

# Alibaba Cloud Apsara Stack Enterprise

## Security Administrator Guide (Basic 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Note:</b> Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other contents.	 <b>Note:</b> You can use <b>Ctrl + A</b> to select all files.
>	Multi-level menu cascade.	<b>Settings &gt; Network &gt; Set network type</b>
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand   slave}</code>

# Contents

---

<b>Legal disclaimer.....</b>	<b>I</b>
<b>Generic conventions.....</b>	<b>I</b>
<b>1 Overview.....</b>	<b>1</b>
<b>2 Configuration requirements.....</b>	<b>2</b>
<b>3 Logon and logout.....</b>	<b>3</b>
3.1 Roles for Apsara Stack Security Center.....	3
3.2 Log on to the Apsara Stack Security.....	4
3.3 Log out of the Apsara Stack Security Center console.....	5
<b>4 Apsara Stack Security Basic Edition Security Center interface.....</b>	<b>6</b>
<b>5 Situation Awareness.....</b>	<b>8</b>
5.1 Overview.....	8
5.1.1 View network traffic information.....	8
5.2 View threat attack information.....	9
<b>6 Network Security.....</b>	<b>10</b>
6.1 Enable network security blocking.....	10
<b>7 Cloud Host Security.....</b>	<b>11</b>
7.1 Host List.....	11
7.1.1 Manage servers.....	11
7.1.2 Manage groups.....	12
7.2 Intrusion detection.....	13
7.2.1 Unusual Sign-in.....	13
7.2.1.1 Check unusual logon.....	14
7.2.1.2 Set the logon security policy.....	14
7.2.2 Webshells.....	15
7.2.2.1 Manage webshells.....	15
7.2.3 Suspicious Host.....	16
7.2.3.1 Manage suspicious hosts.....	16
7.3 Settings.....	17
7.3.1 Security configurations.....	17
<b>8 Physical Machine Security.....</b>	<b>18</b>
8.1 View and handle file tampering events.....	18
8.2 View and handle process exceptions.....	18
8.3 View and handle unusual network connections.....	19
8.4 View and handle suspicious port listening events.....	20
<b>9 Security audit.....</b>	<b>22</b>
9.1 View audit overview.....	22
9.2 View audit events.....	22
9.3 View raw logs.....	23

9.4 Policy settings.....	23
9.4.1 Manage audit policies.....	23
9.4.2 Manage action types.....	26
9.4.3 Set an alert receiver.....	27
9.4.4 Manage event log archives.....	29
9.4.5 Manage export tasks.....	29
<b>10 System management.....</b>	<b>30</b>
10.1 Manage Alibaba Cloud accounts.....	30
10.2 Alert settings.....	32
10.2.1 Set alert contacts.....	32
10.2.2 Set alert information.....	33
10.3 Global settings.....	34
10.3.1 Set CIDR blocks for traffic monitoring.....	34
10.3.1.1 Add CIDR blocks for traffic monitoring.....	34
10.3.1.2 Manage CIDR blocks for traffic monitoring.....	35
10.3.2 Set regions.....	36
10.3.2.1 Add regional CIDR blocks.....	36
10.3.2.2 Manage regional CIDR blocks.....	37



# 1 Overview

---

Apsara Stack Security Basic Edition is a cloud security operations platform designed to ensure the normal operation of cloud computing service platforms. Apsara Stack Security Basic Edition treats computing resources as its basic protection objects, cloud-based business systems as its core protected entities, and security event management as its primary weapon. It promptly and accurately discovers abnormal network activities and security threats on the cloud platform to help security administrators perform security management, risk analysis, emergency response, and make informed decisions.

Apsara Stack Security Basic Edition provides users with real-time protection capabilities, including abnormal traffic detection and analysis, web-layer attack detection and defense, and host intrusion protection. In addition, it provides security audit for ECS, ApsaraDB for RDS, physical servers, and APIs on the cloud computing platform, allowing security auditors to customize audit types.

## 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	<ul style="list-style-type: none"><li>• Internet Explorer: version 11 or later</li><li>• Google Chrome (recommended): version 42.0.0 or later</li><li>• Mozilla Firefox: version 30 or later</li><li>• Safari: version 9.0.2 or later</li></ul>
Operating system	<ul style="list-style-type: none"><li>• Windows XP, Windows 7, or a later versions of Windows</li><li>• macOS</li></ul>

## 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 LeftUser guideCite Right*.

**Table 3-1: Roles for Apsara Stack Security Center**

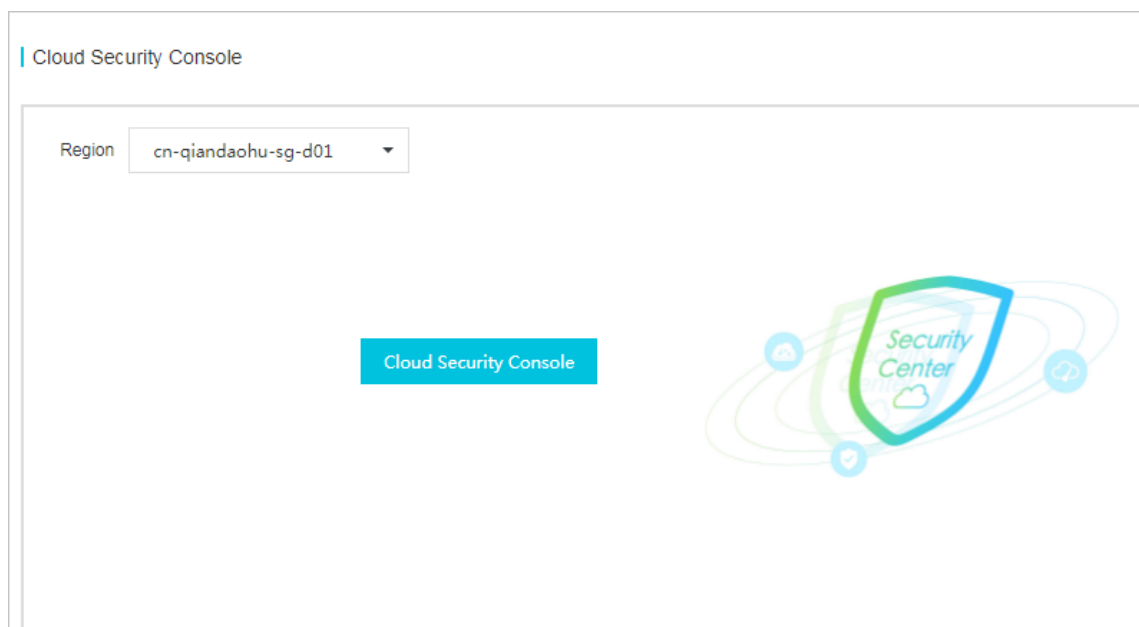
Role	Description
Cloud Security Center System Administrators	Responsible for the Apsara Stack Security Center system management and configuration. They have permissions for managing Apsara Stack accounts, setting alerts, and setting global parameters, but cannot perform intelligence synchronization.
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, 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, 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**.

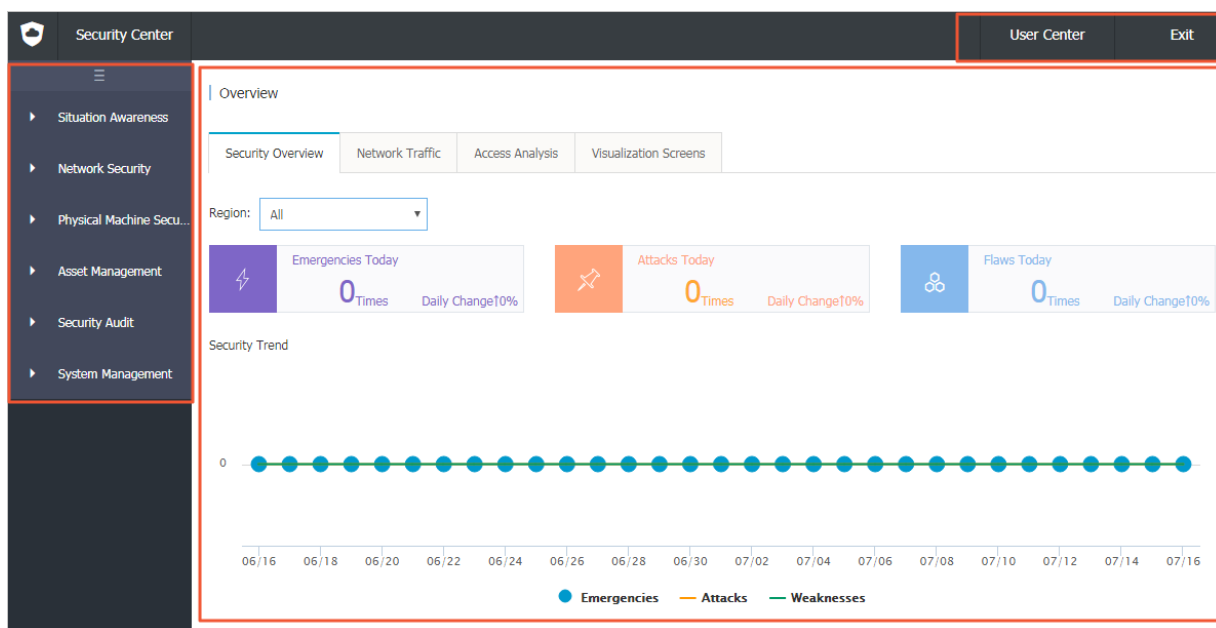
### 3.3 Log out of the Apsara Stack Security Center console

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

## 4 Apsara Stack Security Basic Edition Security Center interface

The Apsara Stack Security Basic Edition Security Center interface is divided into three main areas, as shown in [Figure 4-1: Apsara Stack Security Basic Edition Security Center Interface](#).

**Figure 4-1: Apsara Stack Security Basic Edition Security Center Interface**



**Table 4-1: Web interface**

Region	Description
Top operation button area	<ul style="list-style-type: none"> <li><b>User Center:</b> Click this button to modify your profile page.</li> <li><b>Exit:</b> Click this button to log out.</li> </ul>
Menu navigation area	<p>The Apsara Stack Security Center has five main components: Situation Awareness, Network Security, Host Security, Security Audit, and System Management. These components provide the following functions:</p> <ul style="list-style-type: none"> <li><b>Situation Awareness:</b> Provides an overview of current security trends based on network traffic conditions. It helps security administrators understand the current network traffic situation.</li> <li><b>Network Security:</b> Provides an view of abnormal network behaviors and security threats that are blocked by Apsara Stack Security, including application-layer attack and brute force attack.</li> <li><b>Host Security:</b> Provides host protection and intrusion detection to ensure the security of physical servers and cloud server.</li> </ul>

Region	Description
	<ul style="list-style-type: none"><li>• <b>Security Audit:</b> Presents and audits cloud service operation logs. This allows security auditors to promptly discover and eliminate security risks.</li><li>• <b>System Management:</b> Allows system administrators to configure settings of Apsara Stack Security, such as alert, synchronization, and detection scope settings.</li></ul>
Operation view area	After a menu item is selected, its function configuration interface is displayed in the right-side operation view area.

## 5 Situation Awareness

---

Situation Awareness integrates enterprise vulnerability monitoring, hacker intrusion monitoring, web attack monitoring, DDoS attack monitoring, threat intelligence monitoring, enterprise security reputation monitoring, and other security trend monitoring techniques. 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 scan. 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.

Apsara Stack Security Basic Edition's Situation Awareness mainly displays the network traffic situation in the Apsara Stack environment.

### 5.1 Overview

The **Overview** page provides an overview of current security trends based on network traffic conditions, allowing system administrator to quickly understand the current security status of the Apsara Stack environment.

Network traffic situation displays analysis of outgoing/incoming network traffic and QPS information. This shows system administrator high and low traffic times, speeds, and origin region distribution.

#### 5.1.1 View network traffic information

##### Context

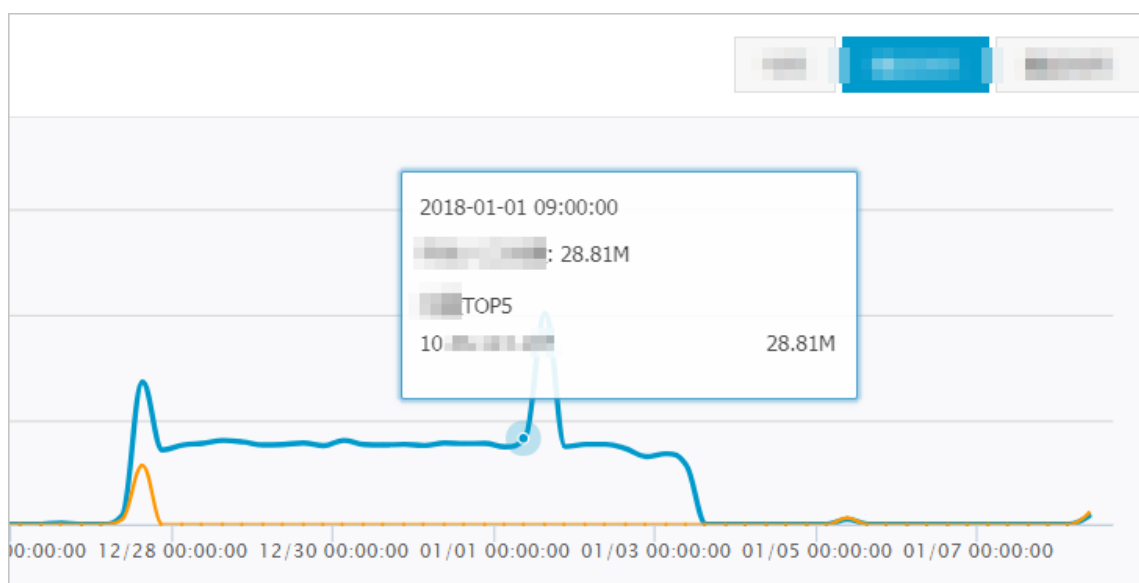
The Network Traffic page uses line graphs to show traffic information for a past time period. By viewing the traffic conditions for different periods, regions, or a single IP address, system administrator can locate high and low traffic periods and view traffic speed and region distributions. This page also shows the five IP addresses that generate the most traffic, so system administrator can effectively block access by malicious IP addresses.

##### Procedure

1. Click **Situation Awareness > Overview** to go to the **Overview** page.
2. View the traffic information of different periods, regions or single IP.
  - Click **Today**, **Past 30 Days**, or **Past 90 Days**, to view traffic information for the selected period.

- Select **Region**, or enter specific IP in the search box, to view traffic information for the selected region or entered IP.
3. View detailed traffic information of specific time.
- Move your cursor over the Network Outbound/Inbound Traffic graph to display the five IP addresses that generate the most traffic, as shown in [Figure 5-1: View top five IP addresses by traffic by traffic](#).

**Figure 5-1: View top five IP addresses by traffic**



- Move your cursor over the QPS (Average) graph to display the detailed QPS information.

## 5.2 View threat attack information

### Procedure

1. Go to **Situation Awareness > Threat Analysis** page.
2. View threat attack information detected by Apsara Stack Security Center.
  - Click **Application Attacks**, select Region, to view reported application attack information and application attack events.
    - View the attack trends and attack type information detected in the recent seven days.
    - View detailed information about all attack events.



#### Note:

In the **Type** area, click an attack type, to view attack events for the selected type.

- Click **Brute-force Cracking** to view brute-force cracking event records.

## 6 Network Security

### 6.1 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 6-1: 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 6-1: Blocking Switches setting**

Protection Settings			
Category	Status	Description	Actions
Web-based Attack Blocking	Activated	Web-based attack blocking is enabled.	
Brute-force Attack Blocking	Disabled	 Brute-force attack blocking is disabled. Only the warning function is provided.	
<div> Total: 2 item(s) , Per Page: 20 item(s) <div> « &lt; 1 &gt; » </div> </div>			

# 7 Cloud Host Security

## 7.1 Host List

### 7.1.1 Manage servers

On the Servers page, you can view the status of the servers that are protected by Server Guard.

#### Context

The following security statuses are available for a server:

- **Online:** Server Guard provides complete security protection for this server.
- **Offline:** Server Guard cannot provide security protection for this server because the Server Guard server cannot connect to the Server Guard client of the server.
- **Disabled Protection:** Security protection is temporarily disabled for this server. For more information, see [Disable Protection](#).


#### Procedure

1. Go to **Cloud Host Security > Host List**.

2. Optional: Search for a server.

If you want to view the security status of a specific sever, enter the IP address of the server and then click **Search**. The detailed security information of the server is displayed.

3. View the security status of the servers and the detailed information.

Click  in the upper-right corner to set the information columns to be displayed for the servers.

4. Manage servers.

Action	Description
Change Group	Select a server, and click <b>Change Group</b> to change the group for the server. For more information about grouping, see <a href="#">Manage groups</a> .
Modify Tag	Select a server, and click <b>Modify Tag</b> to set tag information for the server.
Security Check	Select a server, and click <b>Security Check</b> to perform a full security check.
Delete External Servers	Select an external server, and click <b>More &gt; Delete External Servers</b> to delete the external servers.

Action	Description
Disable Protection	Select a server in <b>Online</b> status, and click <b>More &gt; Disable Protection</b> to temporarily disable security protection for the server. This action reduces the resource consumption of the server.
Enable Protection	Select a server in <b>Disabled Protection</b> status, and click <b>More &gt; Enable Protection</b> to enable security protection for the server.

## 7.1.2 Manage groups

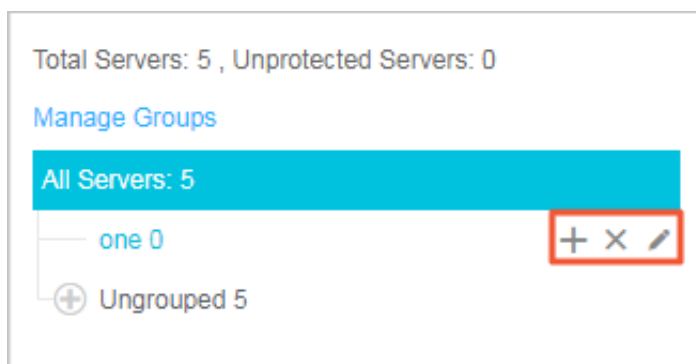
You can check security events and manage servers by group..

### Context

All servers are displayed in **Ungrouped** before they are grouped. If you delete a group, the servers in this group are moved to **Ungrouped**.

### Procedure

1. Choose **Cloud Host Security > Host List**.
2. Manage subgroups.



- Create a subgroup.

Click the Add button next to **All Servers** or a subgroup, enter the subgroup name, and click **Confirm**.



#### Note:

You can create subgroups at three levels.

- Modify a subgroup.

Click the Modify button next to a subgroup, enter the subgroup name, and click **Confirm**.

- Delete a subgroup.

Click the Delete button next to a subgroup, and click **Confirm** in the dialog box that appears.

**Note:**

After you delete this subgroup, the servers in this group are moved to **Ungrouped**.

**3. Assign servers to groups.**

- a) Select the target servers from the right server list.
- b) Click **Change Group**.
- c) Select a target group from the drop-down list in the dialog box that appears.
- d) Click **Confirm**.

**4. Manage groups**

Click **Manage Groups** to move groups that have higher priority to a higher level.

## 7.2 Intrusion detection

The intrusion detection feature detects intrusions on servers. Intrusions include unusual logons, webshells, and suspicious hosts.

### 7.2.1 Unusual Sign-in

On the **Brute-force/Unusual Sign-in** page in the Server Guard console, you can view the unusual logon information and logon alerts on a server. Unusual logon information includes invalid logon IP addresses, invalid accounts, and invalid logon time. Unusual logon alerts include unusual logon location alerts, invalid IP alerts, invalid time alerts, and invalid account alerts.

A Server Guard Agent regularly collects the log entries about the logons on the server and reports the log entries to the Server Guard server. The Server Guard server then analyzes and matches the received log entries. If the Server Guard server detects that a successful logon is from an unusual location or by using an invalid IP, invalid time, or invalid account, the Server Guard server generates an unusual logon alert.

**Note:**

To set the alert notification method to SMS, go to **System management > Alert Settings**, and select a notification method at **Secure > Logon Security: Unusual Logon**. Alerts can be sent by SMS, emails, or system message. By default, all three methods are used.

You can specify a valid IP, valid time, and valid account that are used to log on to a server. Any logon activity that uses an invalid IP, invalid time, or invalid account will trigger an alert. The system preferentially uses the specified valid IP, time, and account rather than the logon location to identify unusual logons.

### 7.2.1.1 Check unusual logon

You can check unusual logon alerts, including logons from unusual locations, brute-force cracking, logons using invalid IP addresses, logons using invalid accounts, and logons at an invalid time.

#### Procedure

1. Choose **Cloud Host Security > Intrusion Detection > Brute-force/Unusual Sign-in**.
2. Check all unusual logon alerts.

You can filter and search the alerts to quickly retrieve the specified unusual logon alerts, as shown in [Figure 7-1: Check all unusual logon alerts](#).

**Figure 7-1: Check all unusual logon alerts**

The screenshot displays a web interface for checking unusual logon alerts. At the top, there is a search section with 'Assets' set to 'All Groups', and input fields for 'Instance IP or name' and 'Server label', followed by a 'Search' button and a refresh icon. Below this, the 'Alarm Types' section contains five buttons: 'Remote Login', 'Brute Success', 'Illegal IP Login', 'Illegal Account Login', and 'Illegal Time Login'. The 'Status' section at the bottom has two buttons: 'Unresolved' and 'Resolved'.

3. Handle unusual logon alerts.

Select an unusual logon alert to check whether this is a false positive.

- If this alert is a false positive, click **Label as Handled**.
- If the logon is an intrusion, improve security on the related instance. For example, use a more complex password, fix vulnerabilities on the instance, remove risks that are detected in the baseline check, and specify a blacklist and a whitelist. Then, click **Label as Handled**.

### 7.2.1.2 Set the logon security policy

Set the logon security policy, including the usual logon locations, valid logon IP, valid logon time, and valid accounts.

#### Procedure

1. Choose **Cloud Host Security > Intrusion Detection > Brute-force/Unusual Sign-in**.
2. On the **Brute-force/Unusual Sign-in** page, click **Logon Security Settings** in the upper-right corner.

3. Set the Valid Logon IPs
4. Set the Valid Logon Time.
5. Set the Valid Logon Accounts.

## 7.2.2 Webshells

Server Guard uses both on-premises and cloud based protection, and supports scheduled protection and real-time scans. Server Guard can detect and quarantine common PHP and JSP backdoor files.

Server Guard checks the files in the directory on your server for webshell Trojan files. If a Webshell file is detected, Server Guard generates an alert.

Server Guard uses dynamic inspection or scheduled inspection to detect webshells.

- Dynamic inspection: If any modification occurs for a file in the directory, Server Guard performs a dynamic inspection on the modification.
- Scheduled inspection: Server Guard performs an inspection by scanning the entire directory between 0:00 and 6:00 every day.



### Note:

By default, all servers that are protected by Server Guard have scheduled inspection. You can also enable scheduled inspection for the specified servers only. Go to **Settings > Security Settings**. In the **Trojan Scan** area, click **Manage** next to **Regular Directory Detection** to specify the servers on which you want to enable scheduled inspection.

### 7.2.2.1 Manage webshells

You can detect and quarantine webshells.

#### Procedure

1. Choose **Cloud Host Security > Intrusion Detection > Webshell**.
2. Select an asset, and check the webshells that have been detected, as shown in [Figure 7-2: Select an asset](#).

**Figure 7-2: Select an asset**

### 3. Handle webshells.

- **Quarantine:** Quarantine one or more Trojan files.
- **Restore:** If you want to restore quarantined webshells, click **Restore**.
- **Ignore:** Server Guard does not generate alerts for an ignored Trojan file.

**Note:**

Server Guard does not delete Trojan files. Server Guard quarantines Trojan files. You can restore a quarantined file if you are sure that the file is a trusted file. Server Guard will not generate alerts for a file that has been marked as trusted.

## 7.2.3 Suspicious Host

You can view unusual processes, sensitive file tampering, unusual network connections, unusual events, and suspicious files that have been detected on the servers.

### 7.2.3.1 Manage suspicious hosts

You can check and handle suspicious host alarms on the instance.

#### Procedure

1. Choose **Cloud Host Security > Intrusion Detection > Suspicious Host**.
2. Select a target asset, and check the corresponding suspicious host events generated by the system.
3. Select a solution according to the specific suspicious host event, as shown in [Table 7-1: Solutions](#).

**Table 7-1: Solutions**

Operation	Description
Fix	Fixes the vulnerability immediately.
Ignore Once	Ignores this alarm if the event does not affect instance security.
Confirm	Confirms this event.
Label as False Positive	Labels this alarm as a false positive.
View	Displays details of this alarm.

## 7.3 Settings

This section provides details of security configurations, alarm configurations, and installing and uninstalling Server Guard.

### 7.3.1 Security configurations

#### Procedure

1. Choose **Cloud Host Security > Settings**.
2. Configure the instance to periodically detect and remove Trojans.
  - a) Click **Manage**.
  - b) Select the instance that requires periodic Trojan detection and removal.
  - c) Click **Confirm** to complete the configuration.
3. Configure the resource utilization for Server Guard.
  - **Business priority mode**: CPU utilization peak is less than 10% and memory usage peak is less than 50 MB.
  - **Protection priority mode**: CPU utilization peak is less than 20% and memory usage peak is less than 80 MB.
  - a) Click **Manage**.
  - b) Specify the work mode of Server Guard on the instance.
  - c) Click **Confirm** to complete the configuration.

## 8 Physical Machine Security

### 8.1 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 8-1: File tampering events](#).

**Figure 8-1: File tampering events**

Physical Machine Protection										
Type: <b>File Tampering</b> Process Exception Unusual Network Connection Suspicious Port Listening										
Status: All Enter server IP; fuzzy search supported Enter file directory; fuzzy search supported Time of Change: Time Period to End Time Search										
<input type="checkbox"/>	IP Address	Region	File Directory	Type of Change	Time of Change	Original File Creation Time	Details of Change	Status	Actions	
<input type="checkbox"/>		Default Data Center	/etc/init.d/pgsql	File Modification	07/26/2018, 16:11:15	05/23/2018, 01:09:37	Source MD5:edad6e83c3c1f344ba17e45e546dd27 Modified MD5:14ef42d5c89f1bd5cf608f2b8d3c84a7	Unhandled	Mark as Handled	
<input type="checkbox"/>		Default Data Center	/etc/init.d/mongodb	File Modification	07/26/2018, 15:45:19	05/23/2018, 22:00:11	Source MD5:671cebd53b1c2cd260959fae330c7b0 Modified MD5:671cebd53b1c2cd260959fae330c7b0	Unhandled	Mark as Handled	
<input type="checkbox"/>		Default Data Center	/etc/init.d/mongodb	File Modification	07/26/2018, 15:44:39	05/23/2018, 21:42:58	Source MD5:3d7382c158bb64a1937f1c3c1ea267ee Modified MD5:3d7382c158bb64a1937f1c3c1ea267ee	Unhandled	Mark as Handled	
<input type="checkbox"/>		Default Data Center	/etc/init.d/mongodb.bak	File Modification	07/26/2018, 15:41:10	05/23/2018, 21:42:58	Source MD5:2b4a7c0c2678597d1f2c03cfc7997bc9 Modified MD5:2b4a7c0c2678597d1f2c03cfc7997bc9	Unhandled	Mark as Handled	

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.

### 8.2 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 8-2: Process Exception](#).

**Figure 8-2: Process Exception**

Physical Machine Protection										
Type:	File Tampering <b>Process Exception</b> Unusual Network Connection Suspicious Port Listening									
Status:	All	Enter server IP; fuzzy search supported		Enter process path; fuzzy search supported		Start Time:	Time Period	to	End Time	Search
	IP Address	Region	Process Path	Process Type	Start Time	File Size	File Hash	File Creation Time	Status	Actions
<input type="checkbox"/>		Default Data Center	/usr/bin/pamdicts	rootkitminer_file	06/27/2018, 15:46:25	11128	ddd268ab28805f60967cbe7275829991	06/10/2018, 04:02:01	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>		Default Data Center	/boot/vfpjyckqma	gate_xordoor_file	06/27/2018, 15:38:41	8464	e0bc372135f5707a7689bd3069c705a	06/05/2018, 16:34:41	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>		Default Data Center	/etc/rc.d/init.d/selinux	gate_backdoor_file	06/27/2018, 15:37:05	8464	4a8e5735fefe17ec4410e5e4889dca3a	06/05/2018, 16:31:11	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>		Default Data Center	/etc/rc.d/init.d/selinux	gate_backdoor_file	Not started	8464	4a8e5735fefe17ec4410e5e4889dca3a	06/27/2018, 16:04:22	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>		Default Data Center	/etc/rc.d/init.d/selinux	gate_backdoor_file	Not started	8464	4a8e5735fefe17ec4410e5e4889dca3a	06/11/2018, 11:42:04	Unhandled	<a href="#">Mark as Handled</a>

**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.

## 8.3 View and handle unusual network connections

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

**Procedure**

- Choose **Physical Machine Security > Physical Machine Protection**, and select **Unusual Network Connection**.
- View unusual network connection records, as shown in [Figure 8-3: Unusual Network Connection](#).

**Figure 8-3: Unusual Network Connection**

Physical Machine Protection									
Type:	File Tampering	Process Exception	Unusual Network Connection	Suspicious Port Listening					
Status:	All	Enter server IP; fuzzy search supported	Enter process path; fuzzy search supported	Connection Time:	Time Period	to	End Time	Search	
	IP Address	Region	Event Type	Connection Time	Process	Process Path	Connection Details	Status	Actions
<input type="checkbox"/>	10.10.10.10	Default Data Center	Connect Internet	07/27/2018, 10:28:23	96013	/usr/bin/curl	Source IP:10.10.2.36:26113 Target IP:12.39.119.4:80	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>	10.10.10.10	Default Data Center	Connect Internet	07/24/2018, 12:48:22	3402	/home/staragent/bin/staragentd	Source IP:10.10.2.211:48324 Target IP:140.205.131.94:80	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>	10.10.10.10	Default Data Center	Connect Internet	07/13/2018, 15:32:59	2758	/home/staragent/bin/staragentd	Source IP:10.10.3.33:47032 Target IP:106.11.80.158:80	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>	10.10.10.10	Default Data Center	Connect Internet	07/04/2018, 17:31:07	45779	/opt/taobao/java/bin/java	Source IP:10.10.2.141:43160 Target IP:1.1.1.1:80	Unhandled	<a href="#">Mark as Handled</a>

### 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.

## 8.4 View and handle suspicious port listening events

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

### Procedure

- Choose **Physical Machine Security > Physical Machine Protection**, and select **Suspicious Port Listening**.
- View suspicious port listening events, as shown in [Figure 8-4: Suspicious Port Listening](#).

**Figure 8-4: Suspicious Port Listening**

Physical Machine Protection									
Type:	File Tampering	Process Exception	Unusual Network Connection	Suspicious Port Listening					
Status:	All	Enter server IP; fuzzy search supported	Port	Enter process path; fuzzy search supported	Listening Time:	Time Period	to	End Time	Search
	IP Address	Region	Listening Port	Listening Start Time	Process	Process Path	Port Status	Status	Actions
<input type="checkbox"/>	10.10.10.10	Default Data Center	3017	07/27/2018, 15:54:04	/u01/mongodb_20170628_0.4.3/bin/mongod	/u01/mongodb_20170628_0.4.3/bin/mongod	Listening	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>	10.10.10.10	Default Data Center	3015	07/27/2018, 15:54:03	/u01/mongodb_20170628_0.4.3/bin/mongod	/u01/mongodb_20170628_0.4.3/bin/mongod	Listening	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>	10.10.10.10	Default Data Center	57834	07/27/2018, 11:36:10	/u01/gpdb_20171116/bin/postgres	/u01/gpdb_20171116/bin/postgres	Listening	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>	10.10.10.10	Default Data Center	60325	07/27/2018, 11:36:09	/u01/gpdb_20171116/bin/postgres	/u01/gpdb_20171116/bin/postgres	Listening	Unhandled	<a href="#">Mark as Handled</a>
<input type="checkbox"/>	10.10.10.10	Default Data Center	46469	07/27/2018, 11:36:09	/u01/gpdb_20171116/bin/postgres	/u01/gpdb_20171116/bin/postgres	Listening	Unhandled	<a href="#">Mark as Handled</a>

**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.

## 9 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.

### 9.1 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.

### 9.2 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](#).

## 9.3 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](#).

## 9.4 Policy settings

### 9.4.1 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
<code>^\d{5,12}\$</code>	Indicates that the fifth to the twelfth numbers are matched in the string.
<code>load_file\((</code>	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 9-1: Audit Policies](#).



**Figure 9-2: Add Policy**

Add Policy

Policy Name
Enter policy name

Audit Type:
Database

Audit Target:
Global

Action Type:
test
Risk Level:
High
Notify:
Alert

Filter Condition:

User	equa	Enter user	x	+
Target	equa	Enter target	x	+
Action	equa	Enter command	x	+
Result	equa	Enter result		
Cause	equa	Enter reason		
Notes	Notes			

Add
Cancel

**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.

## 9.4.2 Manage action types

### Procedure

- Choose **Security Audit > Policy Settings**, and select **Type Settings**. The Type Settings page is displayed, as shown in [Figure 9-3: Type Settings](#).

**Figure 9-3: Type Settings**

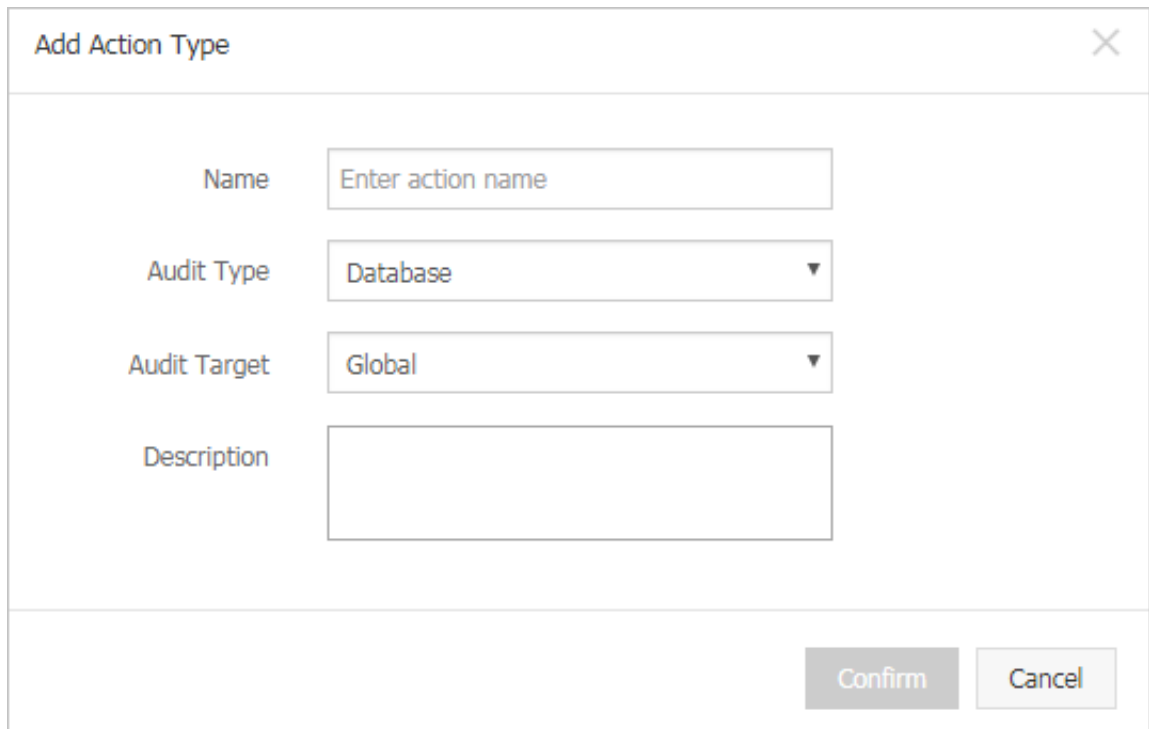
Audit Policies	Type Settings	Alarm Settings	Archiving	Exporting	System Settings
Audit Type: <input type="text" value="Database"/> Audit Target: <input type="text" value="Global"/> <input type="button" value="Search"/> <input type="button" value="New"/>					
Name	Audit Type	Audit Target	Created At	Description	Actions
test	Database	Global	2018-06-15 17:14:12	test	<a href="#">Delete</a>
Database Attacks	Database	Global	2018-03-28 14:38:49	Database Attack	<a href="#">Delete</a>

- 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.

- Manage action types.
  - Click **New**. In the **Add Action Type** dialog box, enter relevant information to add an action type, as shown in [Figure 9-4: Add Action Type](#).

**Figure 9-4: Add Action Type**A dialog box titled "Add Action Type" with a close button (X) in the top right corner. It contains four input fields: "Name" with a placeholder "Enter action name", "Audit Type" with a dropdown menu showing "Database", "Audit Target" with a dropdown menu showing "Global", and "Description" with a text area. At the bottom right, there are two buttons: "Confirm" and "Cancel".

Name	<input type="text" value="Enter action name"/>
Audit Type	<input type="text" value="Database"/>
Audit Target	<input type="text" value="Global"/>
Description	<input type="text"/>

Confirm Cancel

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

**Note:**

The default action types of the system cannot be deleted.

### 9.4.3 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 9-5: Alarm Settings](#).

**Figure 9-5: Alarm Settings**

The screenshot shows the 'Alarm Settings' tab in a management console. At the top, there are tabs for 'Audit Policies', 'Type Settings', 'Alarm Settings' (selected), 'Archiving', 'Exporting', and 'System Settings'. Below the tabs are search filters: 'Audit Type' (dropdown set to 'All'), 'Audit Target' (dropdown set to 'All'), a text input for 'Enter email address', and 'Risk Level' (dropdown set to 'Global'). There are 'Search' and 'New' buttons. Below the filters is a table with columns: Email, Audit Type, Audit Target, Name, Risk Level, and Actions. The table contains three rows of data. At the bottom right, there is a pagination summary: 'Total: 3 item(s) , Per Page: 20 item(s)' and a page navigation control showing '1'.

Email	Audit Type	Audit Target	Name	Risk Level	Actions
[Redacted]	User Actions	Apsara Stack Management Console Operation Log	abc	Global	Delete
[Redacted]	Database	mys1538p_db2	lee	Global	Delete
[Redacted]	Network Device	10.10.10.3	lsp	Global	Delete

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 9-6: Add Alert Receiver](#).

**Figure 9-6: Add Alert Receiver**

The screenshot shows the 'Add Alert Receiver' dialog box. It has a title bar with a close button (X). The form contains five fields: 'Email' (text input with placeholder 'Enter a valid email address. For example: '), 'Name' (text input with placeholder 'Enter name'), 'Audit Type' (dropdown menu set to 'All'), 'Audit Target' (dropdown menu set to 'All'), and 'Risk Level' (dropdown menu set to 'Global'). At the bottom right, there are two buttons: 'Confirm' and 'Cancel'.

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

## 9.4.4 Manage event log archives

### Procedure

1. Choose **Security Audit > Policy Settings**, and select **Archiving**. The Archiving page is displayed, as shown in *Figure 9-7: Archiving*.

**Figure 9-7: Archiving**

<div> <div>Audit Policies</div> <div>Type Settings</div> <div>Alarm Settings</div> <div>Archiving</div> <div>Exporting</div> <div>System Settings</div> </div>					
<div> <div>Audit Type: All</div> <div>Archive Type: All</div> <div>Detected At: Time Period</div> <div>14 : 28</div> <div>to End Time</div> <div>14 : 28</div> <div>Search</div> </div>					
File Name	SHA256 Hash	Archive Type	Created At	Actions	
OPS/2018-07-10/OPS-20180710142243.zip	cc6518344a4c4b57e7403104443e33c55e6e31533f68c788812b360c5c7e59a3	Event Archive	2018-07-10 14:22:44	<a href="#">Download</a>	
USER/2018-07-10/USER-20180710142243.zip	5070252ee61beade9c9c20e746510b8096e33273564ff2650aa6fef9da4b985c	Event Archive	2018-07-10 14:22:44	<a href="#">Download</a>	
NETWORK/2018-07-10/NETWORK-20180710142243.zip	be1b91d9ad6b4c44bd4d8f849a07778220ab4dd119e46a5819ae9efa5cb86981	Event Archive	2018-07-10 14:22:43	<a href="#">Download</a>	

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.

## 9.4.5 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.

# 10 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 three main parts:

- **User Management:** This is used to manage Apsara Stack Security accounts.
- **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.

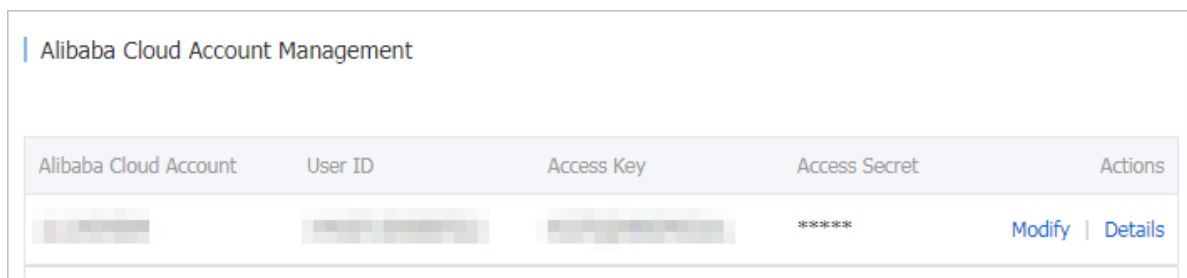
## 10.1 Manage Alibaba Cloud accounts

### 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 10-1: Alibaba Cloud Account Management](#).

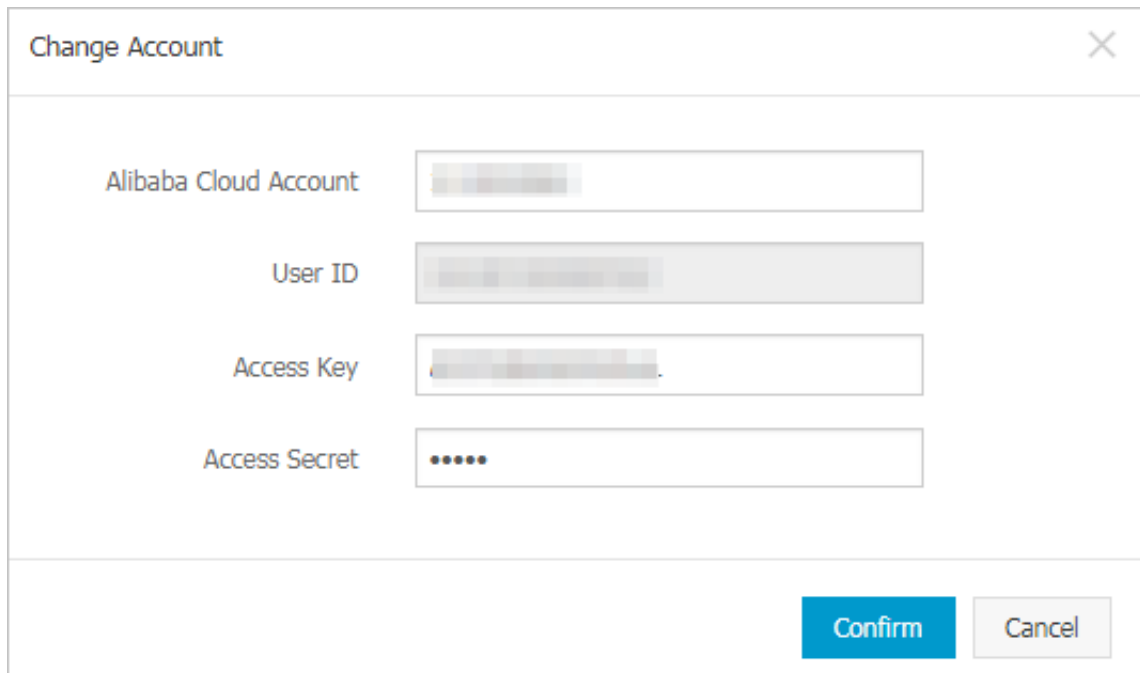
In Apsara Stack Security, all assets are bound to Alibaba Cloud accounts. Be cautious when you modify information.

**Figure 10-1: Alibaba Cloud Account Management**



Alibaba Cloud Account Management				
Alibaba Cloud Account	User ID	Access Key	Access Secret	Actions
			*****	<a href="#">Modify</a>   <a href="#">Details</a>

2. Click **Modify**. In the modification dialog box that appears, modify the information, and click **Confirm** to complete the modification, as shown in [Figure 10-2: Account modification dialog box](#).

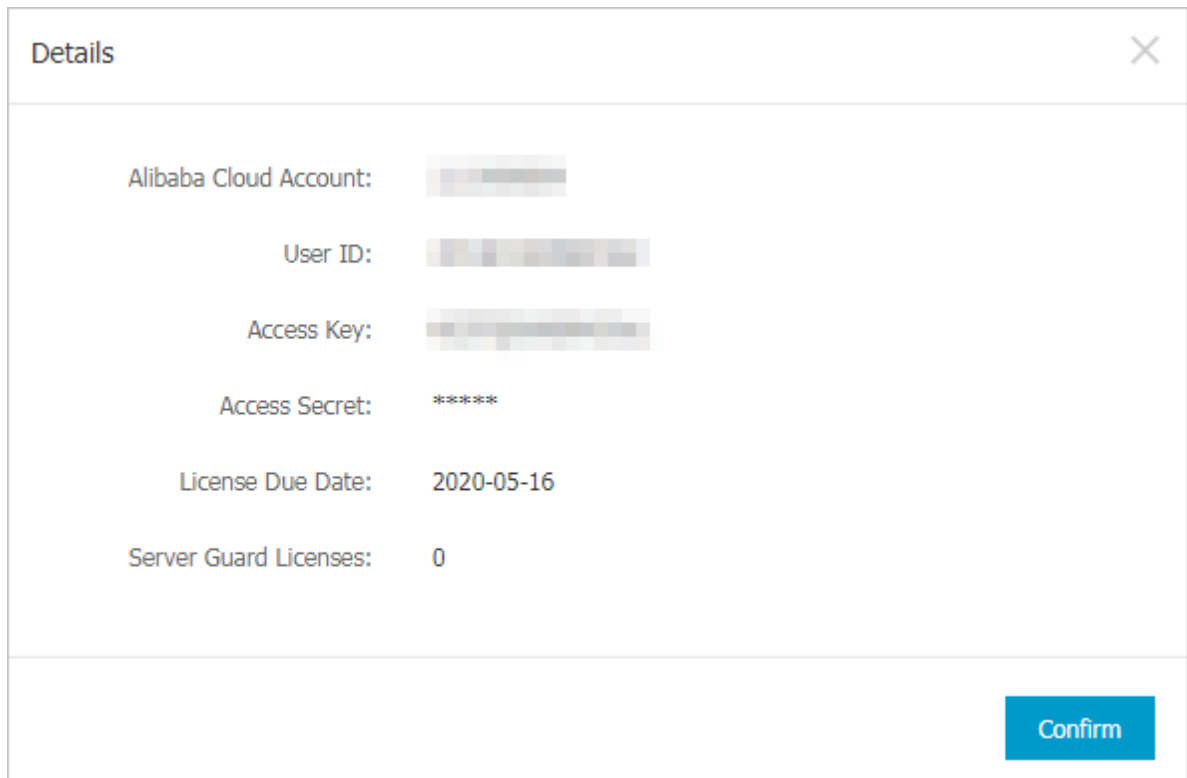
**Figure 10-2: Account modification dialog box**

The image shows a 'Change Account' dialog box with a close button (X) in the top right corner. It contains four input fields for account information: 'Alibaba Cloud Account', 'User ID', 'Access Key', and 'Access Secret'. The 'Access Secret' field is masked with dots. At the bottom right, there are 'Confirm' and 'Cancel' buttons.

Field	Value
Alibaba Cloud Account	[Redacted]
User ID	[Redacted]
Access Key	[Redacted]
Access Secret	.....

Buttons: Confirm, Cancel

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 10-3: Account details](#). You can obtain the information using the user ID and AccessKey that you have configured.

**Figure 10-3: Account details**

The screenshot shows a 'Details' dialog box with a close button (X) in the top right corner. The dialog contains the following information:

Alibaba Cloud Account:	[Redacted]
User ID:	[Redacted]
Access Key:	[Redacted]
Access Secret:	*****
License Due Date:	2020-05-16
Server Guard Licenses:	0

A blue 'Confirm' button is located at the bottom right of the dialog.

## 10.2 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.

### 10.2.1 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 10-4: Alarm Recipient page](#).

**Figure 10-4: Alarm Recipient page**

Alarm Settings

Alarm Recipient

Add Contacts

Contact Name	Mobile Number	Email	Actions
111			<a>Edit</a>   <a>Delete</a>
222			<a>Edit</a>   <a>Delete</a>

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.

## 10.2.2 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 10-5: Alert Settings*.

**Figure 10-5: Alert Settings**

Alarm Settings

Alarm Recipient

Alert Notification

	<input type="checkbox"/> All	<input type="checkbox"/> All
Secure	Notification Mode	
Logon Security: Unusual Logon The account has been logged on elsewhere.	<input type="checkbox"/> Mobile Number	<input type="checkbox"/> Email
Emergency Alarms	Notification Mode	
Page Tampering Web pages tampered with by attackers may affect SEO and are flagged as malicious by the search engine.	<input type="checkbox"/> Mobile Number	<input type="checkbox"/> Email
Zombie Attack If a host launches DDoS attacks or brute-force attacks on other hosts, it may have been controlled by attackers.	<input type="checkbox"/> Mobile Number	<input type="checkbox"/> Email
Password Cracked Attackers attempt to log on to your host by cracking your password. After certain attempts, they may successfully log on to it.	<input type="checkbox"/> Mobile Number	<input type="checkbox"/> Email
Backdoor Detected After host intrusion, attackers may install backdoors for further attacks.	<input type="checkbox"/> Mobile Number	<input type="checkbox"/> Email

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

## 10.3 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.

### 10.3.1 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.

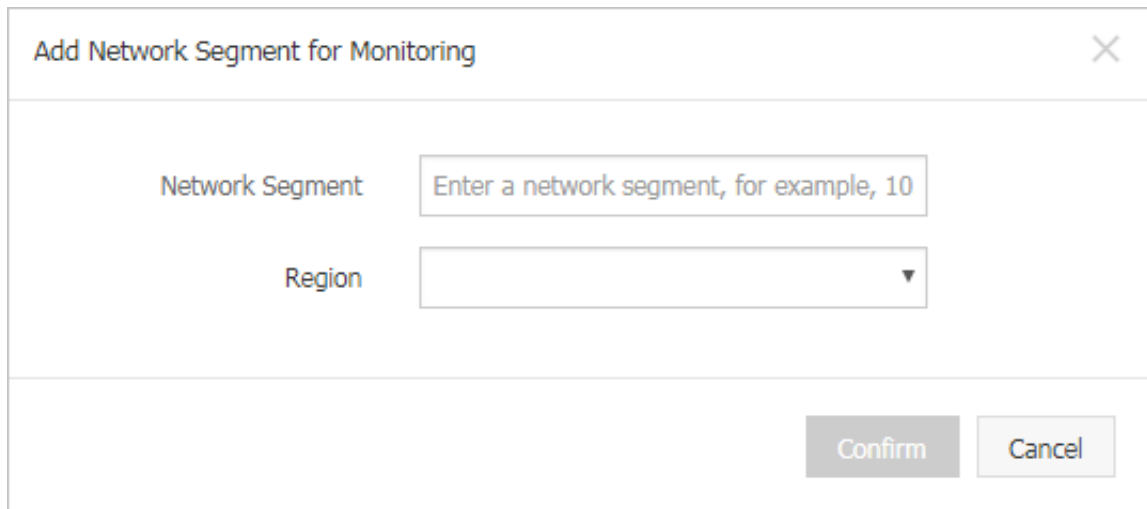
**Note:**

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

#### 10.3.1.1 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 10-6: Add Network Segment](#).

**Figure 10-6: Add Network Segment**

The dialog box titled "Add Network Segment for Monitoring" contains two input fields. The first field, labeled "Network Segment", has a placeholder text "Enter a network segment, for example, 10". The second field, labeled "Region", is a dropdown menu. At the bottom right of the dialog are two buttons: "Confirm" and "Cancel".

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.

### 10.3.1.2 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 10-7: Traffic Collecting Network Segment](#).

**Figure 10-7: Traffic Collecting Network Segment**

Region :	All ▼	Enter network segment	Search	Add
Network Segment	Region	Actions		
[blurred]	cn [blurred] 01	Modify	Delete	
[blurred]	cn [blurred] 01	Modify	Delete	
[blurred]	cn [blurred] 01	Modify	Delete	
[blurred]	cn [blurred] 01	Modify	Delete	
[blurred]	cn [blurred] 01	Modify	Delete	
[blurred]	cn [blurred] 01	Modify	Delete	

**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.

## 10.3.2 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.

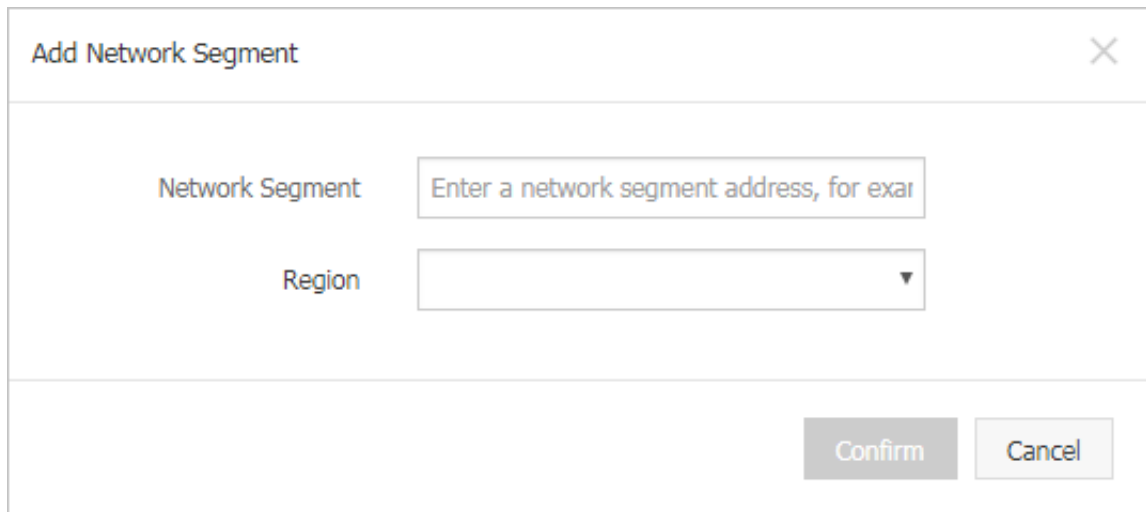
**Note:**

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.

### 10.3.2.1 Add regional CIDR blocks

**Procedure**

- Choose **System Management > Global Settings > Region**.
- Click **Add** to open the **Add Network Segment** dialog box, as shown in [Figure 10-8: Add Network Segment](#).

**Figure 10-8: Add Network Segment**A dialog box titled "Add Network Segment" with a close button (X) in the top right corner. It contains two input fields: "Network Segment" with a placeholder text "Enter a network segment address, for exam" and "Region" with a dropdown arrow. At the bottom right, there are two buttons: "Confirm" and "Cancel".

Add Network Segment

Network Segment

Region

Confirm Cancel

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.

## 10.3.2.2 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 10-9: Region](#).

**Figure 10-9: Region**

Traffic Collecting Network Segment
Region
Whitelist

Region : All
Enter network segment
Search
Add

Region	Region	Actions
<i>i</i> Could not find any record that met the condition.		

**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.