavior resembling credential stuffing attacks. Such attacks indicate that hackers may be using username and password combinations leaked on the Internet in an attempt to forcibly log on to your website. This may harm the interests of your users.
Batch account logon	The system detects attackers using a large number of low-quality accounts to log on to your system. Such accounts are most likely bot accounts.
Fixed point web attack	When the system discovers a fixed point web attack clearly targeting you, this means that hackers are more interested in your website than other users. In addition, they may have carried out SQL injection, command execution, directory scanning, or some other malicious operations on your website.
CMS abnormal logon	The system detects abnormal logon events for the application management background. If you did not perform this login attempt, a hacker may have already stolen your background password. In this event, we suggest you check the strength of your password and change the existing password as soon as possible.

Attacks

The main attack types are web application attacks and brute-force cracking attacks:

- **Web Application Attacks**: All web server access traffic goes through the Alibaba Cloud Security traffic security monitoring module. This module monitors the traffic and extracts attack

information from the traffic. Given specific business needs, the traffic security monitoring module does not currently provide the capability to directly block attack traffic.

- **Brute Force Cracking**: When a hacker attempts to crack an asset, the Server Guard client promptly monitors and reports this cracking attempt to console.

5.3.1 View threat analysis results

- Select**Situation Awareness** > **Threats**to display the **Threat Analysis** page.

  This page displays attack trends for the past seven days, attack analysis information for the past 30 days, the asset IP addresses that most interest hackers, and targeted attack analysis information.

5.3.2 View attack information

- Select**Situation Awareness** > **Attacks** > **Application Attacks**to display the **Application Attack** page.

  This page displays attack trends, attack types, and detailed attack information for the past seven days.
- Select**Attacks** > **Brute-force Cracking**to view brute-force cracking event records.

5.4 Vulnerabilities

The **Vulnerability** page displays existing system vulnerabilities and defects. These vulnerabilities can be exploited by hackers to perform illegal operations. You must promptly eliminate vulnerabilities to improve the security of your system.

Currently, the Vulnerabilities page shows three types of information:

- **Vulnerabilities**
  - Application Vulnerabilities: The vulnerability analysis module uses scan engine rules to scan applications installed on ECS instances. It reports any defects it discovers.
  - Host Vulnerabilities: Server Guard scans host systems for vulnerabilities and reports any vulnerability it detects.
- **Weak Passwords**: The system detects simple asset passwords that are easy to guess or crack. It will remind you to change problematic usernames and passwords and increase their complexity.

  Weak passwords are a major security risk to your system. We suggest that, when setting system and application accounts, you should preferably increase the complexity of passwords

(for example, require them to contain numbers, letters, and special characters, be of a certain length, an so on). At the same time, you should manage passwords hierarchically. For important passwords, such as SSH logon usernames and passwords, you must use more complex passwords and change them regularly.

Custom Weak Passwords Scanning: If necessary, in addition to common usernames and passwords, you can use special usernames and passwords based on your own needs. Apsara Stack Security allows you to set custom weak password rules. You can add common weak usernames and passwords to the vulnerability analysis module's scanning rules for a personalized weak password scan of your system.

- **Configuration Item Leaks**: If your system configuration files or other sensitive files are stored at an improper location, attackers may be able to obtain them illegally, resulting in the leak of key information. The vulnerability analysis module scans your system configuration files and reports any possibility of unauthorized access.

5.4.1 View vulnerability information

Context

Vulnerabilities are classified into application vulnerabilities and host vulnerabilities. Application vulnerabilities are vulnerabilities in installed applications, which are detected and reported by the vulnerability scan module. Host vulnerabilities are vulnerabilities in your hosts, which are detected and reported by the Server Guard module. The following figure shows the Application Vulnerabilities page.

Procedure

1. Select**Situation Awareness** > **Vulnerabilities**to display the **Vulnerabilities** page and view application vulnerability information.

   The **Application Vulnerabilities** page shows vulnerability analysis information for the last seven days and detailed information on specific application vulnerabilities.

   In the Application Vulnerabilities list, click **Verify Now** in the **Repair Result Verification** column to send verification information to the vulnerability analysis module. This module verifies the repair status of the selected vulnerability.

2. Click**Vulnerabilities** > **Host Vulnerabilities**to view host vulnerability information.

   Note:

This vulnerability information is reported by the Server Guard module. To perform specific host vulnerability operations, go to the**Server Security** > **Host Protection** > **Patch Management**page.

5.4.2 View and add weak passwords

Procedure

1. Click **Weak Passwords**, to view information on detected weak passwords.
2. Click **Custom Weak Passwords**, to set custom rules for certain types of weak passwords.

   The Custom Weak Password page displays the weak usernames and passwords currently configured in the vulnerability analysis module. Click **Add** to add custom weak password rules.

   Perform the following procedure to add and activate custom weak password rules:

   1. Click **Add** to open the add weak password dialog box.
   2. Follow the prompts to set a weak password rule and then click **OK**.
   3. After adding the rule, click **Export** to generate and download the new weak password configuration file.

      Note:
      The file is always stored at `C:\Users\Username\Downloads` and downloaded as a .zip archive, which you do not have to extract.
   4. Upload this archive to the system that contains the vulnerability analysis Cactus-keeper module's master project. For example, upload it to the `/root/war/` directory and run the script `cactusConfig.sh`.
   5. After running the script, the new weak password rule takes effect.

5.4.3 View configuration item inspection results

- Click **Configuration Item Inspection** to view configuration item inspection results.

  The Inspection Results page shows the addresses of configuration item leaks detected by the vulnerability scan module.

  If hackers access one of these addresses without authorization, they may obtain your sensitive information, resulting in information leakage.

  Based on the scan inspection results, you must promptly add permission protection to the directories that store configuration files, or move sensitive files to a secure directory.

6 Network Protection

6.1 DDoS detection

The DDoS attack traffic detection function is provided by the Apsara Stack Security traffic security module. The DDoS traffic cleaning module automatically redirects, cleans, and reinjects detected attack traffic. This provides protection against DDoS attacks and ensures that your business functions normally.

6.1.1 DDoS events

6.1.1.1 View DDoS Event list

Procedure

1. Select **Network Security** > **DDoS Detection** > **DDoS Events**to view the list of all detected DDoS events.
2. Set the query conditions and click **Query**. A list of events that match the query conditions is returned.
   - When cleaning traffic, Apsara Stack Security reports security events to the Apsara Stack security center console. On the **DDoS Events** page, click **Query** results to view the event.
   - After cleaning ends, Apsara Stack Security once again reports the security event to its security center console. Now, click **Query** again to check that the security event status has changed to **`Cleaning Complete`**.

6.1.1.2 View DDoS event details

- Select an item listed on the**Apsara Stack Security Center** > **Security Capabilities** > **Anti-DDoS** > **DDoS Events**page and click **Traffic Analysis** to view the proportion of current traffic resulting from attack events and an analysis of the top ten attack targets.
- Select an item listed on the**Apsara Stack Security Center** > **Security Capabilities** > **Anti-DDoS** > **DDoS Events**page and click **View Traffic** to view the current threshold settings and traffic graph for the selected host.

6.1.2 DDoS settings

6.1.2.1 Set an anti-DDoS policy

When you set a DDoS traffic alert threshold, after traffic to this server reaches the threshold, the system triggers a traffic alert. The server's threshold must be set based on the server's traffic. Excessive traffic volume indicates a possible DDoS attack.

For the threshold, we generally recommend a value slightly higher than the server's traffic peak.

Apsara Stack Security supports global threshold settings, CIDR block threshold settings, and single-host threshold settings:

- Global threshold: You cannot add a global threshold. The default value is imported during service initialization.
- CIDR block threshold: You can set alarm thresholds for specific CIDR blocks based on their normal traffic features. The CIDR block threshold allows you to set thresholds for CIDR blocks that are more precise than the global threshold.
- Single-host threshold: This method allows you to set alert thresholds for individual hosts based on their specific traffic features. The single-host threshold setting method allows you to set thresholds for individual hosts that are more precise than the CIDR threshold.

Table 6-1: Anti-DDoS policy parameter descriptions

Paramete	Description
qps	Sets the HTTP request speed alert frequency for data center hosts. When the incoming HTTP request speed reaches this threshold, DDoS detection is triggered. Generally, this value is set up to be slightly higher than the traffic peak. We suggest setting the threshold to 100,000 QPS or more. HTTP request speeds are measured in QPS (requests per second).
pps	Sets the data center's packet speed alert threshold. When the incoming and outgoing packet speed reaches this threshold, DDoS detection is triggered. Generally, this value is set up to be slightly higher than the traffic peak. We suggest setting the threshold to 200,000 PPS or more. Packet speeds are measured in PPS (packets per second)
newconn	Sets the data center hosts' new connection quantity alert threshold. When the quantity of new connections reaches this threshold, DDoS detection is triggered. Generally, this value is set up to be slightly higher than the traffic peak. We suggest setting the threshold to 1,000 or more. New connections are measured in connections per second.

Paramete	Description
bps	Sets the data center's bandwidth alert threshold. When the incoming and outgoing traffic speed reaches this threshold, DDoS detection is triggered. Generally, this value is set up to be slightly higher than the traffic peak. We suggest setting the threshold to 100 Mbit/s or more. Bandwidth is measured in Mbit/s (megabits per second).

Note:

Before adding a threshold, you must make sure the corresponding CIDR block has already been added on the**System Management** > **Global Settings** > **Traffic Collection CIDR Blocks**page.

6.1.2.2 View Threshold list

- Select**Apsara Stack Security Center** > **Security Capabilities** > **DDoS Detection** > **DDoS Settings**to view the list of all thresholds.

6.1.2.3 Set an alert threshold

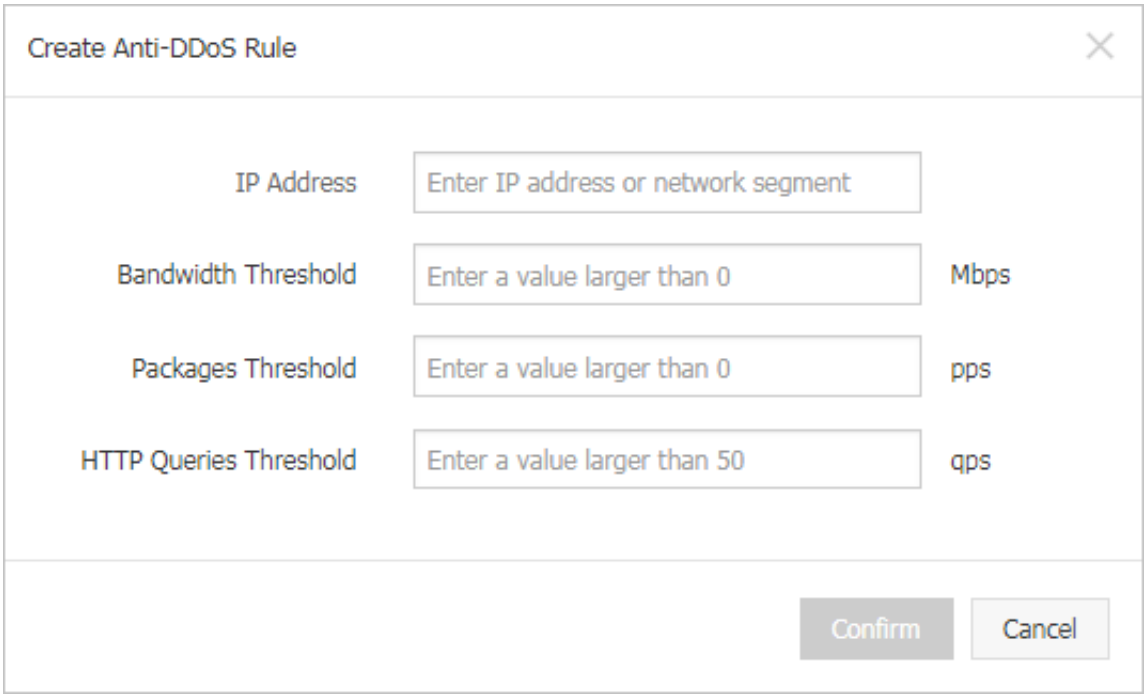
Context

When you set an alert threshold for a specific CIDR block or host, this threshold is used to more accurately trigger DDoS detection. Otherwise, DDoS detection is triggered according to the global threshold.

Procedure

1. On the**Apsara Stack Security Center** > **Security Capabilities** > **DDoS Detection** > **DDoS Settings**page, click **New Protection Policy**.
2. In the **new protection policy** dialog box that appears, enter the appropriate CIDR block and threshold value and click **OK** to set the alert threshold, as shown in *Figure 6-1: New protection policy dialog box*.

Figure 6-1: New protection policy dialog box



6.1.2.4 Modify alert threshold

Procedure

1. On the**Apsara Stack Security Center** > **Security Capabilities** > **DDoS Detection** > **DDoS Settings**page, click **Modify** for a specific protection policy.
2. In the **modify protection policy** dialog box that appears, enter the appropriate threshold value and click **OK** to modify the alert threshold.

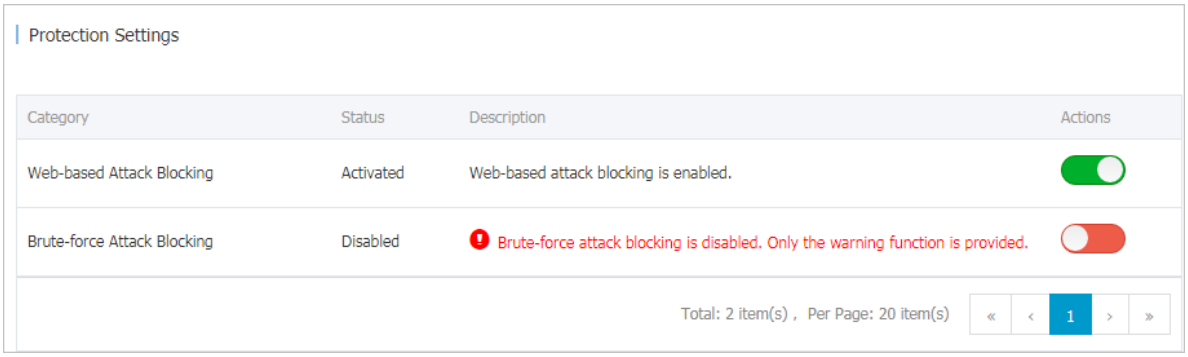
6.1.2.5 Enable network security blocking

Procedure

1. Choose **Network Security** > **Protection Settings**.
2. In the Blocking Switches area, click the Web-based Attack Blocking or Brute-force Attack Blocking switch to enable or disable each feature, as shown in *Figure 6-2: Blocking Switches setting*.

> **Note:**
> After a block feature is disabled, the corresponding interception feature is also disabled, and only the alert feature is available.

Figure 6-2: Blocking Switches setting



6.2 Cloud Firewall

As a firewall product used in cloud environments, Cloud Firewall solves the problem of vague or undefined security boundaries amid the rapid changes of cloud businesses. The Cloud Firewall module can help you partition businesses and deploy isolation policies for ECS instances in Apsara Stack environments.

6.2.1 Before you begin

Before configuring the Cloud Firewall, you must prepare the following plans based on your actual business conditions:

- Plan the necessary business partitions, such as testing areas and development areas.
- Plan the server roles required for each business partition, such as web applications and database servers.
- Determine the relationships between your ECS instances and business partitions and server roles. Each ECS instance must be assigned to a business partition or server role group.

6.2.2 Import ECS instances

Context

Using the following procedure, import ECS instances to the partition.

Procedure

1. On the **Cloud Firewall Topology** page, select the region containing the ECS instances you want to manage and the name of the relevant VPC.
2. Move your cursor to the created business partition and click the Add/Manage Assets button in the upper-left corner of the partition to open the **Add/Manage Assets** page.

3. On the **Add/Manage Assets** page, select the **Add** tab.
4. Based on the plans you have already prepared, select the ECS instances you want to add to this business partition and click **Add Now**.
5. After adding ECS instances to the business partition, you can return to the **Add/Manage Assets** page and select the **Manage** tab. This allows you to manage the ECS instances in the business partition. For example, you can change an ECS instance to another business partition or role group.

6.2.3 Establish a role group and assign imported ECS instances to it.

Establish a role group in a Cloud Firewall business division and then assign imported ECS instances to this role group.

6.2.3.1 Group ECS instances with clearly defined roles

Context

Perform the following procedure to establish a role group and then assign ECS instances with clearly defined roles to this role group.

Procedure

1. Log on to the Cloud Firewall console.
2. On the **Cloud Firewall Topology** page, select the region of the business partition to manage and the name of the relevant VPC.
3. Move your cursor to the created business partition and click **Role Management** in the upper-left corner of the partition.
4. On the **Role Management** page, click the "+" button next to the source role group to create a role group.
5. Enter the role group name and click **OK**.
6. Based on the ECS instance information in the access source, select the source role group created for the relevant ECS instances.

6.2.3.2 Group ECS instances with unclear roles

Context

When ECS instances do not have clearly defined roles, Cloud Firewall provides functions to define the role of each ECS instance. The relevant procedure is as follows:

Procedure

1. On the **Cloud Firewall Topology** page, select the region containing the ECS instances you want to manage and the name of the relevant VPC.
2. Click **Smart Search/Display** in the upper-right corner of the page.
3. On the **Smart Search/Display** page, select the **Between Hosts** traffic line display rule and then click **Save and Run**.

   Note:
   Based on your actual situation, you can select either Between Hosts (no internal group lines) or Between Hosts (with internal group lines).
4. In the business partition, move your cursor over an ECS instance node to view server information for this instance.
5. Click an ECS instance node to view the access relationships between this ECS instance and other servers.

   Note:
   You can go directly to the **Role Management** page to view server information for all ECS instances in the current business partition, as well as the access relationships between ECS instances and other servers. This allows you to determine the appropriate role groups for ECS instances.
6. If the topology shows an excessive number of traffic lines, you can click **Smart Search/Display** in the upper-right corner of the page to filter out unrelated information and show only the information you need:

   - You can choose a time period for the displayed traffic lines. For example, if you select seven days, the Cloud Firewall topology only shows traffic lines that have occurred in the last seven days.

     Note:
     If a traffic line was used once during the selected period, it is displayed in the topology diagram.
   - You can also use basic filters for traffic line rules. The Between Roles option only displays access traffic across role groups. Between Hosts does not show traffic between role groups,

but displays traffic between ECS instances. For the Between Hosts option, you can also choose whether to display traffic between hosts in the same role group.

- In addition, you can use custom search rules to filter traffic lines and remove unnecessary information.

Note:

- The system has one default rule.
- You can add up to 10 custom search rules.
- Search rules can be combined.
- The matching sequence among search rules goes from top to bottom.
- Each search rule can be separately used to show or hide the matching information.
- You can activate or deactivate search rules in the selection box on the left. The default rule cannot be deactivated.
- Example of applying search rules: Add the following rule to only show traffic at port 80 and ECS instances in business partition 1.

6.2.4 Review traffic and deploy access control policies

Context

In the Cloud Firewall console, you can review legality of traffic lines one by one and deploy access control policies. The procedure is as follows:

Note:

If you do not publish a business partition, the operations and deployed policies in this partition are not actually published and do not affect your actual business.

Procedure

1. Log on to the Cloud Firewall console.
2. On the **Cloud Firewall Topology** page, select the region of the business partition for deployment and the name of the relevant VPC.

   The traffic lines are all red by default, and you must confirm the legality of the lines one by one.
3. Through the traffic review process, you define a corresponding whitelist access control policy.

Note:

After a traffic line is approved, it turns green.

- You can click a traffic line and select Allow or Reject, to define the access control policy for the selected traffic line.
- You can also click **Add** in the establish policy area of the Role Management page to add an access control policy.

> **Note:**
> We suggest you use the topology to provide a visual presentation of specific traffic line operations when defining access control policies.

- You can also go to the **Cloud Firewall Topology** page and click **Add Policy** in the upper-right corner to manually add an access control policy.

> **Note:**
> We suggest you use the topology to provide a visual presentation of specific traffic line operations when defining access control policies.

6.2.5 Publish a business partition to issue access control policies

Context

When you have deployed access control policies, publish the business partition. The procedure is as follows:

Procedure

1. Log on to the Cloud Firewall console.
2. On the **Cloud Firewall Topology** page, select the region of the business partition to you want to publish and the name of the relevant VPC.
3. Click **Publish** in the upper-right corner of the page.
4. Select the publishing mode and the business partition to publish and then click **OK**.

> **Note:**
> If you have not yet confirmed the suitability of the policy configuration for this business partition, you can publish in observation mode. In observation mode, Cloud Firewall only simulates traffic to test the access control policies. These policies do not actually block traffic.

5. If, after publishing a business partition, you select **Intercept Mode**, all traffic not defined in the whitelist policy is blocked.

Note:

Before publishing a business partition in intercept mode, you must check all the policies configured in the business partition.

6.2.6 Temporarily use the one-key complete access function

Context

Business interruption may be caused by an error in incorrect firewall policy configuration. In this situation, traditional manual troubleshooting process often does not work and takes a long time.

After publishing a business partition, if the firewall policy configuration interrupts your business , you can use Cloud Firewall's one-key complete access feature to temporarily suspend access policies for the business partition. This gives you more time to find and fix the problem. The procedure is as follows:

Procedure

1. Log on to the Cloud Firewall console.
2. On the **Cloud Firewall Topology** page, select the region of the business partition and the name of the relevant VPC.
3. Click **One-key Complete Access** in the upper-right corner of the page.
4. Select the business partition for which to allow complete access and then click **OK**.
5. After troubleshooting the problem, you can click **One-key Restore** in the upper-right corner of the Cloud Firewall Topology page to automatically reapply the access control policies you had temporarily suspended. This restores the original policy configuration of the business partition.

6.2.7 Manage all Cloud Firewall resources

Context

In the Cloud Firewall console, you can manage your business partitions, role groups, and ECS instance resources on the **Resource List** page. The procedure is as follows:

Procedure

1. Log on to the Cloud Firewall console.
2. On the **Cloud Firewall Topology** page, click **Back to Resource List** in the upper-left corner.
3. Here, select the region of the resources you want to manage and the name of the relevant VPC.

4. On the **Resource List** page, you can manage Cloud Firewall resources.

> **Note:**
> On this page, you can add and modify resources. However, the changes only take effect after the relevant business partition is published.

6.2.8 Manage access control policies

Context

After publishing a business partition, you can view and manage the access control policies you have created on the **Policy Management** page in the Cloud Firewall console. The procedure is as follows:

Procedure

1. Log on to the Cloud Firewall console.
2. On the **Cloud Firewall Topology** page, click **Back to Resource List** in the upper-left corner.
3. Click **Policy Management**.
4. On the **Policy Management** page, select the region of the policies you want to view or manage and the name of the relevant VPC.
5. Manage access control policies.
   - On this page, you can view or delete access control policies configured for the current network region.
   - On the Policy Management page, you can also click **Add Policy** to manually add an access control policy. We strongly recommend that you use the visual traffic line operation display provided by the Cloud Firewall's topology diagram when defining access control policies.

> **Note:**
> On this page, you can add and modify resources. However, the changes only take effect after the relevant business partition is published.

7 Web Application Firewall

7.1 Overview

As one of Apsara Stack's proprietary website security protection products, Web Application Firewall (WAF) can protect website applications against attacks intended to exploit common web vulnerabilities. Such attacks include SQL injection, XSS, and other common web application attacks, or CC attacks and other attacks that affect website availability by consuming resources. At the same time, you can customize precise protection policies based on the individual features of your website business and use these policies to filter malicious web requests targeting your website.

Apsara Stack Security's WAF provides traffic protection for HTTP and HTTPS website businesses. On the WAF management interface, you can independently import certificates and private keys to fully encrypt your business and prevent data monitoring on connections. This product also meets the security protection needs of HTTPS businesses.

7.1.1 Restrictions

WAF is subject to the following restrictions:

- The product can provide access protection for at most 100 domain names. It supports wildcard domain names and has no limit on the number of first or second-level domain names.
- The product only supports domain name protection for HTTP port 80 and HTTPS port 443.

7.1.2 Configure WAF domain name access

You may perform the following procedure to configure WAF access for the domain names you want to protect.

7.1.2.1 Before you begin

To configure domain name access for WAF, you must prepare the following information:

- The information of the domain names you want to protect (you cannot simply use the IP address)
- The IP addresses of origin sites (the real server)

> **Note:**
> WAF allows you to configure up to 20 origin site IP addresses for a single domain name.

- For HTTPS businesses, you must also prepare server credentials and private keys.

7.1.2.2 Add a protected domain name

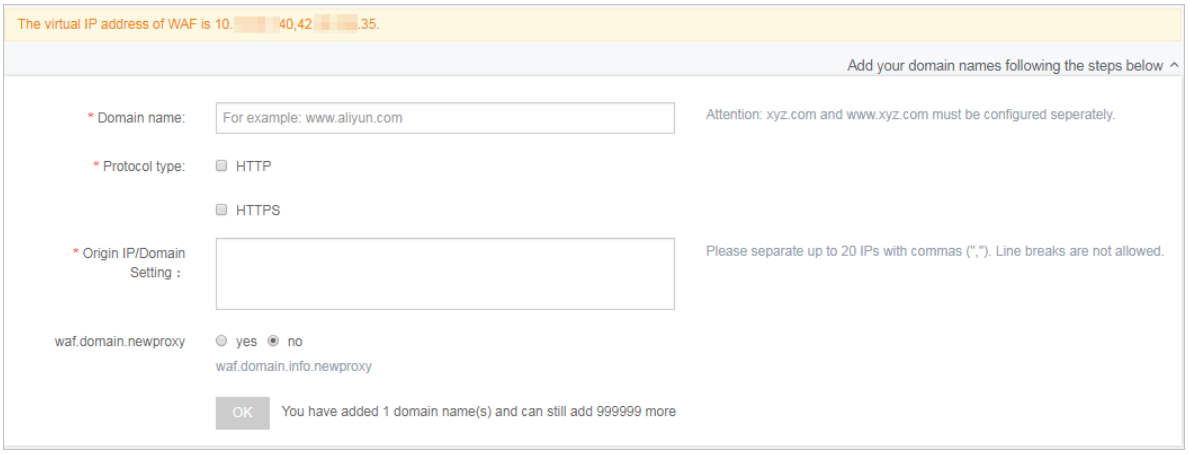
Context

Perform the following procedure to add a domain name to WAF's domain name configuration:

Procedure

1. Log on to the WAF console.
2. Click **Domain Name Configuration**, as shown in *Figure 7-1: WAF Domain Name Configuration page*.

   Figure 7-1: WAF Domain Name Configuration page



3. Enter the domain name you want to protect, select the protocol type, and enter the back-to-source IP address.

   Note:
   Here, the back-to-source setting is the address to which you want WAF to forward requests. Normally, it is the address of the actual server (such as the IP address of your ECS instance). It can also be the IP address of a Server Load Balancer.

4. Click **OK**.

   Note:

   - Wildcard domain names are supported, such as "*.aliyundemo.cn". You can also match related second-level domain names. When both a wildcard domain name and a precise

domain name are configured, the precise domain name has the priority for forwarding and protection policy matching.

- If you have an HTTPS website, you must select the type of HTTPS protocol. We suggest you simultaneously select the HTTP protocol type to ensure smooth access and avoid HTTP redirects and other problems.
- WAF supports up to 20 origin site IP addresses and provides load balancing and health check functions.
- If you have already configured CDN, Anti-DDoS Pro, or another layer-7 proxy for your domain name, you must select Yes for the **Are you already using a proxy?** option. This way, you can ensure the WAF security policies will apply to the real access source IP addresses.

7.1.2.3 Upload HTTPS certificates and private keys (only for HTTPS domain names)

Prerequisites

Note:
If the domain name you want to protect does not support HTTPS protocol, skip this step.

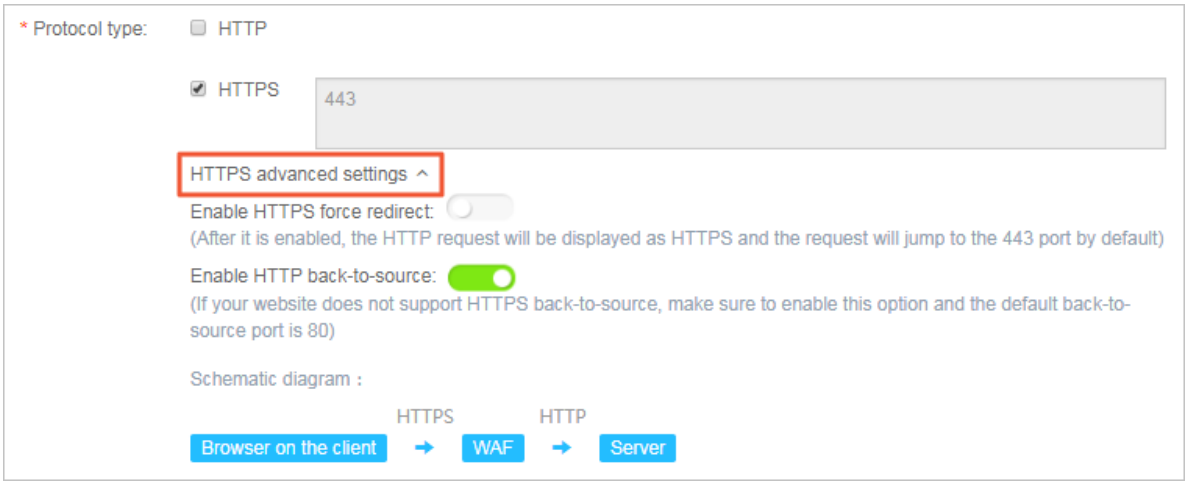
Context

If the website you want to protect has an HTTPS domain name, you must upload server certificates and private keys to WAF. Otherwise, your HTTPS website will not be normally accessible.

Procedure

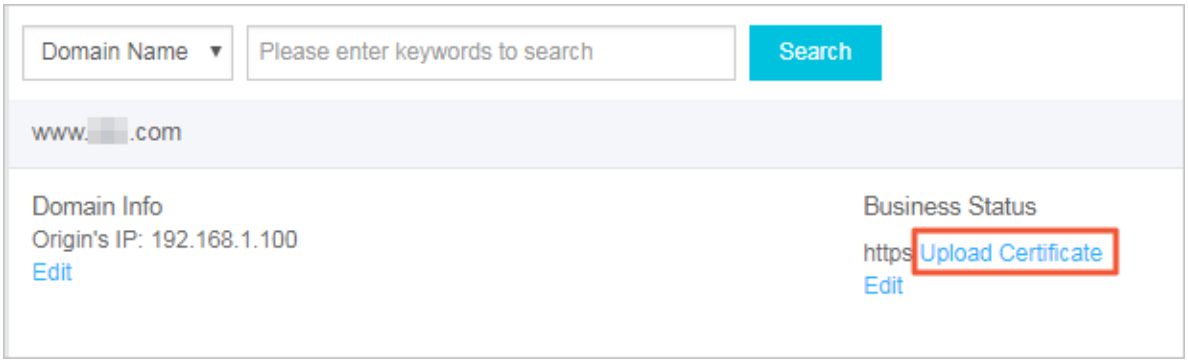
1. When adding an HTTPS website domain name on the **Domain Name Configuration** page, click **HTTPS Advanced Configuration** to select the HTTPS protocol back-to-source method and redirect settings, as shown in *Figure 7-2: HTTPS advanced settings*.

Figure 7-2: HTTPS advanced settings



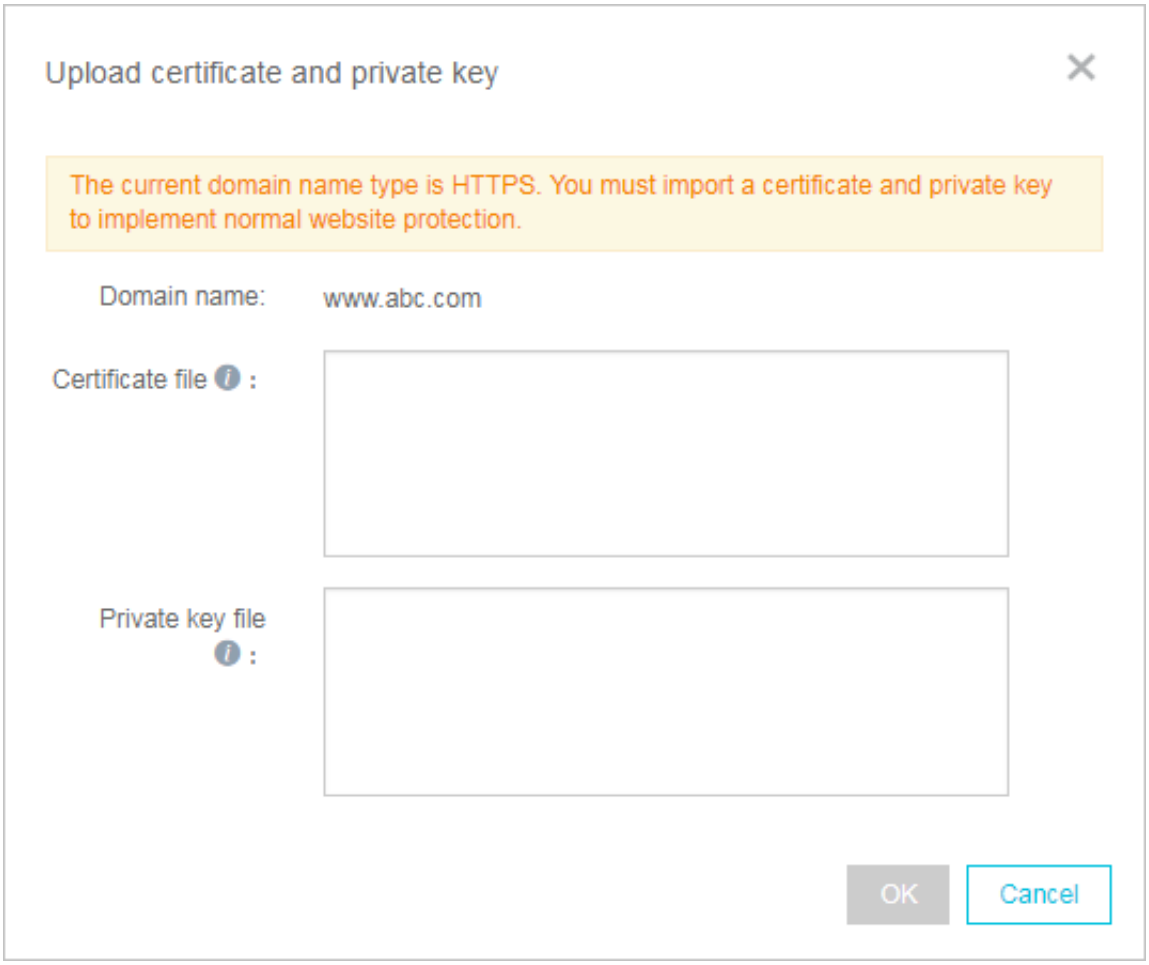
2. After an HTTPS website domain name is added, you can find it on the list of added domain names. Click **Certificate Update**, as shown in *Figure 7-3: HTTPS domain name certificate update*.

Figure 7-3: HTTPS domain name certificate update



3. Upload server certificate files and private key files, as shown in *Figure 7-4: Upload certificates and private keys*.

Figure 7-4: Upload certificates and private keys



Note:

You can simply copy and paste the content of the certificate and private key file in the appropriate text box. Certificates in common formats, such as PEM, CER, and CRT, can be directly opened in a text editor to copy the their contents. Certificates in other formats (such as PFX and P7B) must first be converted to PEM, CER, or CRT format. If there are multiple certificate files (such as a certificate chain), you can splice and upload them together.

- Below is an example of a recognizable certificate format:

```
-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2X
bahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2 cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8P
Ukl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc 65Cgb4mL+n5+DV9uOyTZTW
/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKk vRWvIAqYxX
```

```
Z7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE
-----
```

- Below is an example of a recognizable private key format:

```
-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn
2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQ Cr+ujntC1kN6pGBj2Fw2l
/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYo aMF2EjRwc0
qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----
```

7.1.2.4 Allow access from a WAF back-to-source IP address

Context

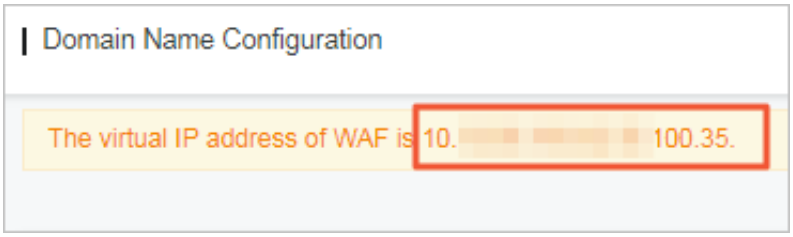
Back-to-source IP addresses are the source IP addresses used when WAF acts as a proxy for client requests. From the perspective of origin site servers, when connected to WAF, all access source IP addresses are changed to WAF back-to-source IP addresses, with the real client addresses added in the XFF field of the HTTP header.

After a domain name is connected to WAF, you must ensure that the origin site servers allow access by WAF back-to-source IP addresses. That is, these IP addresses must be added to the whitelist. Otherwise, the website may become inaccessible or load extremely slowly.

Procedure

1. Log on to the WAF console and click **Domain Name Configuration**. Then, view the WAF back-to-source IP addresses on the top of the page, as shown in *Figure 7-5: WAF back-to-source IP addresses*.

   Figure 7-5: WAF back-to-source IP addresses

2. Add the WAF back-to-source IP address to the whitelist for the security group containing the origin site server.

7.1.2.5 Local domain name WAF access configuration verification

Context

Before you switch your business traffic to WAF, we recommend you first perform local verification to ensure the configuration is correct and WAF forwarding works properly.

Procedure

1. First, modify the local hosts file so that local requests to the protected website are first directed to WAF. Here, we will use a Windows system as an example. The hosts file is usually located at "C:\Windows\System32\drivers\etc\hosts". Open the file in Notepad, Notepad++, or another text editor and add the following to the last line:

   `<WAF back-to-origin IP address> <Protected domain name>`

   Using the domain name www.aliyundemo.cn as an example, add the content to the hosts file.

   Note:
   The preceding IP address is the back-to-source IP address assigned by WAF.

2. After modifying the hosts file, send a ping to the protected domain name from your local device. The resolved IP address should be the WAF back-to-source IP address in the hosts file.

   Note:
   If the address is still resolved to the origin site address, you can try refreshing the local DNS cache.

3. After confirming that the address in the hosts file becomes effective, enter this domain name in your browser to access the website. If the WAF access configuration is correct, you can browse the site normally.
4. At the same time, you can use commands to simulate a simple web attack. For example, add "/?alert(xss)" at the end of the domain name URL to simulate a web attack request, such as www.aliyundemo.cn/?alert(xss). In this case, WAF displays the blocked page.

7.1.2.6 Modify DNS resolutions

Context

You can officially connect your business to WAF by redirecting its DNS resolution to WAF.

Note:
If your website domain name is not resolved by a DNS provider (for example, if your website uses a Server Load Balancer instance to connect to the Internet), you can perform the following procedure to modify the Server Load Balancer instance back-to-source IP address to the WAF back-to-source address, connecting your website to WAF for protection.

Procedure

1. Record the WAF back-to-source IP address assigned by WAF to the protected domain name.
2. Log on to the console provided by your DNS provider and find the domain name resolution settings for the relevant domain name. Then, change the A-recorded value to the WAF back-to-source IP address.

   Note:
   We generally recommend setting the domain name resolution TTL value to 600 seconds. The higher the TTL value, the longer it takes to sync and update DNS records.

7.1.3 Configure WAF protection functions

After connecting your domain names to WAF, you can configure detailed protection rules for them.

7.1.3.1 Configure web application attack protection

Context

Web application attack protection provides two modes, observation and interception:

- In observation mode, WAF alerts you to, but does not immediately block, suspected attacks, so you can evaluate the reports to detect false positives.
- In interception mode, WAF automatically blocks attack behavior.

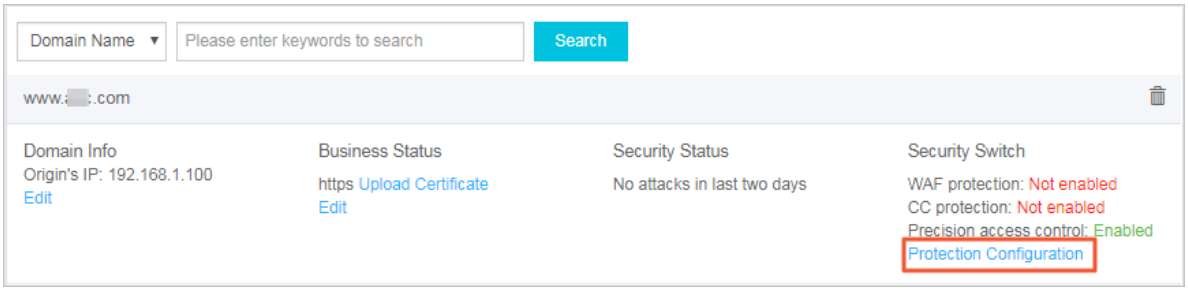
At the same time, WAF provides loose, normal, and strict protection policies:

- The default mode for protection rules is "normal".
- If you find that normal mode rules intercept many normal requests by mistake or your business has a relatively high amount of uncontrollable user input (such as rich text editors and technical forums), we recommend you select loose mode.
- If you need more rigorous protection rules to protect against path traversal, SQL injection, command execution, and other behavior, we suggest you select strict mode.

Procedure

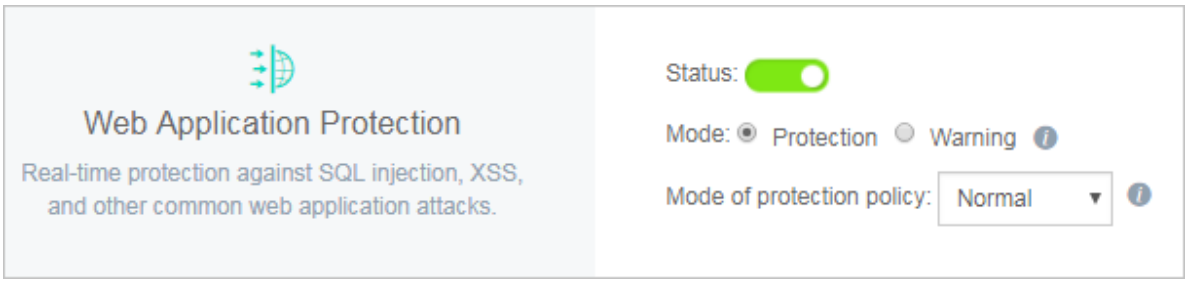
1. Log on to the WAF console and click **Domain Name Configuration**.
2. Select a protected domain name connected to WAF, and click **Protection Configuration**, as shown in *Figure 7-6: Domain name protection configuration*.

Figure 7-6: Domain name protection configuration



3. Find the web application attack protection options and select the appropriate protection mode and protection policy, as shown in *Figure 7-7: Web application attack protection options*.

Figure 7-7: Web application attack protection options



7.1.3.2 Configure malicious IP address penalties

Context

Almost all traditional web application firewall products use a combination of IP addresses and URLs to intercept traffic. After a request is determined to be an attack, the request is intercepted . In fact, attackers scan and attack your site each day. Hackers may stay up all night looking for vulnerabilities with your site, researching and attempting to bypass your protection policies.

To defend against these attacks, the Apsara Stack Security WAF provides a penalty mechanism for malicious IP addresses. When detecting that an IP address is launching sustained attacks, WAF can automatically mark and ban it as a malicious IP address.

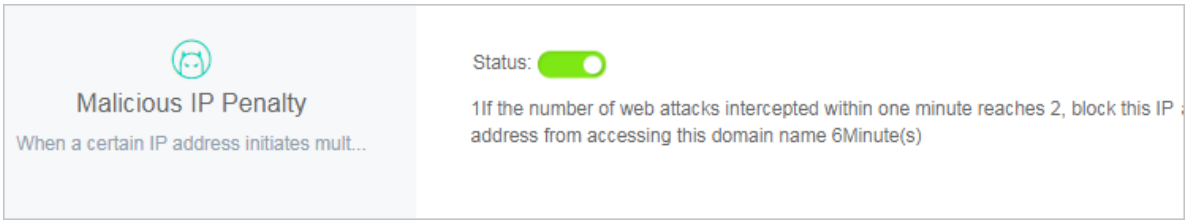
WAF uses the massive malicious IP address library accumulated by the Apsara Stack platform and its machine learning function to study and analyze the IP addresses used to launch attacks and their attack frequencies. This generates judgement rules automatically. When an IP address

is determined to be launching sustained attacks, WAF directly blocks all access requests from this IP address.

Procedure

1. Log on to the WAF console and click **Domain Name Configuration**.
2. Select a protected domain name connected to WAF and click **Protection Configuration**.
3. Locate the malicious IP address penalty option and click the Enable button next to the status bar to enable the malicious IP address penalty function, as shown in *Figure 7-8: Malicious IP address penalty option*.

Figure 7-8: Malicious IP address penalty option



7.1.3.3 Configure HTTP flood security protection

Context

WAF offers two HTTP flood protection modes, normal and attack emergency:

- The default HTTP flood security protection mode is "normal". In normal mode, there is a low likelihood of false positives, but the system only intercepts clearly abnormal requests.
- If you find that your domain name is under HTTP flood attack and the attack cannot be blocked in normal mode, you can select attack emergency mode. Attack emergency mode provides stronger HTTP flood attack blocking performance, but has a higher rate of false positives.

> **Note:**
> Attack emergency mode is only suitable for normal websites and HTML5 pages. It may produce a large number of false positives for APIs and native apps. If you need to configure HTTP flood attack protection for APIs or native apps, use custom HTTP flood attack protection rules.

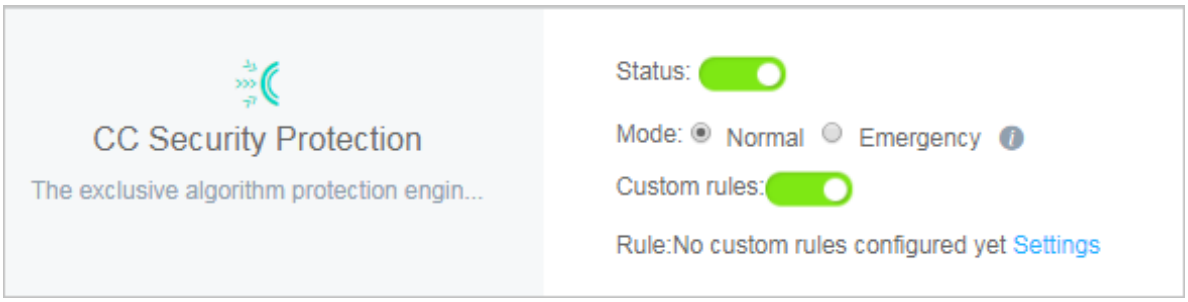
WAF also provides custom HTTP flood attack protection rules that allow you to set custom access frequency limits for specific URL paths in the console. For example, you can set a custom

protection rule that blocks an IP address for an hour if it is used to access the www.abc.com/login.html domain name more than 20 times in 10 seconds.

Procedure

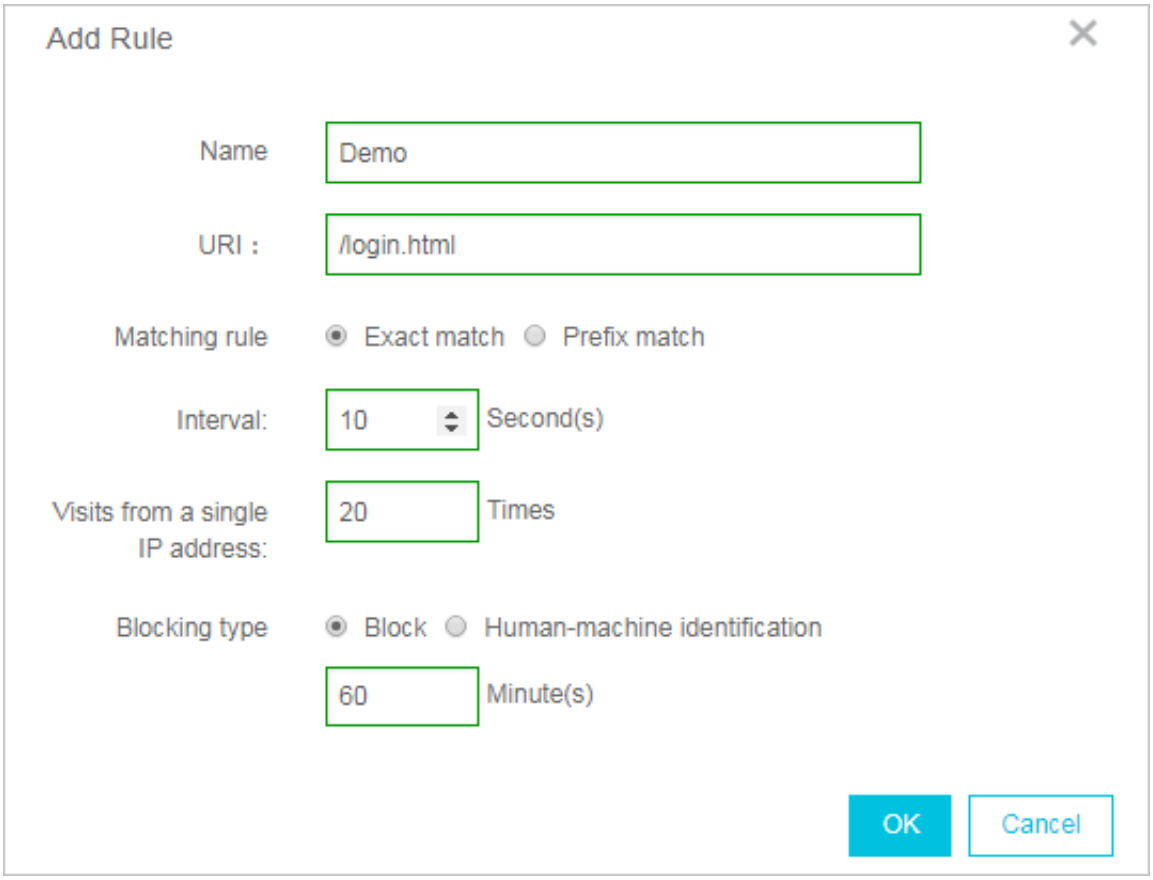
1. Log on to the WAF console and click **Domain Name Configuration**.
2. Select a protected domain name connected to WAF and click **Protection Configuration**.
3. Find the HTTP flood security protection function option and select the HTTP flood security protection mode, as shown in *Figure 7-9: CC security protection function option*.

   Figure 7-9: CC security protection function option

4. Click the Enable button next to the custom rule bar to enable custom HTTP flood security protection rules.
5. Click **Configure** to configure custom protection rules.
6. On the Custom CC Protection Rules page, click **Add Rule** to add a custom rule, as shown in *Figure 7-10: Add a custom rule*.

Figure 7-10: Add a custom rule



- **URI**: The specific URI address to be protected, as shown in `/register`. You can also enter parameters, as shown in `/user?action=login`.
- **Matching rules**:
  - Full match indicates an exact match is required. In this scenario, a request must completely match the configured URI for this rule to apply.
  - Prefix match is an includes-type match. The request's URI only needs to contain the configured URI address header for this rule to apply, as shown in `/register.html`.
- **Interval**: This is the period during which access attempts are counted and matched with the single IP address access count configuration.
- **Single IP address access count**: The number of visits from a single source IP address to the URL during the interval period.
- **Blocking type**:
  - Ban: After the rule is triggered, the connection is immediately closed.

  - Human/Machine identification: After the rule is triggered, the client is redirected to a human/machine identification test. Only verified requests are given access.
- **Blocking time**: The time during which the IP address is blocked.

7.1.3.4 Configure precision access control

Context

The precision access control function allows you to set access control rules using combinations of conditions for common HTTP fields (such as IP, URL, Referer, UA and parameters). This feature lets you customize protection policies for different business scenarios, such as anti-leech protection and website management background protection.

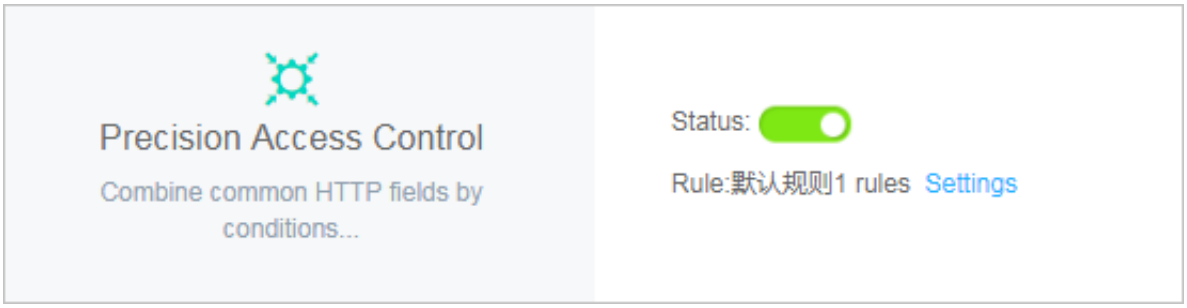
Before configuring precision access control rules, note the following:

- Each rule allows a combination of up to three conditions.
- The multiple conditions in a rule are connected by the logical relationship "AND", that is, a request must satisfy all the conditions to match the rule.
- You can take any of the following three actions when requests match the rule:
  - Block: Blocks the request.
  - Allow: After selecting this option, you can choose whether to apply web application attack or CC attack protection to such requests in the future.
  - Alert: The system records but does not block the request.
- Precision access control rule matching follows a specific order. You can adjust the order of the rules to achieve optimal protection performance.

Procedure

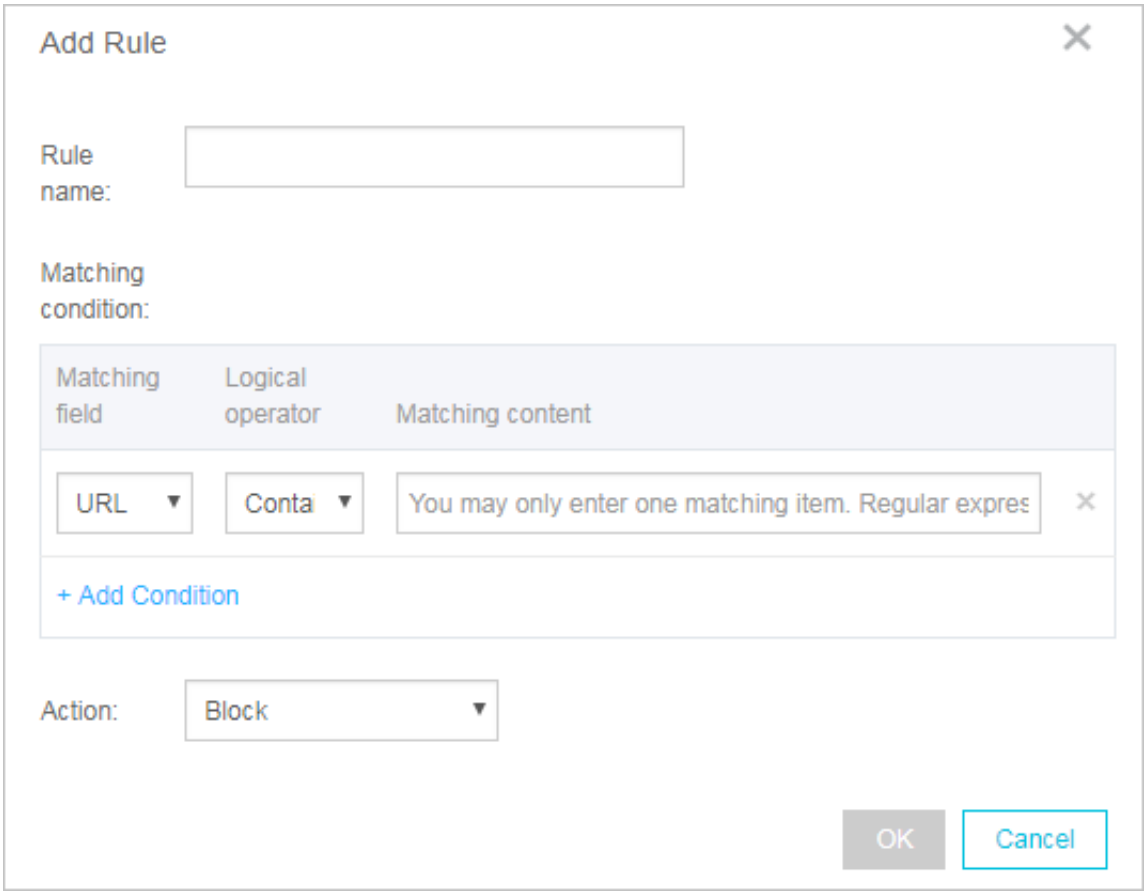
1. Log on to the WAF console and click **Domain Name Configuration**.
2. Select a protected domain name connected to WAF and click **Protection Configuration**.
3. Locate the precision access control function option and click the Enable button next to the status bar to enable the function, as shown in *Figure 7-11: Precision access control function option*.

Figure 7-11: Precision access control function option



4. Click **Configure** to configure precision access control rules.
5. Click **Add Rule**, as shown in *Figure 7-12: Add a precision access control rule*.

Figure 7-12: Add a precision access control rule



Note:

Precision access control rules support multiple matching fields and logical operators. You can set the rules according to your actual business needs.

6. On the Precision Access Control page, click **Sort Rules** to set the order of precision access control rules. Then, click **Save** to save the new order. The precision access control rules function matches requests with the rules following the order you have set.

7.1.3.5 Configure blocked regions

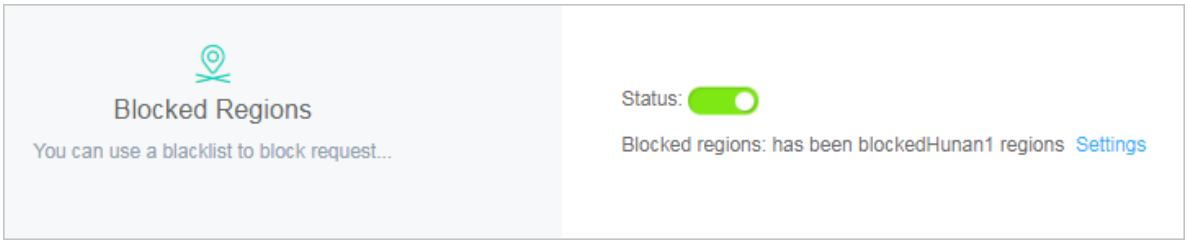
Context

WAF allows you to ban all source IP addresses from a specified region. Based on the IP address region information library, the block region function can ban IP addresses from specified Chinese provinces and foreign regions.

Procedure

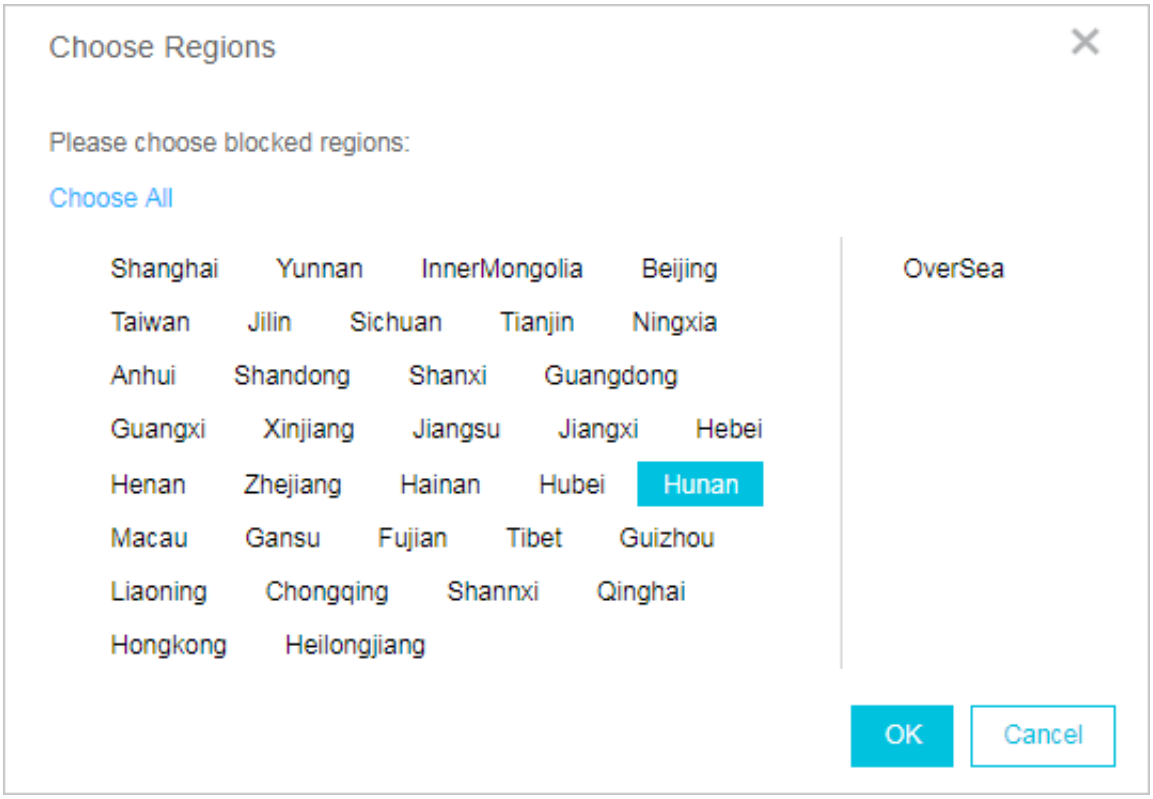
1. Log on to the WAF console and click **Domain Name Configuration**.
2. Select a protected domain name connected to WAF and click **Protection Configuration**.
3. Locate the block region function and click the Enable button next to the status bar to enable the function, as shown in *Figure 7-13: Block region function option*.

Figure 7-13: Block region function option



4. Click **Settings** to set blocked regions, as shown in *Figure 7-14: Set blocked regions*.

Figure 7-14: Set blocked regions



7.1.4 View WAF security reports

WAF provides various security reports that show the security statuses of protected domain names in real time.

7.1.4.1 View security overview

Context

The Security Overview page displays attack protection reports and web protection rule information.

- In the attack protection reports, you can view web and HTTP flood attack protection information and the number of attacks that have been prevented yesterday, today, or in the last 30 days. This helps you quickly understand the overall security status of your protected domain names. Click the View Details button in that upper-right corner of the report to view detailed attack protection information.
- In the message area, you can view real-time WAF protection rule update messages published by Alibaba Cloud.

- Log on to the WAF console and click **Security Overview** to view WAF attack protection information.

7.1.4.2 View security reports

Context

On the Security Reports page, you can view detailed protection information for the domain names protected by WAF.

- For web attacks, you can view the attack type distribution, attack source IP addresses, attack source regions, and detailed attack records.
- For HTTP flood attacks, you can view queries per second (QPS) information for servers, including total QPS, attack QPS information, and detailed records of malicious HTTP flood attack events.

Procedure

1. Log on to the WAF console and click **Security Reports**. Select a type, a protected domain name, and a query time range to view detailed WAF security reports.
2. In a web application security report, click **View Attack Details** to view attack event details and the triggered interception rules.

7.1.4.3 View business analysis

Prerequisites

The WAF business analysis function relies on MaxCompute (formerly ODPS) to perform data analysis. If you have not deployed MaxCompute in your Apsara Stack environment, you cannot use the business analysis function.

Context

The business analysis function incorporates WAF's attack interception information and access traffic information. It uses the big data engine to analyze access to the businesses on protected domain names. This allows you to immediately detect business vulnerabilities and improve your defensive capabilities.

- Log on to the WAF console and click **Business Analysis**. Select a domain name and query period and then click **Search** to view business analysis results.

  The Business Analysis page also provides an advanced search function, supporting fuzzy searches based on request fields, such as IP, URL, User-Agent, and Referer.

8 Cloud Server Protection

8.1 Protection baselines

The Server Guard protection status must remain in "online" status to provide stable and reliable intrusion protection and alerts for your hosts. Therefore, Apsara Stack Security provides the ability to query host protection status. This allows administrators to query Server Guard protection statuses, so they can see if the current status is "online" or the last time the status was "online".

8.1.1 Principles

The Server Guard clients and servers send messages over persistent TCP connection channels. As the core component of the Server Guard module, these channels provide up to 99.99% stability . The channels simulate SSL encryption and strictly ensure protocol handling over one channel does not affect other channels.

After the Server Guard client successfully establishes a connection and is logged on to the Server Guard server, this host's protection status changes to "online". Then, the Server Guard server regularly sends heartbeat detection requests to the client. If the client's connection is interrupted , the server updates its Server Guard protection status and records the last time the status was " online".

The Aegis-health-check project sends a security inspection command to the Linux or Windows system host through the Server Guard server. Then, the Server Guard server receives the inspection result returned by the client and forwards it to Aegis-health-check through the message center module to update the inspection result.

The protection baseline function supports repair, verification, or ignore operations based on the inspection results to improve host security. Its interface also displays the last 10 inspection records. Historical inspection records cannot be verified, ignored, or repaired, but can be rolled back. At the same time, you can view ignored inspection records and un-ignore them as needed.

8.1.2 View host protection status

Context

Host protection status can be online and offline. You can filter hosts by status and region, perform fuzzy queries by host IP address and host name, and refresh the host list.

By default, the hosts in all regions are displayed and sorted by IP addresses.

- Choose **Server Security** > **Host Protection** > **Protection Baselines**, set the query conditions, and click **Query** to view host protection status.

8.1.3 Immediately perform host security inspection

Procedure

1. If no security inspection has been performed on a host, select the host and click **View Details**.
2. Click **Inspect Now**.
3. In the **select inspection content** dialog box, select the items you want to inspect.
4. Click **OK** to send the security inspection command.

8.1.4 Perform host security inspection again

Procedure

1. If you need to reinspect the security of a host, select the host and click **View Details**.
2. Click **Reinspect**.
3. In the **select inspection content** dialog box, select the items you want to inspect.
4. Click **OK** to send the security reinspection command.

8.1.5 View host security inspection records

Procedure

1. After an inspection, select the host and click **View Details**.
2. Click **View Inspection Records** to view the last 10 inspection records.

Note:

Historical inspection results cannot be verified, ignored, or repaired, but can be rolled back.

8.1.6 View ignored inspection items

Procedure

1. After an inspection, select the host and click **View Details**.
2. Click **Ignored Items** to view items you have manually ignored. After un-ignoring an item, you can perform risk detection.

8.1.7 Process risk items

Procedure

1. After an inspection, select the host and click **View Details**.
2. Select the risk item to be processed and then choose **Repair**, **Verify**, or **Ignore**.

8.1.8 Offline issue troubleshooting

The troubleshooting process is follows:

- Check that there is a network connection.
- Check whether ACL rules have been set for the firewall. You must add the Server Guard server 's IP address to the whitelist in your firewall for access to the network (port 80).
- Check whether there are any third-party antivirus products. If any such product is found, disable it and reinstall the Server Guard agent. Some third-party antivirus software may prevent the Server Guard agent from accessing the network.

8.2 Logon security

Logon security detects remote logon and brute-force cracking. On the Apsara Stack Security Center, administrators can view alerts for remote logon and brute-force cracking, query logon records and brute-force cracking sources, handle records for remote logon and successful brute-force cracking, and mark the handled records to avoid alerts again.

8.2.1 Logon records

On the Configuration Center page, you can set frequent logon locations for servers. When logon attempts from unusual locations are discovered, the Apsara Stack Security Center generates alerts for the remote logon events. On the Alert Setup page, you can choose the way to send notifications, by text message or by email.

For information on setting frequent logon locations, see *Configure logon locations*.

Overview

1. The Server Guard client reports logon information to the Server Guard server through the TCP protocol.
2. The Server Guard server sends the report from the messaging module to the defender module.
3. The defender module analyzes the logon information, determines whether it is a remote logon event, and writes the result to Aegis-db. For a remote logon event, a message is sent to Situation Awareness, which determines whether or not to send a notification by text message and email.

8.2.2 Query logon records

Context

Logon records are available in the following states: remote logon, normal logon, and handled. You can fuzzy query logon records by host IP address and host name, and filter records by user and time.

By querying logon records, administrators can find and promptly troubleshoot the remote logon events discovered by Server Guard, and check for hacking activities.

Procedure

1. On the**Server Security** > **Host Protection** > **Logon Security**page, select **Logon Records**.
2. Set the query conditions.
3. Click **Search** to display the logon records that match the query conditions.
4. After confirming that a logon event is normal, you can click **Mark as Handled**.
5. In the displayed dialog box, click **OK**. This changes the event status to **Handled** and alerts for this record are no longer displayed on the console.

8.2.3 Brute-force cracking

On the Configuration Center page, you can set a logon whitelist. If a brute-force cracking attack succeeds while the source IP address is not in the whitelist, an alert is shown on the Apsara Stack Security Center console. On the Alert Setup page, you can choose the way to send notifications, by text message or by email.

For information on setting a whitelist, see *Configure the whitelist*.

Process analysis

1. The Server Guard client monitors host logon records. If any brute-force cracking event is detected, the client reports the event to the Server Guard server through the TCP protocol.
2. The Server Guard server sends the report from the messaging module to the defender module.
3. The defender module analyzes the brute-force cracking information, determines the attack type and result, and writes the event information to Aegis-db. For a successful brute-force cracking attack, a message is sent to Situation Awareness, which determines whether or not to send a notification by text message and email.

Brute-force cracking event types

The main types of brute-force cracking events are successful, threat, no threat, and handled. For a description of each event type, see *Table 8-1: Brute-force cracking event type table*.

Table 8-1: Brute-force cracking event type table

Event type	Description
Successful	The brute-force cracking attack was successful
Threat	Cracking was attempted many times
No threat	Cracking was attempted few times
Handled	The successful cracking event has been resolved

8.2.4 Query brute-force cracking events

Context

By querying brute-force cracking events, you can view the sources of the attacks, the attack count , and interception status. When the console displays a 'successful brute-force cracking attack' message, this means a hacker has cracked the password of your host and successfully logged on . In this case, the administrator must promptly troubleshoot the problem.

You can fuzzy query brute-force cracking events by host IP address and host name, and filter events by user and time.

Procedure

1. On the**Server Security** > **Host Protection** > **Logon Security**page, select **Brute-force Cracking**. Then, set the query conditions and click **Search** to view brute-force cracking events.
2. Investigate the cause of the event and eliminate any risks. Then, click **Mark as Handled**. In the displayed dialog box, click **OK** to change the event status to **Handled**.

8.3 Trojan scan

A Trojan file is usually stored in the web server directory, just like the normal files, accessed through a web browser, and used in the control of the website server. The Trojan scan function promptly detects Trojan files and alerts the administrators. In the Apsara Stack Security Center , administrators can view found Trojan files and perform necessary operations, for example, to quarantine files, to ignore threads, to restore quarantined file, and to remove trusted files. If you

have set to send notifications by text message or by email, a notification is sent only if a Trojan file is detected for the first time. For information on setting notifications, see Alert Setup.

8.3.1 Operation instructions

Note:
After a trusted file is removed, this alert is deleted and subsequent scans will report this Trojan information again.

Table 8-2: Description of Trojan file operations

Operation	Description	Status before operation	Status after operation
Ignore	After a Trojan is ignored, scans will no longer report it	Pending	Trusted file
Restore	Downloads the Trojan file from the FTP server to the local device	Quarantined	Trusted file
Remove trusted file	After removing a trusted file, scans will continue to report the risk	Trusted file	No data
Quarantine	Deletes the local Trojan file and uploads the Trojan to the FTP server for quarantine	Pending	Quarantined/No action needed

8.3.2 Status description

Table 8-3: Description of Trojan event status

Status	Description
Pending	This is a hazardous Trojan file.
Quarantined	This Trojan has been detected and eliminated.
Trusted file	This file has been inspected and found to be safe.
No action needed	This Trojan no longer exists when being quarantined.

8.3.3 Query Trojan file information

Context

The Trojan scan function classifies the found Trojans files into "Pending", "Quarantined", or " Trusted" status. You can perform a fuzzy query of detected Trojans files by host names or by host IP addresses. You can also filter the results by time period. The Trojan event list can be sorted according to degree of urgency, or be grouped by server.

By querying Trojan events, you can view information about the Trojan files discovered by Server Guard.

Procedure

1. Go to the**Server Security** > **Host Protection** > **Trojan Scan**page, set the query conditions, and click **Query**.

   Sort by degree of urgency

   The Trojan files in the "Pending" status are displayed first, sorted in descending order of detection time.

   Group by server

   Servers are listed in descending order by the number of pending Trojan files.
2. In group by server display, click the **View Details** button for a server to view information for all the Trojans detected on this server. These Trojans are sorted by urgency and time of detection.
3. Click **Back to Trojan Scan** to return to the Trojan scan page and perform another query.

8.3.4 Handling trojan files

Context

Server Guard automatically isolates files that only contain trojans. When malicious code in embedded in the normal content of a file, the administrator must decide whether or not to isolate the malicious file.

You can perform isolation when preparing to delete a trojan file. You can perform the restore operation on isolated files wrongly identified as trojans. You can perform the ignore operation on non-trojan files, which will then be retained. For a trusted file, you can perform the remove trusted file operation to delete this record from the list.

- Isolate a trojan file

  On the**Server Security** > **Host Protection** > **Trojan Scan**page, click **Isolate** for an event awaiting processing to isolate this trojan file.
- Restore an isolated trojan file

On the**Server Security** > **Host Protection** > **Trojan Scan**page, click **Restore** for an event that has been isolated to restore the isolated file.

- Ignore a trojan file

  On the**Server Security** > **Host Protection** > **Trojan Scan**page, click **Ignore** for an event awaiting processing to ignore this trojan file.

- Remove a trusted file

  On the**Server Security** > **Host Protection** > **Trojan Scan**page, click **Ignore** for a trusted file event to remove this trusted file.

8.4 Patch management

Patch management allows you to promptly obtain the latest vulnerability alerts and corresponding patches. Then, the Server Guard service issues patch updates. Thus, vulnerabilities are quickly discovered and repaired. Patch management helps you solve many problems, such as the inability to promptly discover and fix vulnerabilities and the inability to update patches in batches.

8.4.1 Principles

Vulnerability detection principles

Through vulnerability scan and update issuance of the Server Guard clients installed on your ECS instances, the patch management feature is designed to scan for vulnerabilities randomly once a day. If vulnerabilities are discovered on your servers, they are reported to the **Patch Management** page.

Vulnerability repair principles

- **Web application vulnerabilities**

  Server Guard identifies the MD5 values of common web files with vulnerabilities and replaces the affected files to repair web vulnerabilities.

  Note:
  If you have already manually repaired vulnerabilities on your ECS instances, the MD5 values of the files may remain the same, so Server Guard will still indicate that your servers are affected by these vulnerabilities. In this situation, go to the **Patch Management** page and ignore these vulnerabilities.

- **Linux system software vulnerabilities**

Server Guard subscribes to the official CVE vulnerability source. It collects and identifies the version information for software installed on your servers to detect system software vulnerabilities. The system software vulnerability function detects Vim, Bind, OpenSSL, and other software vulnerabilities on your servers.

> **Note:**
> Currently, you cannot use the "One-key Repair" function for Linux system software vulnerabilities. Instead, try to use the repair commands provided by Server Guard to fix these vulnerabilities. After repairing a vulnerability, you can use the verification function provided by Server Guard to quickly verify that it has actually been repaired.

- **Windows system vulnerabilities**

  Server Guard subscribes to official Microsoft patch updates. If there is a major vulnerability update (such as the "SMB remote code execution vulnerability"), Server Guard provides you with automatic detection and repair functions.

8.4.2 View server vulnerabilities

Context

On the **Patch Management** page, use the following procedure to view vulnerabilities Server Guard has discovered on your servers:

Procedure

1. On the**Server Security** > **Host Protection** > **Patch Management**page, select a vulnerability type and the **Group by Server** sort method.
2. Select a server and click **View Details**.
3. Select a vulnerability and click on its name to view detailed information.

8.4.3 Process server vulnerabilities

Context

On the **Patch Management** page, use the following procedure to process vulnerabilities Server Guard has discovered on your servers:

Procedure

1. On the**Server Security** > **Host Protection** > **Patch Management**page, select the vulnerability type.

2. To process discovered server vulnerabilities:
   - Find the vulnerability to process and click **Repair Now** in its operations column to repair this vulnerability.

     Note:
     Currently, you cannot use the "One-key Repair" function for Linux system software vulnerabilities. Instead, click **Generate Repair Command** and use the repair command provided by Server Guard to repair a vulnerability. After repairing a vulnerability, you can use the verification function to quickly verify that it has actually been repaired.
   - Find the vulnerability to verify and click **Verify** in its operations column to verify if the vulnerability has been repaired or still exists.
   - Find the vulnerability to process and click **Ignore** in its operations column to ignore this vulnerability.

8.5 Configuration center

8.5.1 Overview

The Configuration Center page allows you to configure the following items:

- **Whitelist Setup**: The logon IP address whitelist is mainly used to filter brute-force cracking attempts and successful brute-force cracking events. If the access source IP address and target IP address are in the logon IP address whitelist, brute-force cracking is not reported.
- **Logon location setup**: Frequent logon locations are mainly used to identify remote logon events. If you do not set frequent logon locations, no logon attempts are considered remote logon attempts. If you set frequent logon locations, the first and fifth logon attempts from a location out of the whitelist are reported as remote logon attempts. Other logon attempts are considered as normal logon events. If a user logs on from a location six or more times, this location is automatically added as a frequent logon location and displayed in the whitelist.
- **Baseline detection setup**: This configuration allows you to set periodic automatic security inspection policies.

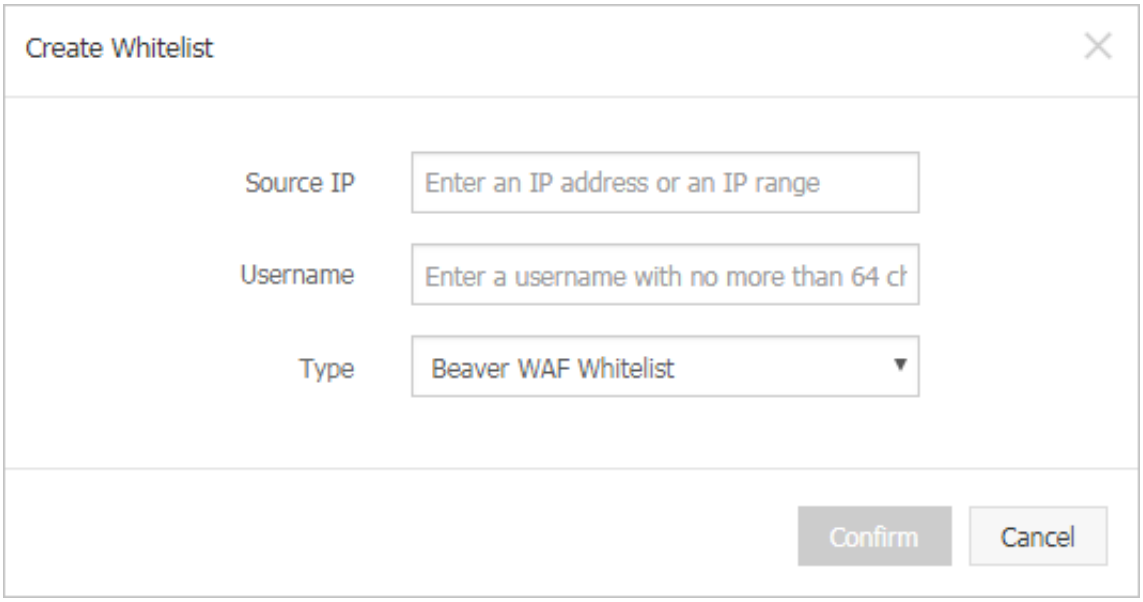
8.5.2 Configure the whitelist

Procedure

1. Choose**Server Security** > **Host Protection**, click **Configuration Center**, and then click **Whitelist Configuration** to go to the **Whitelist Setup** page.

2. Click **Add**.
3. In the **Add to Whitelist** dialog box, add the IP addresses, and click **OK**, as shown in *Figure 8-1: Add to Whitelist dialog box*.

Figure 8-1: Add to Whitelist dialog box



8.5.3 Configure logon locations

Procedure

1. Go to**Server Security** > **Host Protection** and click **Configuration Center** and then **Logon Location Settings** to display the **logon location settings** page.
2. Click **Add**.
3. In the **"add frequent logon location"** dialog box, set the frequent logon location to set and click **OK** to add the location.

8.5.4 Configure baseline detection policies

Procedure

1. Go to**Server Security** > **Host Protection** and click **Configuration Center** and then **Baseline Detection Settings** to display the **Baseline Detection Settings** page.
2. Click **Add**.
3. In the **security inspection policy** dialog box, set the required periodic security inspection policy and click **OK** to add this policy.

9 Physical Machine Protection

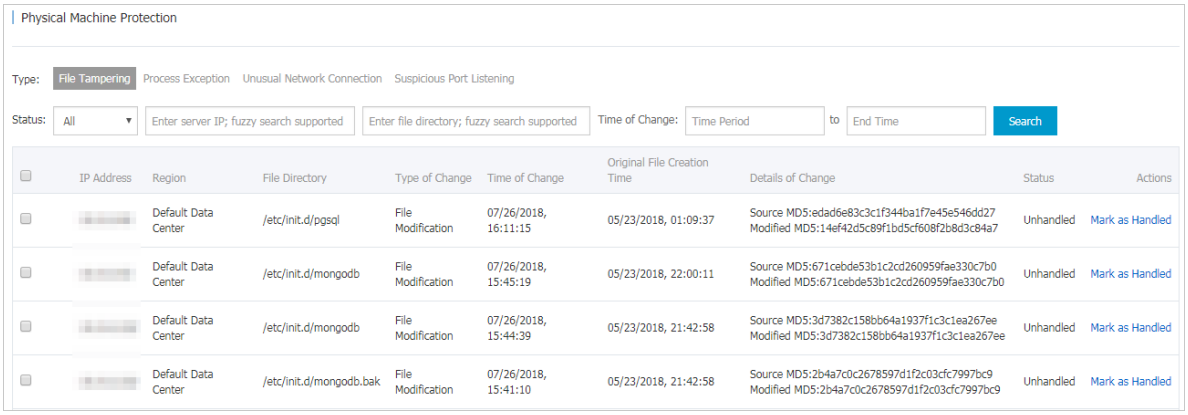
9.1 View and handle file tampering events

You can check the integrity of files in the specified directories on a host, detect file tampering in real time, and generate related alerts.

Procedure

1. Choose **Physical Machine Security** > **Physical Machine Protection**, and select **File Tampering**.
2. View file tampering events, as shown in *Figure 9-1: File tampering events*.

Figure 9-1: File tampering events



3. Handle a specified file tampering event.
   - If you have detected a file tampering event, take immediate security measures to protect the server, and further analyze the causes.
   - If an event is a normal event or an intrusion event that has already been handled, click **Mark as Handled**. In the dialog box that appears, click **Confirm** to change the event status to Handled.

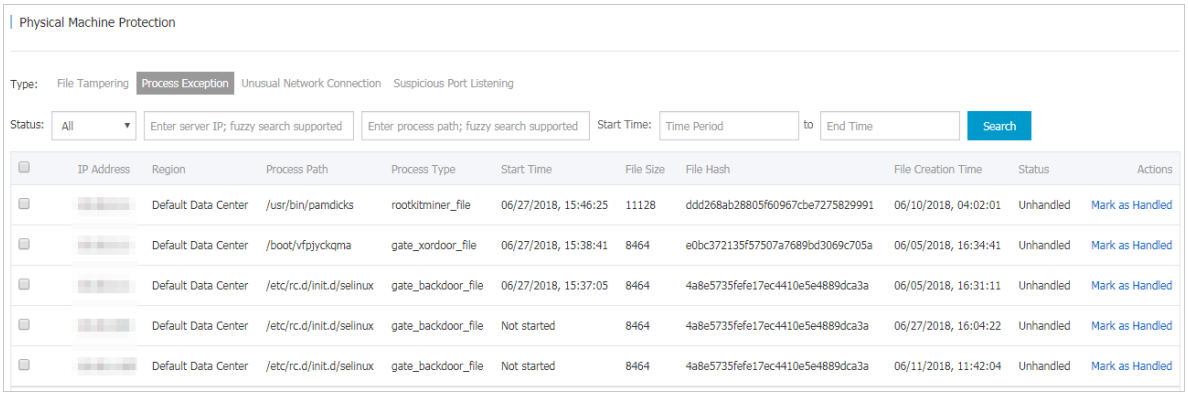
9.2 View and handle process exceptions

The system detects the startup of process exceptions in real time, and generates alerts.

Procedure

1. Choose **Physical Machine Security** > **Physical Machine Protection**, and select **Process Exception**.
2. View process exceptions, as shown in *Figure 9-2: Process Exception*.

Figure 9-2: Process Exception



3. Handle a specified process exception.
   - If you have detected a process exception, take immediate security measures to protect the server, and further analyze the causes.
   - If a process is a normal event or a process exception that has already been handled, click **Mark as Handled**. In the dialog box that appears, click **Confirm** to change the event status to Handled.

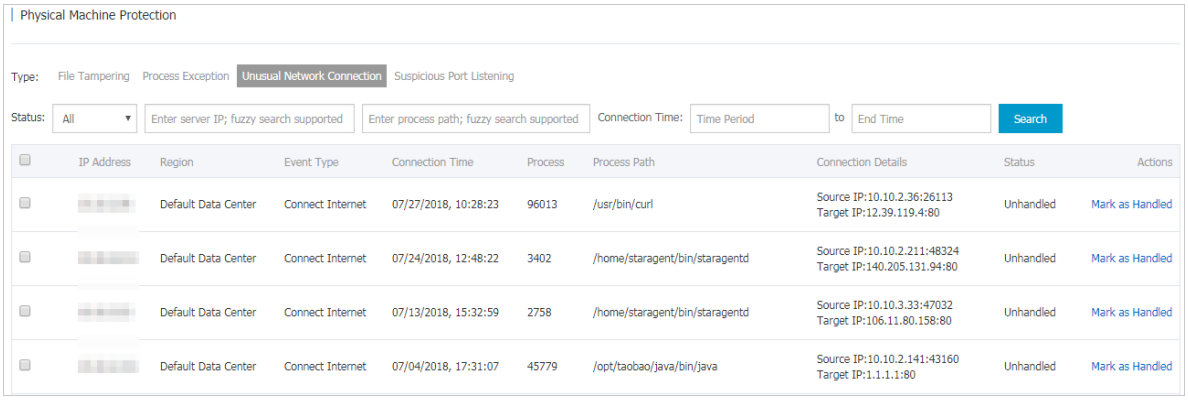
9.3 View and handle unusual network connections

The system detects active connections with external networks in time, and generates alerts accordingly.

Procedure

1. Choose **Physical Machine Security** > **Physical Machine Protection**, and select **Unusual Network Connection**.
2. View unusual network connection records, as shown in *Figure 9-3: Unusual Network Connection*.

Figure 9-3: Unusual Network Connection



3. Handle a specified unusual network connection.
   - If you have detected an unusual connection, take immediate security measures to protect the server, and further analyze the causes.
   - If a process is a normal connection or an unusual connection that has already been handled, click **Mark as Handled**. In the dialog box that appears, click **Confirm** to change the event status to Handled.

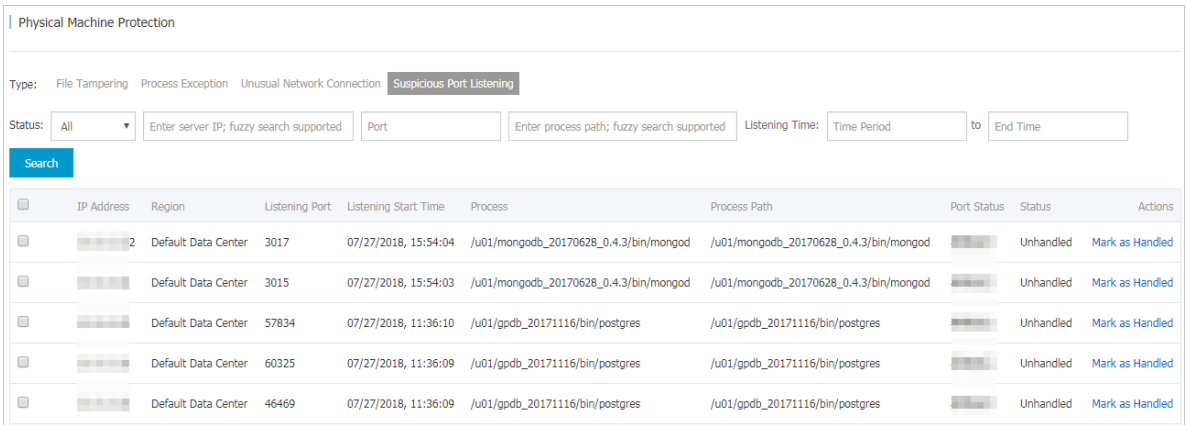
9.4 View and handle suspicious port listening events

The system detects new port listening events in real time, and generates alerts.

Procedure

1. Choose **Physical Machine Security** > **Physical Machine Protection**, and select **Suspicious Port Listening**.
2. View suspicious port listening events, as shown in *Figure 9-4: Suspicious Port Listening*.

Figure 9-4: Suspicious Port Listening



3. Handle a specified suspicious port listening event.
   - If you have detected a suspicious port listening event, take immediate security measures to protect the server, and further analyze the causes.
   - If a process is a normal port listening event or a suspicious port listening event that has already been handled, click **Mark as Handled**. In the dialog box that appears, click **Confirm** to change the event status to Handled.

10 Asset overview

Apsara Stack Security center presents your current total assets (classified as host assets and NAT assets) in charts, their increase/decrease frequency, regional distribution, and other statistical information. This allows administrators to query and view asset information by group or type, increasing their understanding of the asset situation for better asset management.

On the**Asset Management** > **Asset Overview**page, you can view an intuitive presentation of information on your overall asset situation, including total assets, new assets this month, group quantity, region quantity, asset reporting time distribution, asset group distribution, and asset region distribution. This allows you to better manage your assets. The interface is shown in *Figure 10-1: Asset Overview page*.

Figure 10-1: Asset Overview page

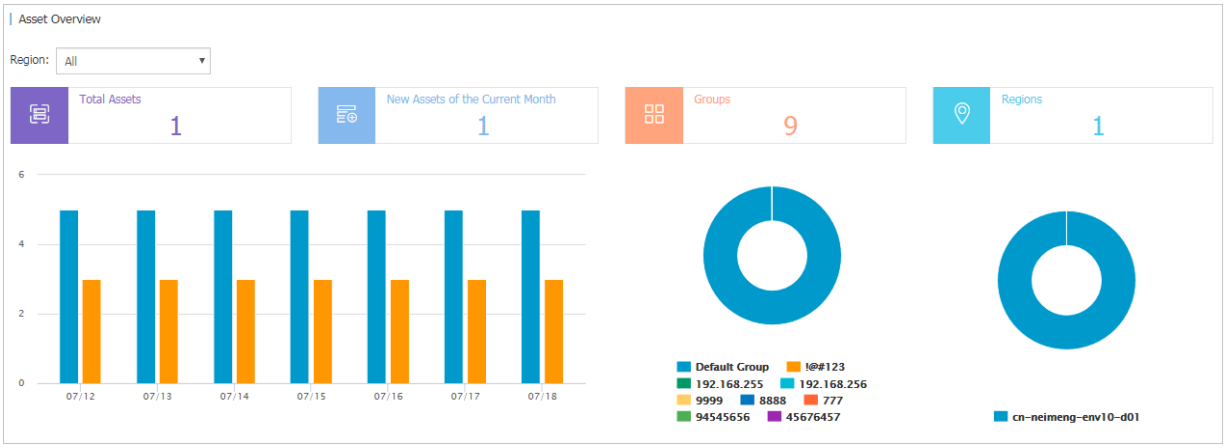


Table 10-1: Asset Overview page parameter descriptions

Parameter	Description
Group quantity	The current number of groups
Region quantity	The current number of configured regions
New assets this month	The total number of new assets created this month, including host assets and NAT assets
Asset group distribution	The chart shows the number of assets in each group as a share of the total number of assets.
Asset region distribution	The chart shows the number of assets in each region as a share of the total number of assets.

Parameter	Description
Total number of assets	The total number of assets reported by the Server Guard client, including host assets and NAT assets
Asset time distribution	The chart shows the changes in asset quantity by host asset and NAT asset over the past seven days.

10.1 Group management

Group management is mainly used to add, delete, and re-sort asset groups. Asset groups make it easier to distinguish different assets for specific purposes, query asset information, and modify asset information.

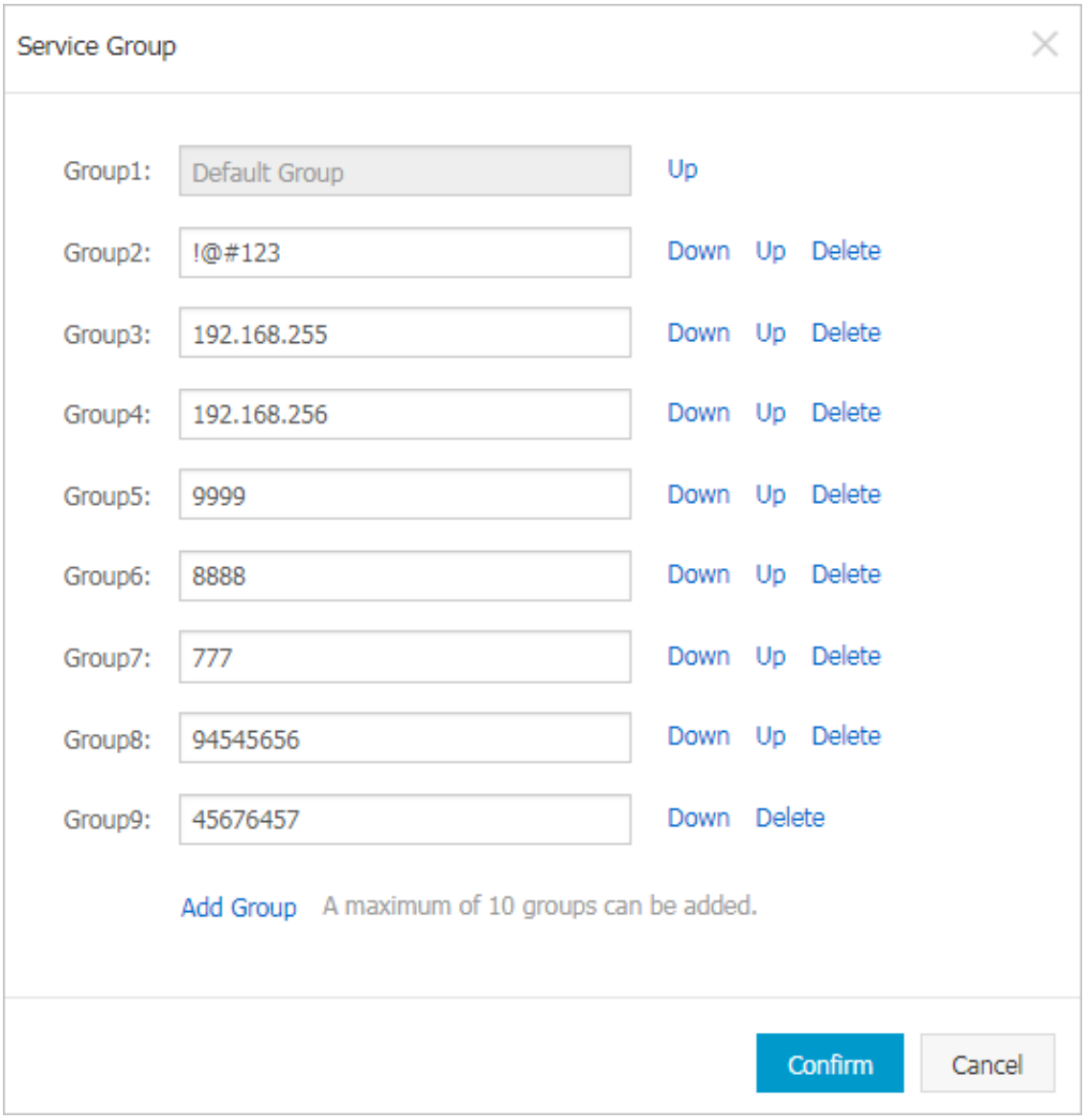
The system supports up to 10 asset groups. The default group cannot be deleted or renamed. Groups that currently contain assets cannot be deleted.

10.1.1 Add group

Procedure

1. On the**Asset Management** > **Asset Overview**page, click the **Group Management** button to display the **business group** dialog box, as shown in *Figure 10-2: Business group dialog box*.

Figure 10-2: Business group dialog box



2. Click the **Add Group** button.
3. Enter the group name.
4. Click **OK** to add the asset group.

10.1.2 Delete group

Procedure

1. In the **business group** dialog box, click the **Delete** button after a group.
2. Click **OK** to delete the asset group.

10.1.3 Adjust group order

Procedure

1. In the **business group dialog box** click **Move Up** or **Move Down** next to a group to change the group order.
2. Click **OK** to save the new group order.

10.2 Asset information

Assets are classified into Host assets and NAT assets. The two types of assets provide slightly different information and are managed slightly differently. You can switch between the interfaces for the two types of assets.

Table 10-2: Asset type table

Asset type	Description
Host assets	Server assets protected by Server Guard clients
NAT assets	IP address assets, whose intranet addresses undergo NAT conversion before being exposed on the Internet

10.2.1 Manage host assets

Host assets are mainly server assets. Once installed on a host and connected to the Server Guard server, the Server Guard client is reported as an asset.

Context

By querying host assets, you can view the overall situation of each asset, such as their operating systems, open ports, and installed software. You can also adjust the asset regions and groups.

Host asset queries support filtering by operating system, region, and group. You can fuzzy query assets by host IP address and host name. By default, the **Host Asset** page shows assets in all regions, which are sorted by IP address.

- On the**Asset Management** > **Asset Overview**page, select **Host Assets**, set the query conditions, and click **Query** to view host asset information.
- On the **Host Asset** page, click **Details** to view host open port information.
- On the **Host Asset** page, click **Expand Application Information** to view information on monitored applications installed on the host.

- On the **Host Asset** page, click **Modify** to display the **modify asset information** dialog box.

  Modify the information as needed and click **OK** to save the changes.
- On the **Host Asset** page, click **Delete** to display the deletion dialog box. Click **OK** to delete the asset.

  If you uninstall the Server Guard client from the host or delete an ECS instance from Apsara Stack, you need to manually delete the assets associated with the host.

10.2.2 Manage NAT assets

Context

NAT assets can be considered as IP address assets. These are IP address assets, whose intranet addresses undergo NAT conversion to allow access to the Internet. Thus, the IP address assets are exposed on the Internet. One of these IP addresses can be used by multiple hosts, with different ports directed to different hosts. When an IP address is configured as a NAT asset, the Situation Awareness module analyzes the asset to detect attack events.

By querying NAT assets, you can see basic information about the NAT assets currently under the protection of Apsara Stack Security. You can also modify groups and regions. You can add NAT assets one each time or in batches according to CIDR block.

You can query NAT assets by region and group. You can fuzzy query assets by host IP address. By default, the **NAT Asset** page shows assets in all regions, sorted by IP address.

Procedure

1. On the**Asset Management** > **Asset Overview**page, select **NAT Assets**.
2. Set the query conditions and click **Query** to view NAT assets.
3. On the **NAT Asset** page, click the **Add** button in the upper-right corner of the list to display the "add asset" dialog box. Enter an IP address or IP address expression, select the business and region, and click **OK** to add the asset.

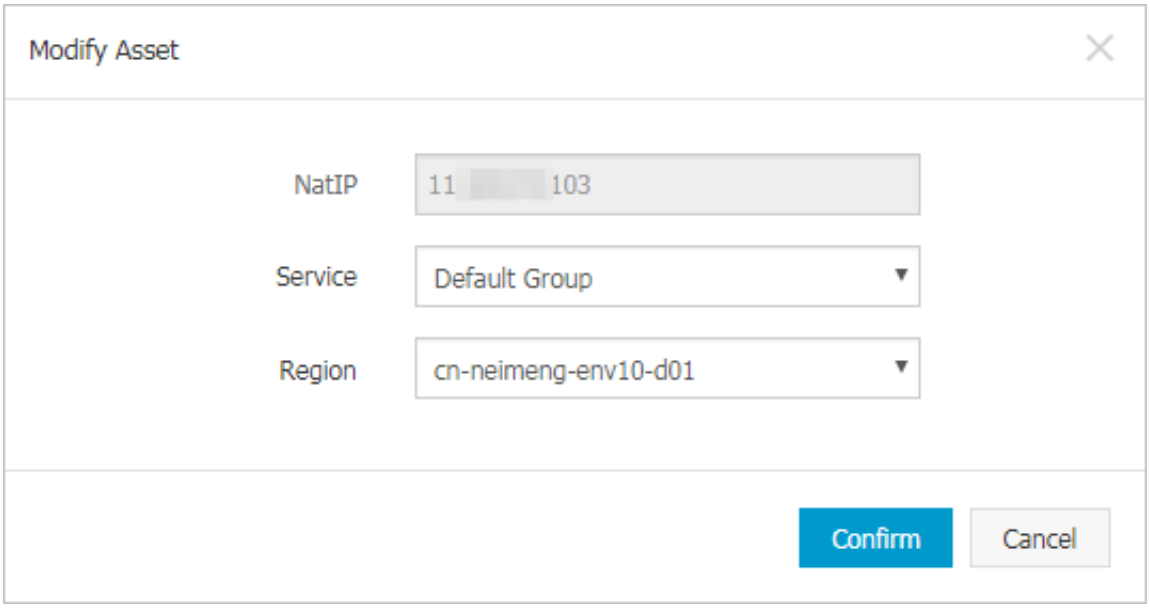
   The IP address of the asset you want to add must not conflict with an existing IP address. The NAT IP address must contain a legitimate IP address or CIDR block.
4. Select the required NAT asset to perform the following operations:

   - View details

     On the **NAT Asset** page, click **Details** to view open port information.
   - Modify a NAT asset

On the **NAT asset** page, click **Modify** to display the modification dialog box. Modify the information as needed and click **OK** to save the changes, as shown in *Figure 10-3: Modify asset information dialog box*.

Figure 10-3: Modify asset information dialog box



- Delete a NAT asset

  On the **NAT Asset** page, click **Delete** to display the deletion dialog box. Click **OK** to delete the asset.

10.2.3 Batch modify asset groups

Context

You can modify asset group information in two ways: individual modification and batch modification. Individual modification applies when you only need to modify the information of one host, or when you need to modify multiple hosts that do not share the same CIDR block and their names do not fit any pattern. See the preceding section for a detailed description of the individual asset modification method. Batch modification allows you to modify multiple host that belong to the same CIDR block.

Note:
The host IP addresses, host names, and operating systems/versions are fixed information that cannot be changed.

In addition, the system does not allow you to batch delete assets.

Procedure

1. On the**Asset Management** > **Asset Overview**page, click the **Modify Group** button to display the **modify group** dialog box.
2. You can batch modify CIDR block or host name information.
3. Click **OK** to save the changes.

11 Security audit

Security audit is a systematic, independent process of inspecting and verifying relevant activities or behaviors in a computer networking environment. It is followed by corresponding opinions from professional auditors entrusted by property owners and authorized by administrative authorities, based on relevant laws and regulations. Security audit can help a system administrator backtrack operations in the system.

Security audit is a long-term security management activity throughout the lifecycle of cloud services. The security audit feature of Apsara Stack Security can collect system security data, analyze weaknesses in system operations, report audit events, and classify audit events into high , moderate, and low risk levels. The security administrator views and analyzes audit events to continuously improve the system and ensure the security and reliability of cloud services.

11.1 Auditing overview

The **Auditing Overview** page provides four types of reports: cloud platform log trends, audit event trends, audit risk distributions, and hazardous event distributions. These four reports provide weekly statistics on log counts, event counts, event level distributions, and event type distributions, respectively. The data is presented in trend diagrams or pie charts so that administrators can easily analyze the trend of risks that cloud services are facing.

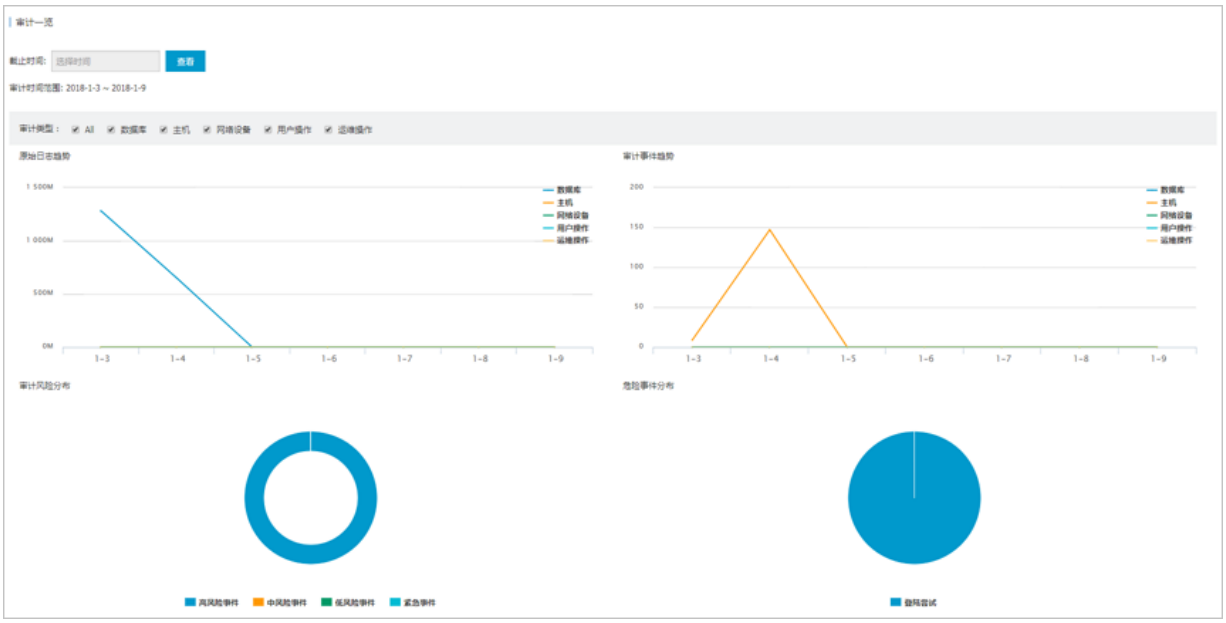
- The cloud platform log trend reports the number of logs generated by physical servers, network devices, RDS instances, ECS instances, and OpenAPIs in the last week. Accordingly, administrators can check whether the system generates a normal number of logs.
- The audit event trend reports the number of audit events generated by physical servers, network devices, RDS instances, ECS instances, and OpenAPIs in the last week. Accordingly, administrators can check whether the system generates a normal number of audit events.
- The audit risk distribution reports the numbers of high-risk, moderate-risk, and low-risk events that occurred in the last week. Accordingly, administrators can check whether the system generates a normal number of audit events of each level.
- The hazardous event distribution reports the proportions of different event types in the last week. Accordingly, administrators can get the types of audit events that occurred most frequently, identify high-risk events, and take preventive measures.

Choose**Security Audit** > **Auditing Overview**, set the query time, and click **Query** to view audit reports, as shown in *Figure 11-1: Auditing overview page*.

Note:

By default, weekly audit reports are displayed.

Figure 11-1: Auditing overview page



11.1.1 View audit overview

Procedure

1. Choose **Security Audit** > **Overview**. The **Overview** page is displayed.
2. Select **`End Time`** and click **View** to view auditing overview within one week before the end time.

   Note:

   `Audit Time Period` indicates the specific time range of the displayed audit logs.
3. Select or cancel a type in **`Audit Type`** to check whether to display the audit log for this type.

11.2 Audit queries

On the **Audit Query** page, you can view log creation times, log content, log types, event types, and risk levels. The log content is the debugging information from the log of the corresponding module.

Note:

For the meaning of the log content, contact the O&M staff.

Audit query generation process: The system matches the logs collected by the security audit module to the audit rules. If the log content matches any regular expression in the audit rules, it is reported as an audit event. You can go to**Security Audit** > **Policy Setup** > **Audit Policy**to view the default audit rules. You can also customize regular expressions in the audit rules.

Go to the**Security Audit** > **Audit Query**page and set the query conditions to find matching audit log records.

11.2.1 View audit events

Procedure

1. Choose **Security Audit** > **Audit Query** to view the **Audit Query** page.
2. Select **`Audit Type`**, **`Audit Target`**, **`Action Type`**, **`Risk Level`**, set the search time, and click **Search** to view audit events found in the time range.

   Note:
   Click **Advanced Search** to set more specific audit event filter conditions.
3. Click **Export** to export the searched audit events. For more information, see *Manage export tasks*.

11.3 Raw logs

On the **Raw Log** page, you can view the essential debugging information generated when applications are running. Based on this debugging information, administrators can identify system faults.

Choose **Security Audit** > **Raw Logs** to go to the **Raw Log** page. There, select an audit type and audit object, enter query keywords, and set the start time. Then, click **Query** to view raw log records.

11.3.1 View raw logs

Procedure

1. Choose **Security Audit** > **Raw Log**. The **Raw Log** page is displayed.
2. Select **`Audit Type`** and **`Audit Target`**, set the search time, and then click **Search** to view the raw log of a specific audit target within the specified time range.
3. Click **Export** to export the raw log. For more information, see *Manage export tasks*.

11.4 Policy settings

11.4.1 Manage audit policies

Audit policies are rules defined based on regular expressions. When a string in a log matches the regular expression of an audit rule, the system reports an audit event.

Context

Regular expressions describe a string matching mode and can be used to check whether a string contains a substring. The following table contains two examples:

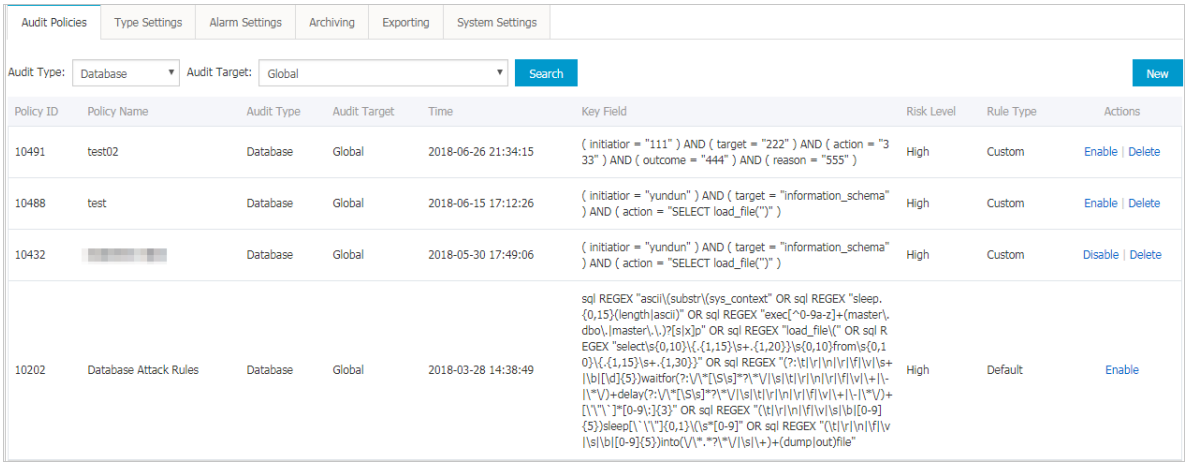
Regular expression	Description
`^\d{5,12}$`	Indicates that the fifth to the twelfth numbers are matched in the string.
`load_file\(`	Indicates that the string contains the “load_file(” substring.

The security audit module defines the default audit policy based on the string output in the log when an audit event is reported. The security administrator can also define the audit policy based on the string output in the log when the system encounters an attack.

Procedure

1. Choose **Security Audit** > **Policy Settings**, and select **Audit Policies**. The Audit Policy page is displayed, as shown in *Figure 11-2: Audit Policies*.

   Figure 11-2: Audit Policies



2. Specify the **Audit Type** and **Audit Target**, and click **Search** to view the current audit policy.

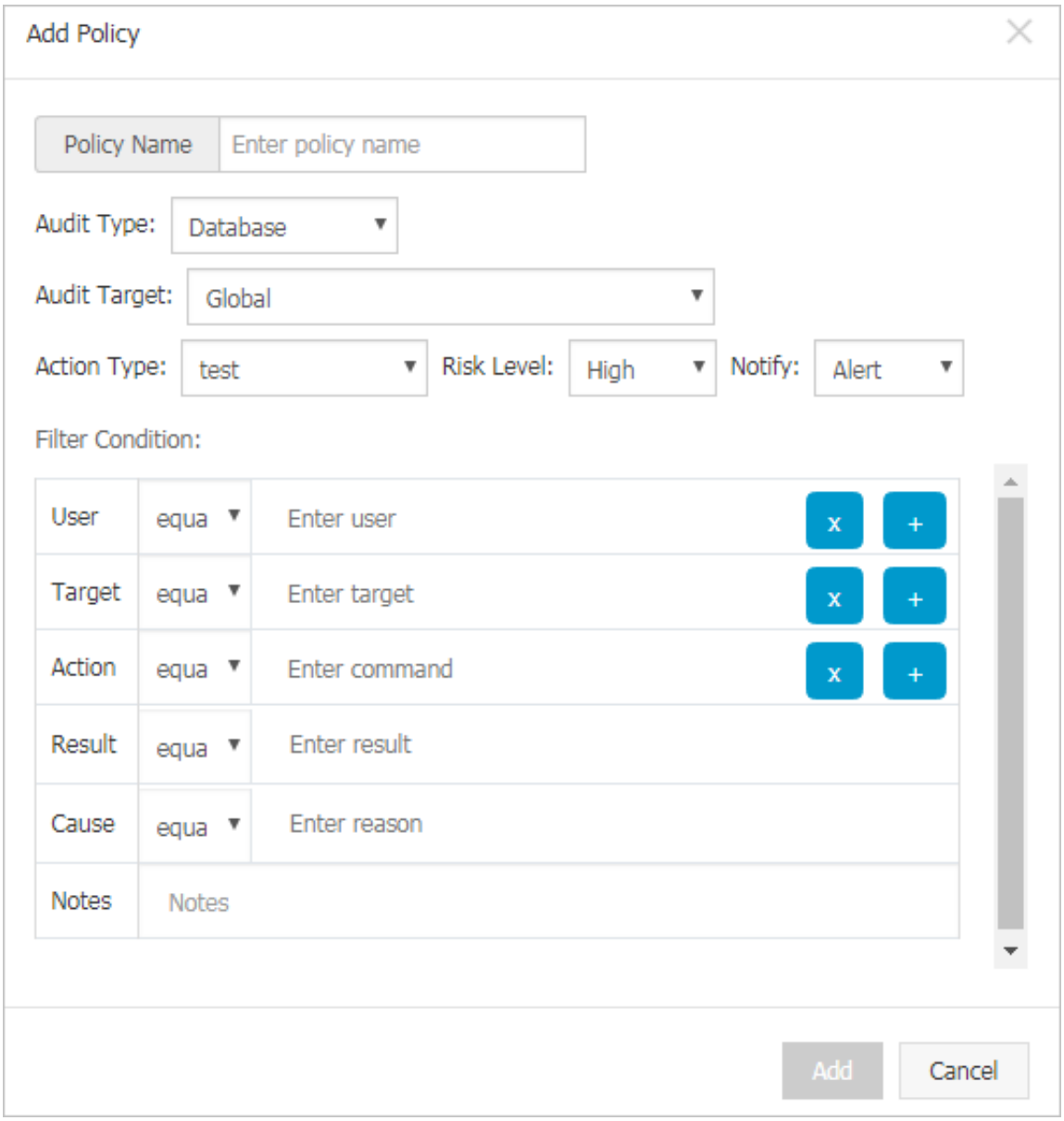
Note:

In **Audit Target**, select Global. The audit policies applicable to all audit targets of the audit type are displayed.

3. Manage audit policies.

   - Click **New**. In the **Add Policy** dialog box, enter relevant information and click **Add** to add an audit policy, as shown in *Figure 11-3: Add Policy*.

Figure 11-3: Add Policy



Note:

After an audit policy is added, if any string in audit logs of the specified audit type, audit target, and risk level matches the regular expression of an audit policy, an alert email is

sent to the specified recipient. For example, the regular expression *hi|hello* is added and the audit policy is set for ECS log types, logon attempt events, and high-risk events. If **hi** or **hello** appears in ECS logs, a logon attempt high-risk audit event is reported and an alert email is sent to the recipient.

- Click **Delete** to delete the audit policy.

  Note:
  The default audit policy of the system cannot be deleted.

- Click **Enable** or **Disable** to enable or disable an audit policy.

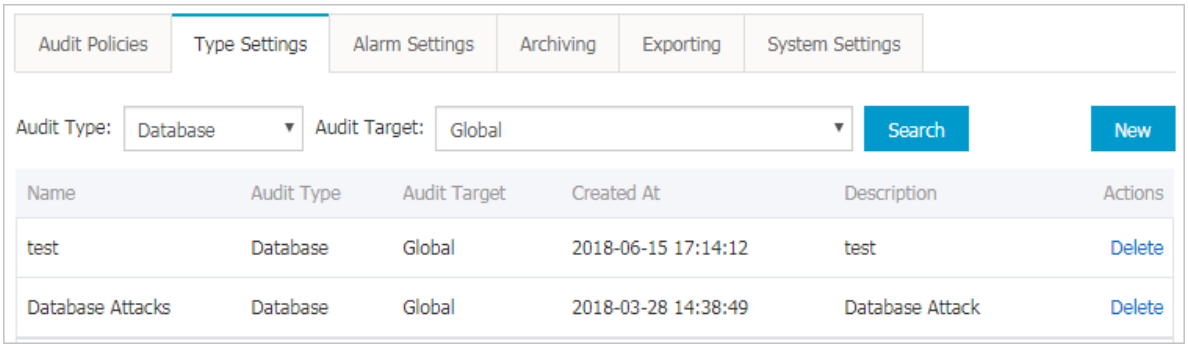
  Note:
  New audit policies are enabled by default.

11.4.2 Manage action types

Procedure

1. Choose **Security Audit** > **Policy Settings**, and select **Type Settings**. The Type Settings page is displayed, as shown in *Figure 11-4: Type Settings*.

   Figure 11-4: Type Settings

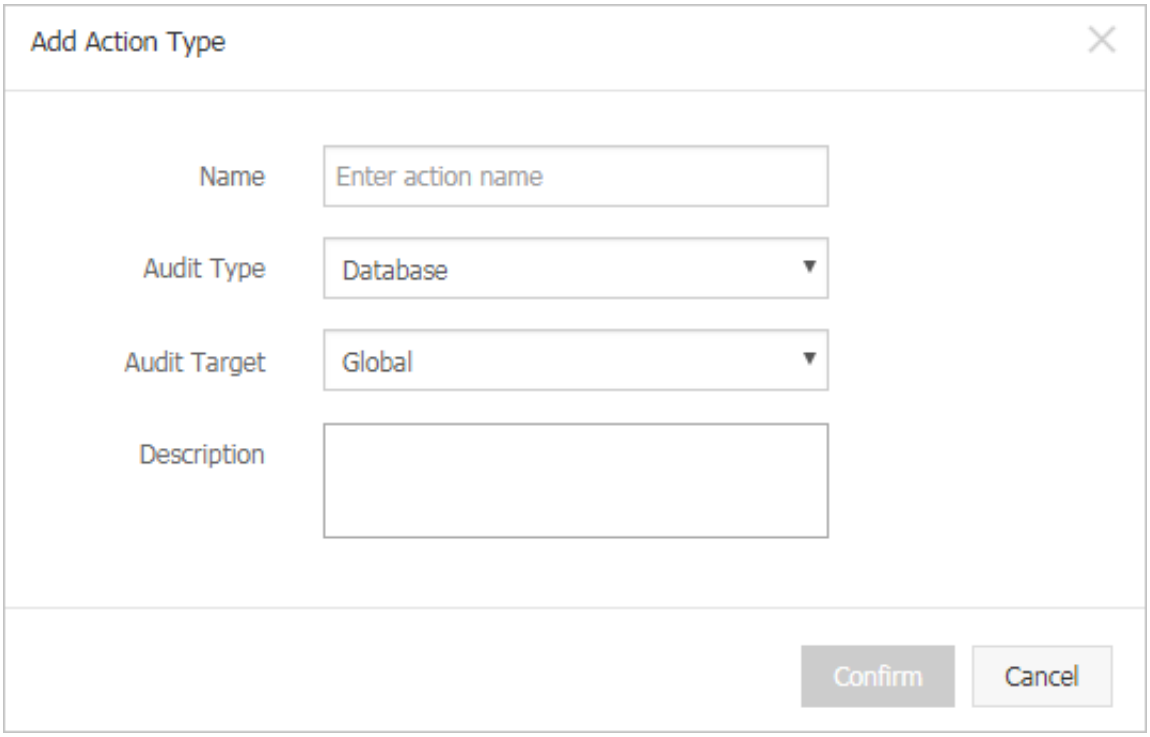
2. Select **Audit Type** and **Audit Target** and click **Search** to view the action type that is currently set.

   Note:
   In **Audit Target**, select **Global**. The action types applicable to all audit targets of the audit type are displayed.

3. Manage action types.

- Click **New**. In the **Add Action Type** dialog box, enter relevant information to add an action type, as shown in *Figure 11-5: Add Action Type*.

  Figure 11-5: Add Action Type



- Click **Delete** to delete the action type.

Note:
The default action types of the system cannot be deleted.

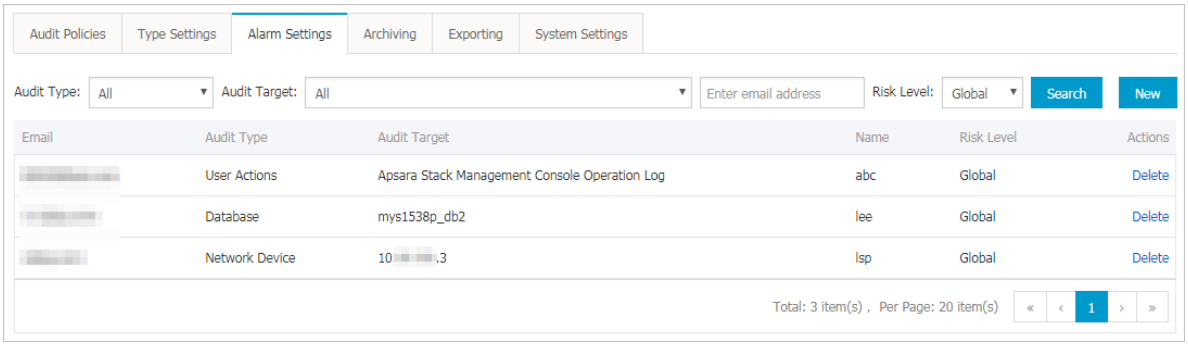
11.4.3 Set an alert receiver

Set the mailbox of the alert receiver. Once an audit event occurs, the event is reported to the mailbox of the alert receiver.

Procedure

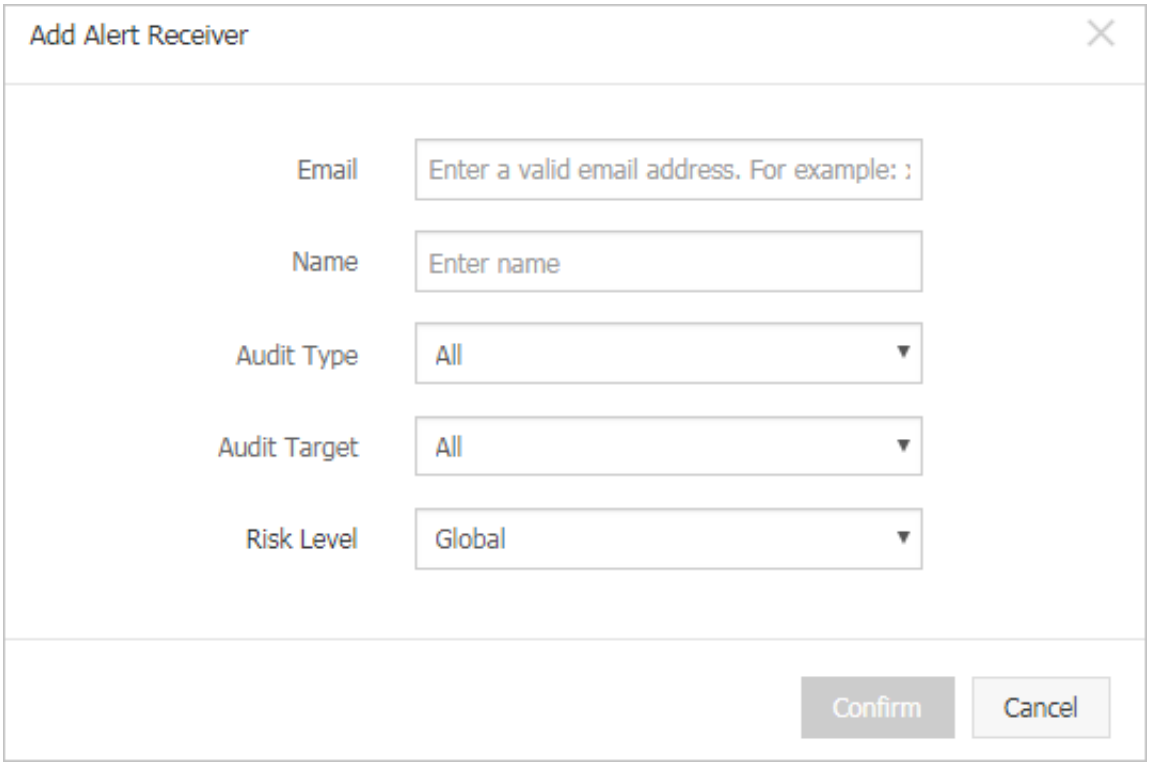
1. Choose **Security Audit** > **Policy Settings**, and select **Alarm Settings**. The **Alarm Settings** page is displayed, as shown in *Figure 11-6: Alarm Settings*.

Figure 11-6: Alarm Settings



2. Select **`Audit Type`**, **`Audit Target`**, and risk level and click **Search** to view the alert receiver that is currently set.
3. Set an alert receiver.
   - Click **New**. In the **Add Alert Receiver** dialog box, enter relevant information to add an alert receiver, as shown in *Figure 11-7: Add Alert Receiver*.

     Figure 11-7: Add Alert Receiver

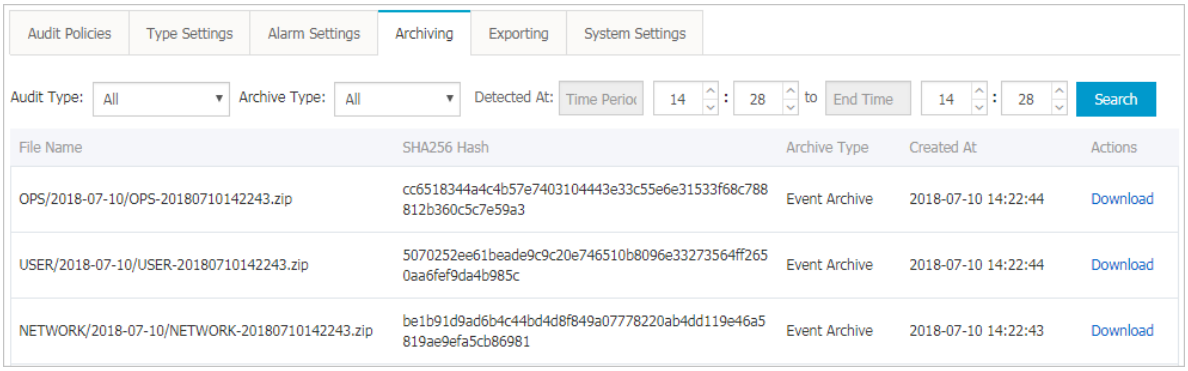
   - Click **Delete** to delete the alert receiver.

11.4.4 Manage event log archives

Procedure

1. Choose **Security Audit** > **Policy Settings**, and select **Archiving**. The Archiving page is displayed, as shown in *Figure 11-8: Archiving*.

   Figure 11-8: Archiving



2. Specify the **`Audit Type`** and **`Archive Type`**, set **`Detected At`**, and click **Search** to view archive information.
3. Click **Download** to download the archived file to a local computer.

11.4.5 Manage export tasks

On the **Audit Query** or **Raw Log** page, after exporting audit events or logs, you can manage export tasks on the Exporting page.

Procedure

1. Choose **Security Audit** > **Policy Settings**, and select **Exporting** to display the Exporting page.
2. View the export tasks that you have created.
3. After an export task is completed, select the task, and click **Download** in the operation bar to download audit event or log files to a local device.
4. Click **Delete** to delete an export task.

12 System management

As an essential part of Apsara Stack Security center, the system management module enables administrators to easily adjust system staff and configurations.

The system management module has four main parts:

- **User Management**: This is used to manage Alibaba Cloud Security accounts.
- **Intelligence Sync**: This is used to view the method and status of updating Apsara Stack Security intelligence database.
- **Alert Settings**: This is used to configure alert methods and contact information for various security events, emergency messages, and other alerts.
- **Global Settings**: This is used to configure Apsara Stack Security CIDR block information including traffic monitoring CIDR blocks and region CIDR blocks.

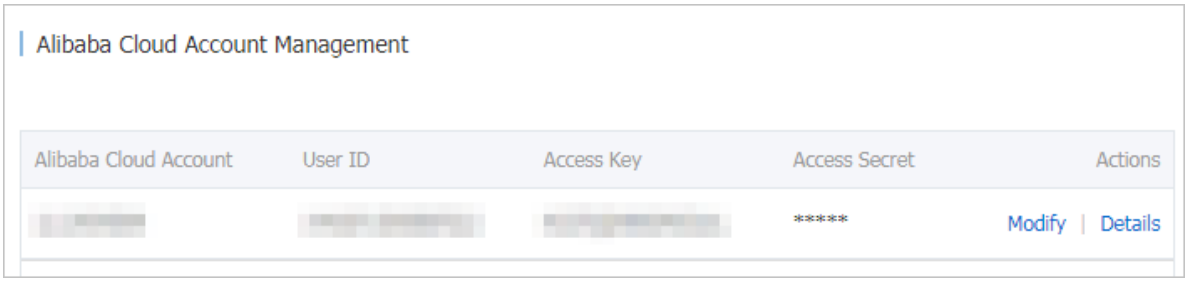
12.1 Manage Alibaba Cloud accounts

Procedure

1. Choose **System Management** > **Alibaba Cloud Account Management** to view and modify information about Alibaba Cloud accounts that are bound to the system, as shown in *Figure 12-1: Alibaba Cloud Account Management*.

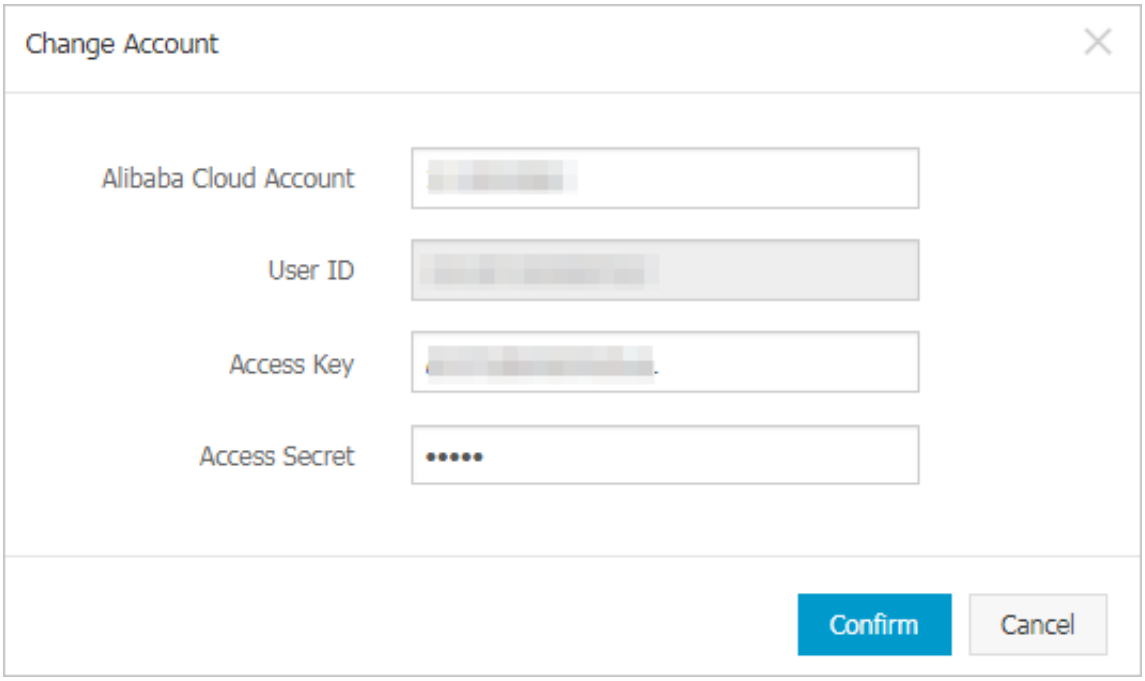
   In Apsara Stack Security, all assets are bound to Alibaba Cloud accounts. Be cautious when you modify information.

   Figure 12-1: Alibaba Cloud Account Management

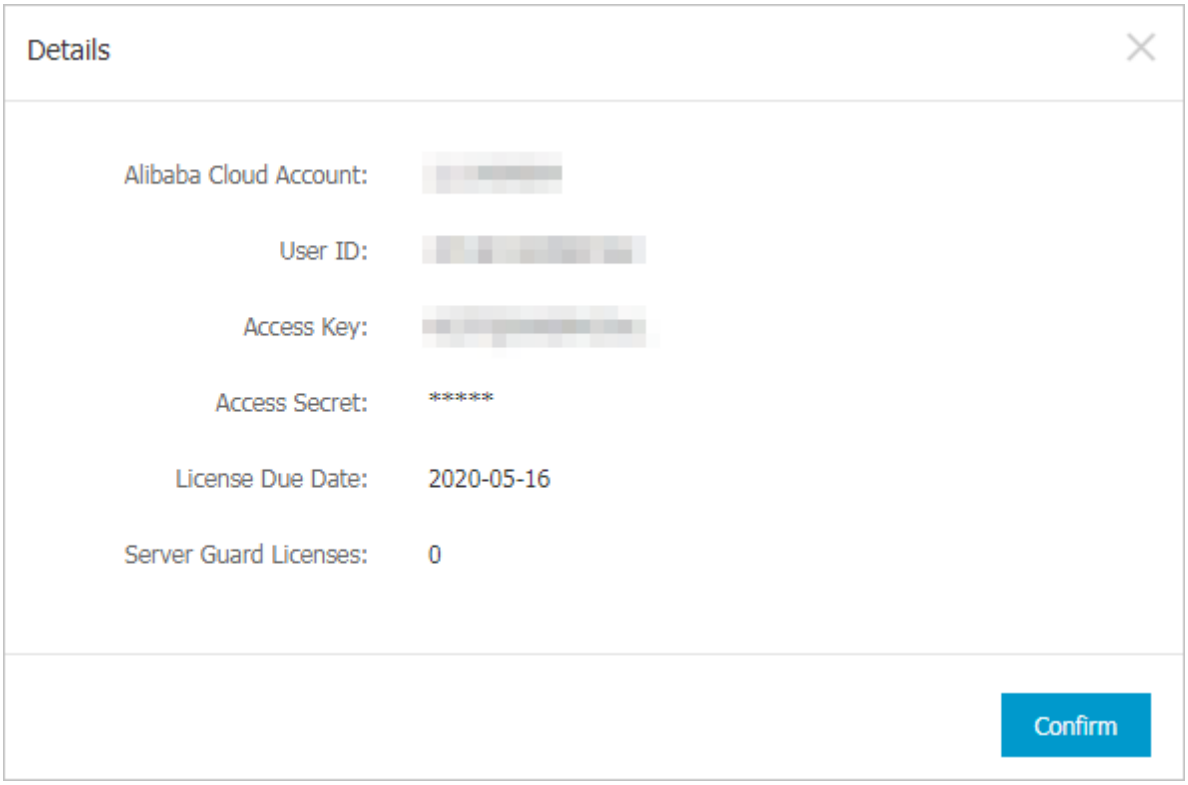
2. Click **Modify**. In the modification dialog box that appears, modify the information, and click **Confirm** to complete the modification, as shown in *Figure 12-2: Account modification dialog box*.

Figure 12-2: Account modification dialog box



3. Click **Details** to view details of an Alibaba Cloud account, including the license expiration date and number of Server Guard licenses, as shown in *Figure 12-3: Account details*. You can obtain the information using the user ID and AccessKey that you have configured.

Figure 12-3: Account details



12.2 Intelligence sync

Intelligence sync synchronizes the emergency response information library, staff account registration library, staff leak information library, staff information scan library, 0-day rule library, vulnerability analysis library, master vulnerability library, and industry news library on the Alibaba Cloud public cloud to your local database. The information synchronized from the emergency response information library, staff account registration library, staff leak information library, staff information scan library, 0-day rule library, vulnerability analysis library, master vulnerability library, and industry news library is displayed as Situation Awareness intelligence. This provides important security reference and intelligence information for your system. The 0-day rule library is used in big data model analysis. The data from this analysis is displayed as threats in Situation Awareness. This shows the security threats currently facing your system.

Intelligence is synced in two ways: information is pushed by the cloud or pulled by the client. For more information, see *Table 12-1: Intelligence sync methods*.

Table 12-1: Intelligence sync methods

	Cloud push solution	Client pull solution
Solution details	1. The local client registers its locally monitored ports and IP addresses on the cloud to subscribe to synced data. 2. After the initial connection, the cloud pushes all its data to the local client. 3. Afterwards, when informatio n is added or changed, it pushes incremental data to the client. 4. When the local client receives data, it must verify the version of the synced data. If the version is the same as its current version, it does not process the data. 5. The local client can initiate data sync requests. In such a case, the cloud pushes all data of the current version to the client. 6. After the data is synced to the local machine, it must be confirmed in Alibaba Cloud Security's security center before taking effect.	1. The first time the local client connects to and registers with the cloud, it pulls the data you are interested in. 2. Then, the local client regularly pulls data from the cloud. It first checks that the data versions are consistent. If the versions on the client and cloud are the same, the client does not pull the data. If not, the current data version is synced to the client. 3. By default, data is pulled once a day, but you can modify the frequency. 4. After the data is synced to the local machine, it must be confirmed in Apsara Stack Security's security center before taking effect.
Advantages	Data can be synced to the client in real time.	You can easily customize the data sync frequency.
Disadvanta ges	When there are frequent data updates or large data volumes and you need to simultaneo usly sync multiple clients, the sync operations are relatively complicated and will put a great burden on your system.	You cannot sync data in real time.
Conclusion	We recommend using the client pull method when you do not need highly real-time data.	

12.2.1 Sync status description

When data in the Intelligence Sync list is initialized, only the emergency response information library, staff account registration library, staff leak information library, staff information scan library , 0-day rule library, vulnerability analysis library, master vulnerability library, and industry news library on the Alibaba Cloud public cloud are synced to your local database. The sync frequency and time for each data type can be set by administrators and the operation can be triggered manually or automatically. If you do not set the frequency, the initial settings apply.

To buffer data, the data synced from the cloud is first synced to the buffer and then to the actual database. Therefore, the Intelligence Sync data statuses are: downloading, downloaded, installing , or installed.

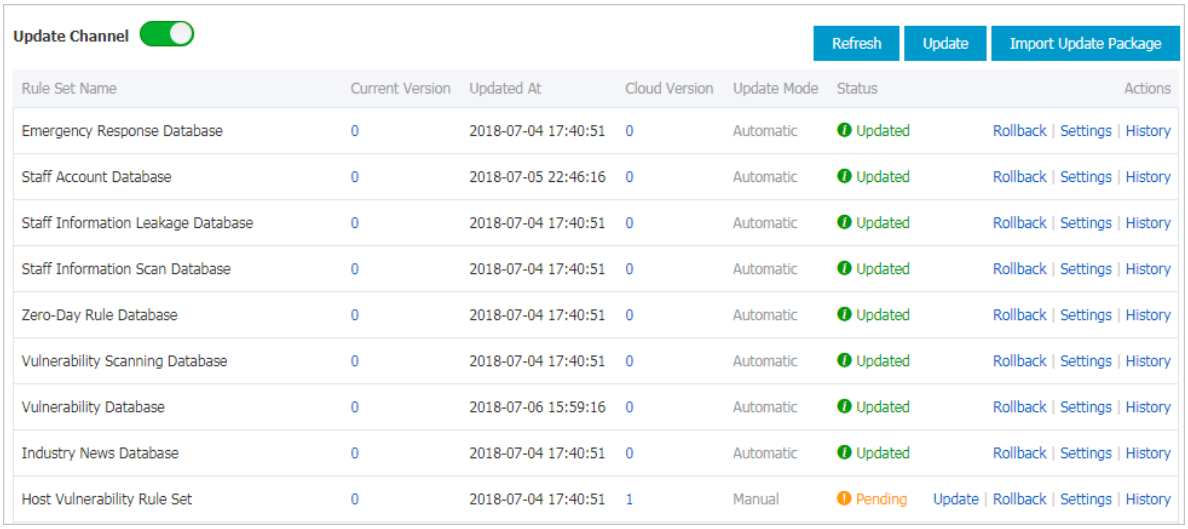
Table 12-2: Sync status descriptions

Status	Description
Downloading	The data is being downloaded from the cloud to the buffer.
Downloaded	The data has been downloaded from the cloud to the buffer.
Installing	The data is being downloaded from the buffer to your database.
Installed	The data has been downloaded from the buffer to your database.
Awaiting update	There is a new intelligence version on the cloud that you can download.

12.2.2 Update Intelligence Sync list

- On the**System Management** > **Intelligence Sync**page, click **Update** to refresh the Intelligence Sync list, as shown in *Figure 12-4: Intelligence Sync page*.

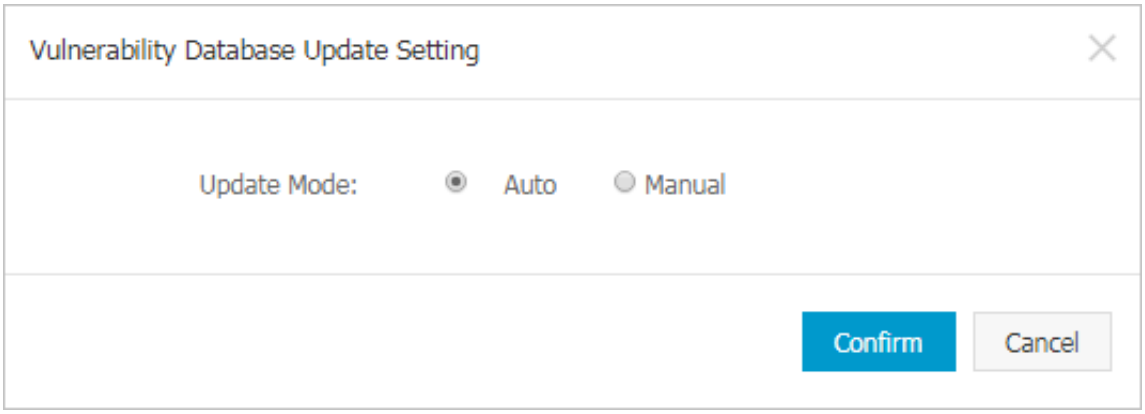
Figure 12-4: Intelligence Sync page



12.2.3 Check for intelligence updates

- On the**System Management** > **Intelligence Sync**page, click **Check for Updates** to check for new data versions on the cloud, indicating that you must update your intelligence data. If there is a new version, the status of the corresponding data type changes to **Awaiting Update**, as shown in *Figure 12-5: Check for intelligence updates*.

Figure 12-5: Check for intelligence updates



12.2.4 Update all intelligence

- On the**System Management** > **Intelligence Sync**page, click **Update All** to download all current intelligence data on the cloud to your database.

12.2.5 Check historical records

- By checking historical records, you can see the data sync records for a selected data type.

12.3 Alert settings

The alert settings feature allows you to set alert contacts and alert methods for different security events. When a security event occurs, the system automatically reports the event and sends an alert to keep the security administrator informed of system security events.

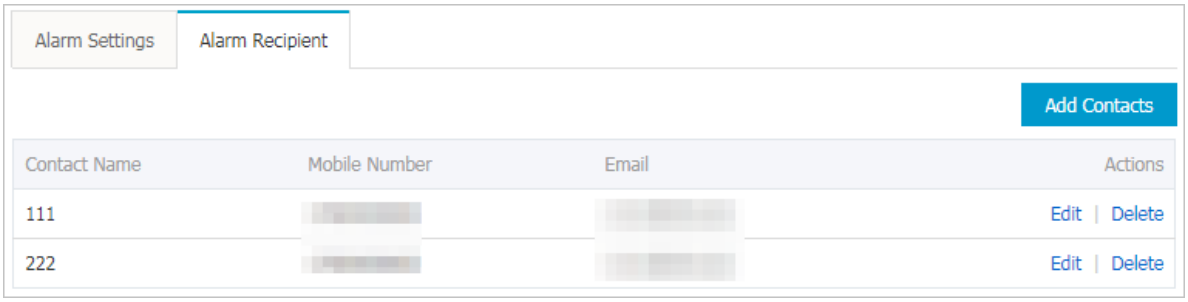
12.3.1 Set alert contacts

Alert contacts are receivers of alert messages. The system sends alert messages using SMS or emails. When the defined security event occurs, the system sends an alert message to the alert contact.

Procedure

1. Choose **System Management** > **Alert Settings** > **Alarm Recipient**, as shown in *Figure 12-6: Alarm Recipient page*.

   Figure 12-6: Alarm Recipient page

2. Click **Add Contacts**.
3. Enter the contact information and click **OK** to add an alert contact.

   After adding an alert contact, click **Edit** or **Delete** to edit or delete the contact information.

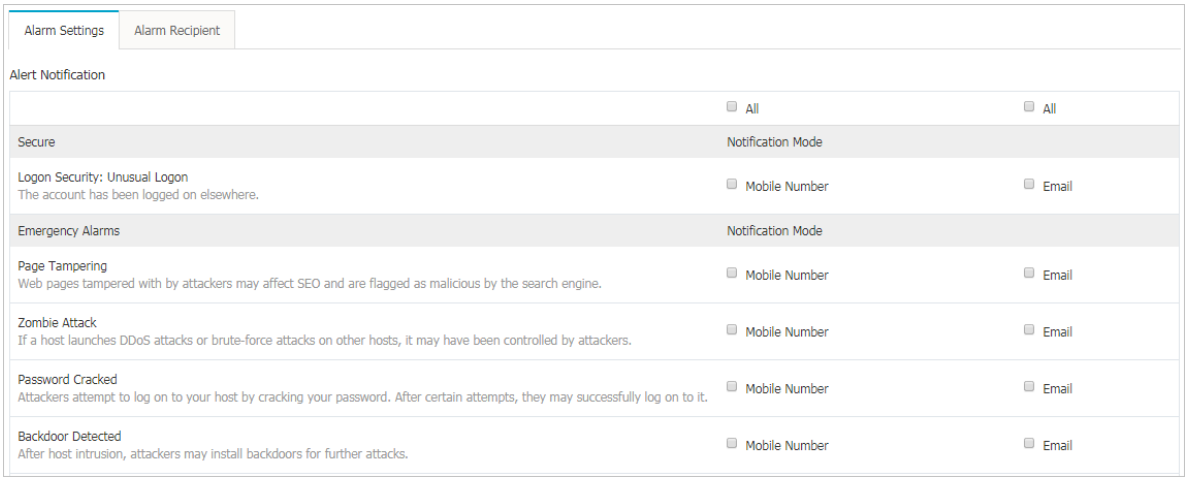
12.3.2 Set alert information

You can set alerts to indicate all security events using SMS and emails.

Procedure

1. Choose **System Management** > **Alert Settings** > **Alert Settings**.
2. In the **`Alert Notification`** area, select the alert notification method for different security events, as shown in *Figure 12-7: Alert Settings*.

Figure 12-7: Alert Settings



3. Click **Confirm** to complete settings.

12.4 Global settings

The Apsara Stack Security Center console provides global settings for the security administrator to set the CIDR block range of the traffic security monitoring module and the regions for reporting and detection by the Server Guard module.

Note:
If you set the same CIDR block for the collection CIDR block and the region of the traffic security monitoring module, the region information must be consistent.

12.4.1 Set CIDR blocks for traffic monitoring

The security administrator can configure CIDR blocks for the traffic security monitoring module, and change the monitored CIDR block range as needed. Settings of the monitored CIDR block only apply to data centers in the region.

Note:
Changes of CIDR blocks take effect immediately without further operations by the security administrator.

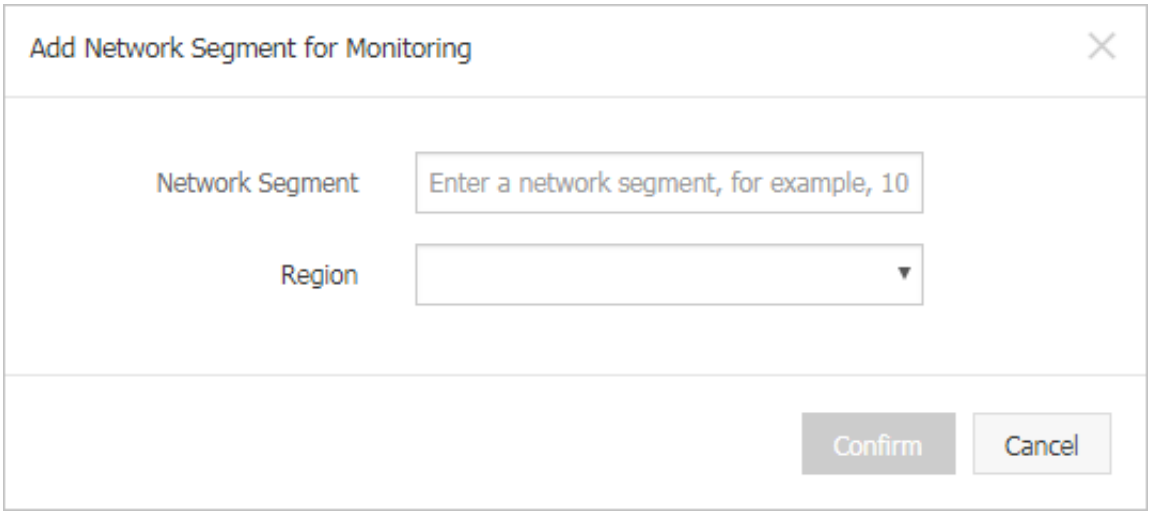
12.4.1.1 Add CIDR blocks for traffic monitoring

Procedure

1. Choose **System Management** > **Global Settings** > **Traffic Collecting Network Segment**.

2. Click **Add** to open the **Add Network Segment** dialog box, as shown in *Figure 12-8: Add Network Segment*.

Figure 12-8: Add Network Segment



3. Set parameters for monitoring traffic from the specified CIDR block.
   - Enter a CIDR block.

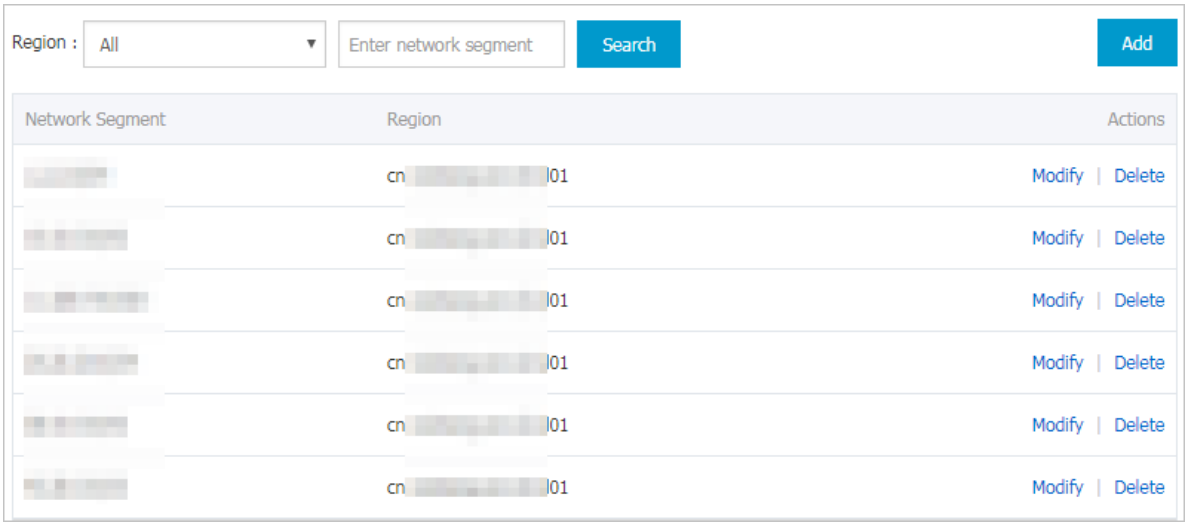
     Note:
     A CIDR block must be valid and cannot be entered more than once.
   - Select a region.
4. Click **OK** to add the CIDR block.

12.4.1.2 Manage CIDR blocks for traffic monitoring

Procedure

1. Choose **System Management** > **Global Settings** > **Traffic Collecting Network Segment**.
2. Select a region and enter the CIDR block you want to query. Then, click **Search** to view traffic collection CIDR block information, as shown in *Figure 12-9: Traffic Collecting Network Segment*.

Figure 12-9: Traffic Collecting Network Segment



3. Manage traffic collection CIDR blocks.
   - Click **Modify** to modify the region in the **Change Network Segment** dialog box, and click **Confirm** to modify the region of a traffic collection CIDR block.
   - Click **Delete** to delete the traffic collection CIDR block.

12.4.2 Set regions

Region settings are used to detect regions for Server Guard clients that are located in different data centers. After configuration, when the Server Guard hosts report the regions of CIDR blocks, the system automatically detects and matches hosts that are located in the same data centers.

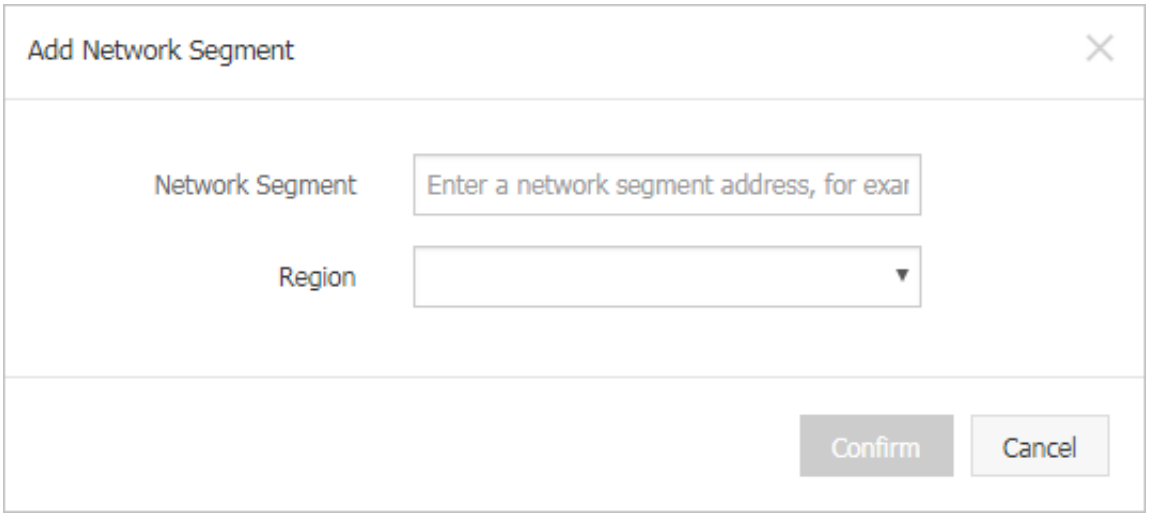
Note:
This feature allows you to change the region of a configured CIDR block. After modification, you must modify multiple regions of related assets in this CIDR block in Asset Overview at the same time.

12.4.2.1 Add regional CIDR blocks

Procedure

1. Choose **System Management** > **Global Settings** > **Region**.
2. Click **Add** to open the **Add Network Segment** dialog box, as shown in *Figure 12-10: Add Network Segment*.

Figure 12-10: Add Network Segment



3. Set the parameters of the CIDR block.
   - Enter a CIDR block.

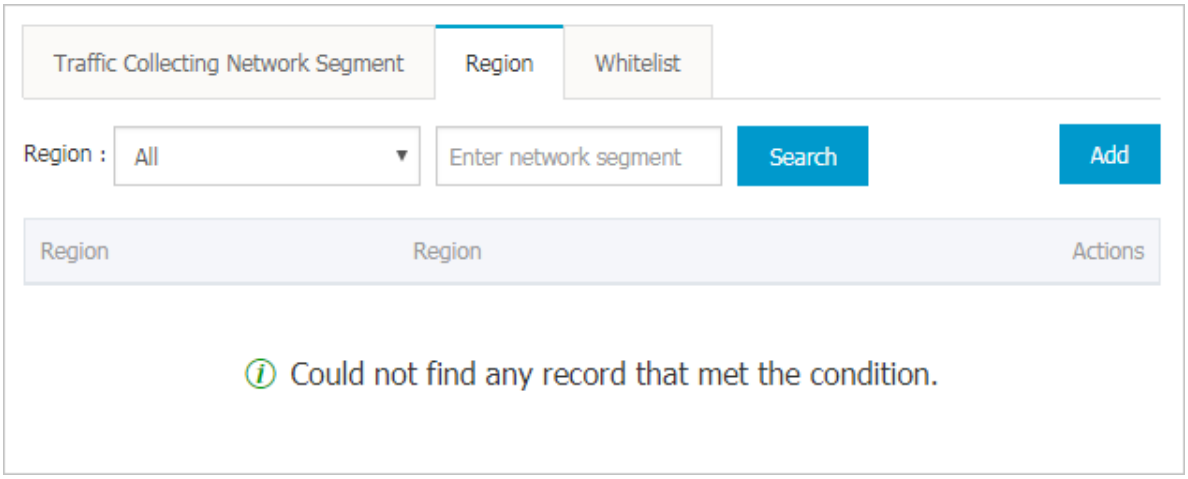
     Note:
     A CIDR block must be valid and cannot be entered more than once.
   - Select a region.
4. Click **OK** to add the CIDR block.

12.4.2.2 Manage regional CIDR blocks

Procedure

1. Choose **System Management** > **Global Settings** > **Region**.
2. Select a region and enter the CIDR block you want to query. Then, click **Search** to view region CIDR block information, as shown in *Figure 12-11: Region*.

Figure 12-11: Region



3. Manage region CIDR blocks.
   - Click **Modify** to modify the region in the Change Network Segment dialog box, and click **OK** to modify the region CIDR block information.
   - Click **Delete** to delete the region CIDR block information.