Alibaba Cloud
Apsara Stack Enterprise
Apsara Stack Security

Security Administrator Guide

Version: 1901

Issue: 20190528

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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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

Legal disclaimer I
Generic conventions I
1 Restrictions 1
2 Log on to Cloud Security Operations Center 2
3 Cloud Security Operations Center interface 3
4 Monitoring center 5
4.1 Dashboard 5
4.1.1 View the security overview dashboard 5
4.1.2 View User Dashboard 7
4.2 User monitoring 8
4.2.1 Query security events 8
4.2.2 Query security vulnerabilities 9
4.2.3 Query network traffic 10
4.2.4 Query web protection status 11
4.2.5 Asset monitoring 12
4.2.5.1 Query asset security information 12
4.2.5.2 View servers 13
4.2.5.3 View RDS instances 14
4.2.5.4 View OSS instances 15
4.2.5.5 View SLB instances 15
4.2.5.6 View EIP instances 16
5 Services 17
5.1 Traffic monitoring and management 17
5.1.1 Manage the detection threshold list 17
5.1.1.1 Add a traffic protection policy 17
5.1.1.2 Manage traffic protection policies 18
5.1.2 Configure traffic collection 18
5.1.2.1 Set a traffic collection CIDR block 18
5.1.2.2 Set a region 19
5.1.2.3 Set a whitelist 20
5.1.3 Enable attack blocking 21
5.2 Anti-DDoS management 21
5.2.1 Manage the DDoS console 21
5.2.1.1 Set the traffic scrubbing threshold for a single IP address 22
5.2.1.2 Set the traffic scrubbing threshold for multiple IP addresses 23
5.2.1.3 Customize a traffic scrubbing policy 24
5.2.1.4 Manually scrub traffic 27
5.2.2 Manage DDoS events 28
5.3 WAF management 29

5.3.1 Manage domain names.....29
5.3.2 Rules.....30
5.3.2.1 Manage rules.....30
5.3.2.2 Manage rule groups.....31
5.3.2.3 Publish a rule.....31
6 Tasks.....32
6.1 Add operation logs.....32
6.2 View the operation calendar.....32
7 Reports.....34
7.1 Create a report task.....34
7.2 View reports.....36

1 Restrictions

Before logging on to Apsara Stack Security Center, make sure that your local PC meets the requirements

described in *Table 1-1: Configuration requirements*.

Table 1-1: Configuration requirements

Item	Requirements
Browser	• Internet Explorer: 11 or later • Google Chrome (recommended): 42.0.0 or later • Mozilla Firefox: 30 or later • Safari: 9.0.2 or later
Operating system	• Windows XP, Windows 7, or later • Mac

2 Log on to Cloud Security Operations Center

This topic describes how to log on to Cloud Security Operations Center.

Prerequisites

- Obtain the logon address of Apsara Stack Operation.
- Obtain the username and password for logging on to Apsara Stack Operation.

Procedure

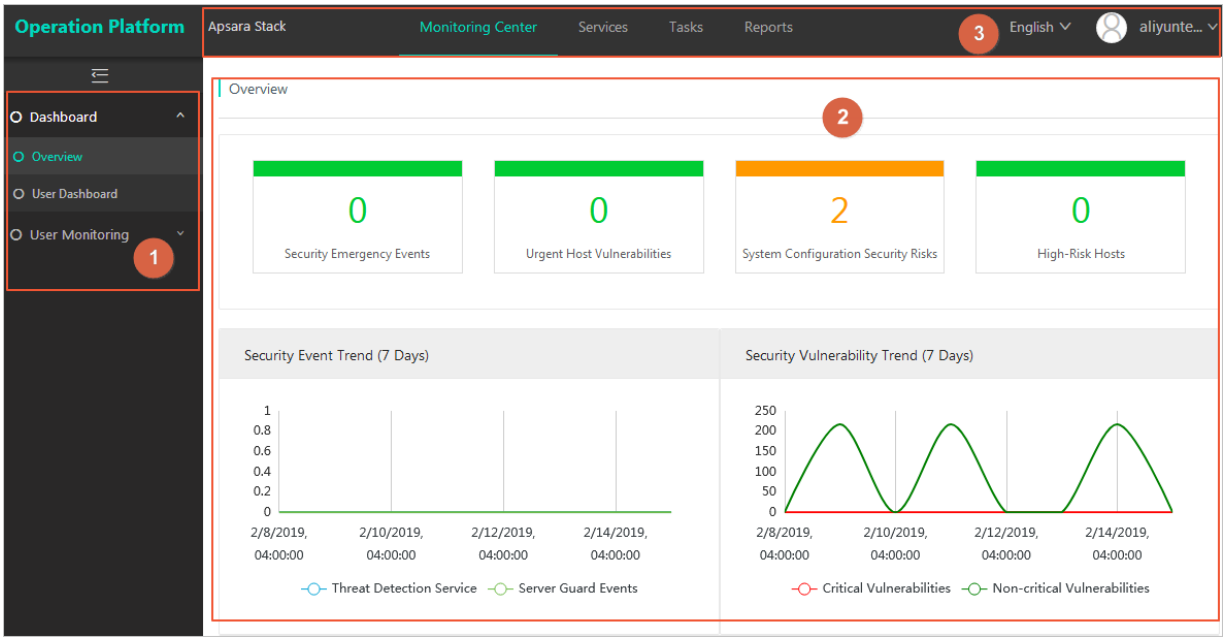
1. In the browser address bar, enter `https://Apsara Stack Operation logon address`, and press Enter.
2. On the logon page, enter the username and password, and click **Log On**.
3. In the left-side navigation pane, click **Products**.
4. In the product list, click **Cloud Security Operation Center**, and **Cloud Security Operations Center** is displayed.

3 Cloud Security Operations Center interface

This topic describes the interface of Cloud Security Operations Center.

The interface is divided into three areas, as shown in *Figure 3-1: Cloud Security Operations Center*.

Figure 3-1: Cloud Security Operations Center



SN	Area	Description
1	Top navigation bar	The top navigation bar consists of the following modules: • **Monitoring Center**: allows you to view the security status of Apsara Stack. • **Services**: allows you to manage Apsara Stack Security services. • **Tasks**: allows you to manage operation logs. • **Reports**: allows you to manage and use report templates and view reports. You can also change the display language or click the username to log out.
2	Left-side navigation pane	The left-side navigation pane displays the features of each module in the top navigation bar.

SN	Area	Description
3	Operation view	After you select a feature in the left-side navigation pane , its configuration is displayed in the right-side operation view area.

4 Monitoring center

4.1 Dashboard

4.1.1 View the security overview dashboard

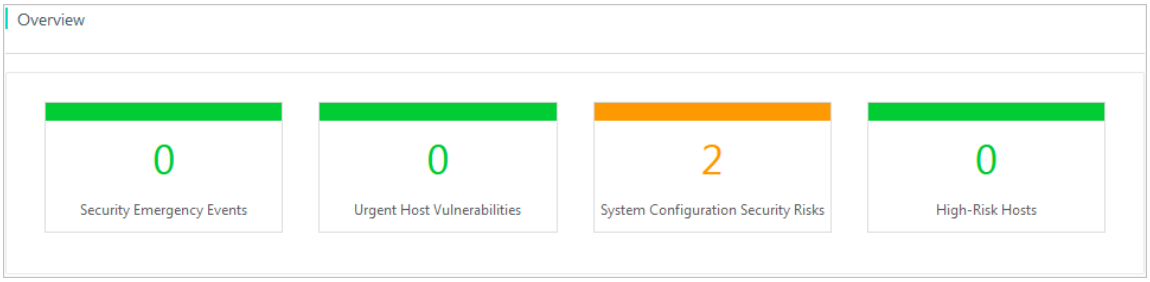
This topic describes how to view the security overview dashboard.

Context

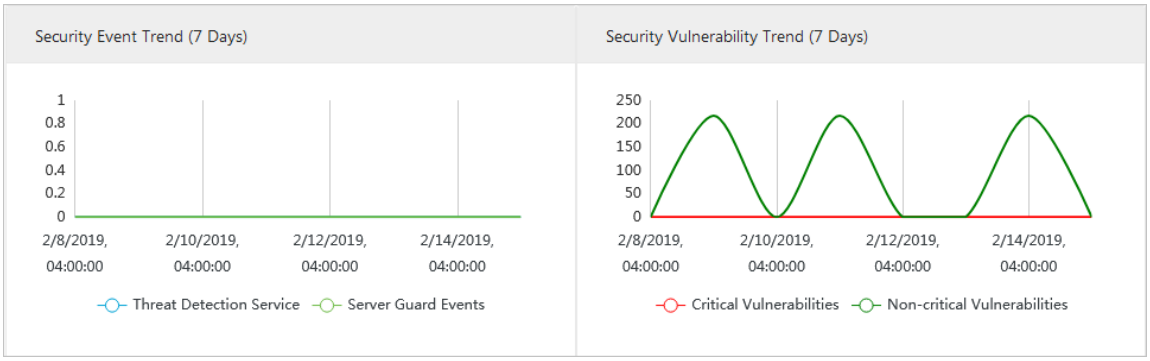
This dashboard displays the overall security status of Apsara Stack. IT administrators can check the security threats and attacks on Apsara Stack and enhance the security of the most vulnerable servers and accounts.

Procedure

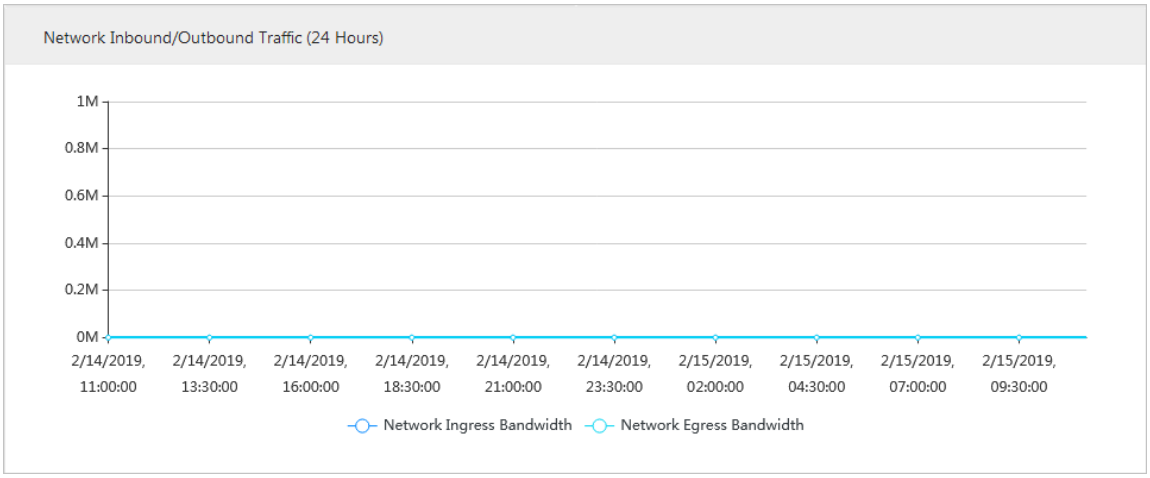
1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **Dashboard** > **Overview**.
3. View the security overview dashboard.
   - The first part on this dashboard displays the overview of security events in the system, including security emergencies, urgent host vulnerabilities, system configuration security risks, and high-risk hosts.



   - The second part displays the security events and vulnerabilities for the previous 7 days.

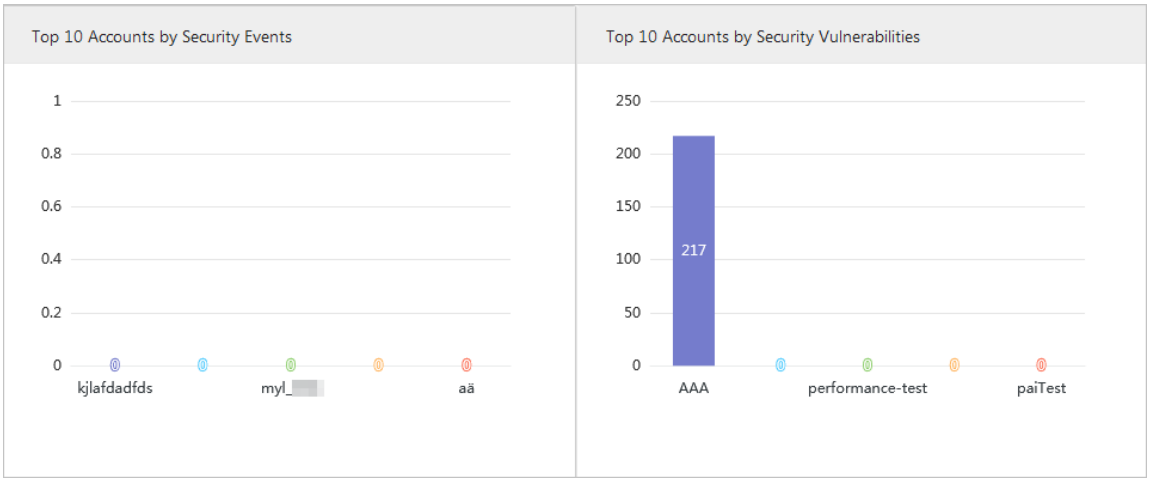


   - The third part displays the inbound and outbound network traffic for the previous 24 hours.

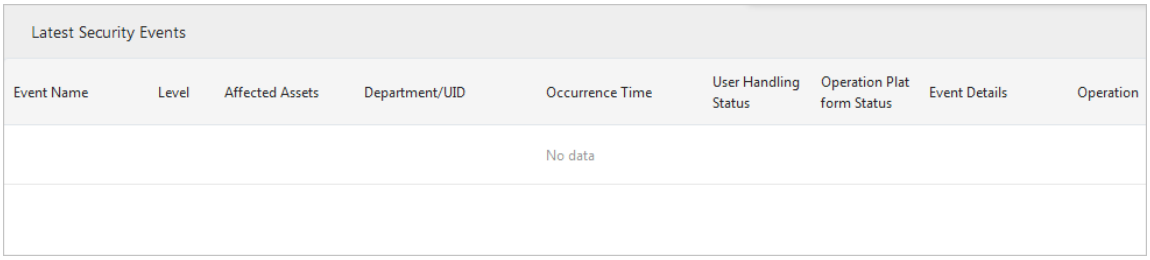


- The fourth part lists the five hosts with the most security events or vulnerabilities.

- The fifth part displays the 10 accounts with the most security events or vulnerabilities.



- The sixth part displays the information of the latest security events.



- You can move the mouse pointer to the information icon in the **Event Details** column for an event to view the details.
- You can click **Processed** or **Ignored** in the **Operation** column for an event to update the event status.

> **Note:**
> You can also select multiple events and click **Processed** or **Ignored** below the table to update the status of multiple events.

4.1.2 View User Dashboard

This topic describes how to view the overall security status of each department.

Context

User Dashboard displays the overall security status of a specified department. IT administrators can check the security threats and attacks on Apsara Stack and enhance the security of the most vulnerable servers.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **Dashboard** > **User Dashboard**.
3. Select a department from the drop-down list, and click **Search**.
4. View the overall security status of the specified department.
   - The first part on this dashboard displays the overview of security events related to the account, including security emergencies, urgent host vulnerabilities, system configuration security risks, and high-risk hosts.
   - The second part displays the security events and vulnerabilities for the previous 7 days.
   - The third part displays the event type distribution and vulnerability priority distribution.
   - The fourth part lists the five hosts with the most security events or vulnerabilities.
   - The fifth part displays the information of the latest security events.

- You can move the mouse pointer to the information icon in the **Event Details** column for an event to view the details.
- You can click **Processed** or **Ignored** in the **Operation** column for an event to update the event status.

> **Note:**
> You can also select multiple events and click **Processed** or **Ignored** below the table to update the status of multiple events.

4.2 User monitoring

4.2.1 Query security events

This topic describes how to view security events.

Context

The Security Event Query page displays the previous and ongoing security events. These events are detected and reported by Threat Detection Service or Server Guard. An Apsara Stack Security user can search for a security event to check the attack type and affected servers and handle the events.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Event Monitoring** > **Security Event Query**.
3. Set the search conditions and click **Search**.

Search condition	Description
Host IP	The IP address or name of the queried host. This is an optional condition that is used to query the events on a specific host.
Instance ID	The ID of the queried instance. This is an optional condition that is used to query the events of a specific instance ID.
User account	The department name or username. This is an optional condition that is used to query the events on all servers of a specific user.
Event type	The security event type. You can select all or some of the event types.

Search condition	Description
Emergency type (Server Guard)	You can select: • All • Critical-risk • High-risk • Medium-risk • Low-risk
Operation platform status	You can select from the following event handling statuses: • All • Pending • Processing • Processed • Ignored

4. Click the **Threat Detection Service** or**Server Guard** tab to view related security events.
   - You can move the mouse pointer to the information icon in the **Event Details** column for an event to view the details.
   - You can click **Processed** or **Ignored** in the **Operation** column for an event to update the event status.

     Note:
     You can also select multiple events and click **Processed** or **Ignored** below the table to update the status of multiple events.

4.2.2 Query security vulnerabilities

This topic describes how to view the security vulnerabilities.

Context

The Security Vulnerability Query page displays the information of security vulnerabilities on a server. By searching for the vulnerability information, an Apsara Stack Security user can check the affected servers and fix the vulnerabilities or take other measures to enhance server security.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Vulnerability Monitoring** > **Security Vulnerability Query**.

3. Set the search conditions and click **Search**.

Search condition	Description
Host IP	The IP address or name of the queried server. This is an optional condition that is used to query the vulnerabilities on a specific server.
Instance ID	The ID of the queried instance. This is an optional condition that is used to query the vulnerabilities of a specific instance ID.
User account	The department name or username. This is an optional condition that is used to query the vulnerabilities on all servers of a specific user.
Severity	You can select from the following vulnerability priorities: • All • Fix immediately • Fix later • Ignore
Operation platform status	You can select from the following vulnerability handling statuses: • All • Not fixed • Fixing • Fixed • Ignored

4. Click the **Linux Software Vulnerabilities** tab, the **Windows System Vulnerabilities** tab, the **Other Vulnerabilities** tab or the **Web CMS Vulnerabilities** tab to view related vulnerabilities.

   You can click **Processed** or **Ignored** in the **Operation** column for a vulnerability to update the vulnerability status.

   Note:
   You can also select multiple vulnerabilities and click **Processed** or **Ignored** below the table to update the status of multiple vulnerabilities.

4.2.3 Query network traffic

This topic describes how to query network traffic of a server.

Context

You can query the network traffic metrics, including the BPS, PPS, and QPS of the specified IP address, to check whether any exception occurs based on the network traffic trend within a specified period. By querying the network traffic information, you can check whether the current bandwidth resources meet the business requirements and whether your server are subjected to DDoS attacks.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Traffic Monitoring** > **Traffic Query**.
3. In the **Traffic Query** area, set the search conditions and click **Search**.

Parameter	Description
Region	The region to which the server belongs.
Query Type	IP: Query by IP address
IP	The IP address of the target server whose network traffic is to be queried.
Cycle	The query cycle. The query cycle and the query duration interact with each another.
Duration	The start time and end time for querying the network traffic.

4. View the network traffic information in the **Search Result** area.
   - **Traffic (bit/s)**: bits per second, which is specified as the sum of the inbound and outbound traffic rates.
   - **Packet (pps)**: packets per second, which is specified as the sum of the inbound and outbound packet rates.
   - **NewCon & QPS**: queries per second.

4.2.4 Query web protection status

This topic describes how to query the protection status of all websites in Apsara Stack.

Context

On the **WEB Protection Details** page, you can view the status of all websites protected by WAF in Apsara Stack.

Procedure

1. *Log on to Cloud Security Operations Center.*

2. Choose **Monitoring Center** > **WEB Security** > **WEB Protection Details**.
3. Optional: On the **Web Security Monitoring** tab page, set **Department** and **Domain Name** and click **Search** to quickly locate the specific website.
4. In the domain name list, view the protection status of each domain name.

Column name	Description
Domain Name	The domain name protected by WAF.
Department	The department to which the domain name belongs.
Protocol	The website protocol. HTTPS and HTTP are supported.
Source Address	The IP address of the origin site.
Protection Status	Whether the **Web Application Protection** feature is enabled.
Rule Application	The protection policy selected in **Web Application Protection**.
Malicious IP Penalty	Whether the **Malicious IP Penalty** feature is enabled.
CC Attack Protection	Whether the **CC Attack Protection** feature is enabled.
Precise Access Control	Whether the **Precise Access Control** feature is enabled.

4.2.5 Asset monitoring

4.2.5.1 Query asset security information

This topic describes how to query the asset security information.

Context

On the Overview page, you can query the asset security information of each ECS instance, including its basic information and whether Apsara Stack Security products are running on it. You can also view security events and security vulnerabilities of each server. By querying the asset security information, you can have a comprehensive view of the security status of the ECS instance and take necessary security measures accordingly.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Asset Monitoring** > **Overview**.
3. Enter the IP address of the server and click **Search**.
4. View the asset security information of the server.

Item	Description
Basic Information	Displays the basic information of the ECS instance, including the product name, instance ID, IP address type, and department.
Alibaba Cloud Security Information	Displays the running status of various Apsara Stack Security products.
Security information list	Displays the information of security events and security vulnerabilities on different tab pages. • **Threat Detection Service** tab page: Displays the list of security events detected by Threat Detection Service (TDS). • **Server Guard** tab page: Displays the list of security events detected by Server Guard. • **Linux Software Vulnerabilities** tab page: Displays the list of Linux security vulnerabilities detected by Server Guard. • **Windows System Vulnerabilities** tab page: Displays the list of Windows system vulnerabilities detected by Server Guard. • **Other Vulnerabilities** tab page: Displays the list of other vulnerabilities detected by Server Guard. • **Web-CMS Vulnerabilities** tab page: Displays the list of Web-CMS vulnerabilities detected by Server Guard.

4.2.5.2 View servers

This topic describes how to view the instance types, disks, and security groups of servers.

Context

On the ECS Instances page, you can view the instance types, disks, and security groups of all servers in Apsara Stack to manage them in a unified manner and locate problems quickly.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Asset Monitoring** > **ECS Instances**.
3. Click the **Instances** tab to view the instance information.
   - In the instance list, view the instance information.

     You can view the basic information, status, and security events of each instance.
   - View the instance details.

     Click **Details** for an instance in the **Operation** column. Then, view the instance details under **Security Events**, **Vulnerabilities**, **Disks**, **Snapshots**, and **Security Groups**.

- Export data.

  Click **Export Data** to save the instance information to your local disks.

4. Click the **Disks** tab to view the disk information.
   - In the disk list, view the basic information and status of each disk.
   - Export data.

     Click **Export Data** to save the disk information to your local disks.
5. Click the **Security Groups** tab to view the security group information.
   - In the security group list, view the basic information and the number of rules of each security group.
   - View the security group details.

     Click **Details** for a security group in the **Operation** column to view the instances and rules of the security group.
   - Export data.

     Click **Export Data** to save the security group information to your local disks.
   - Set the whitelist of ports that do not need to be detected.
     a. Click **Set Suspicious Rule**.
     b. In the **Set Suspicious Rule** dialog box, enter the ports that do not need to be listened on.

        To add multiple ports, separate ports with commas (,) or line breaks.

        Except the whitelisted ports, other ports that are open to `0.0.0.0/0` (indicating all IP addresses) are considered as suspicious.
     c. Click **OK**.

4.2.5.3 View RDS instances

This topic describes how to view the list of RDS instances in Apsara Stack and details of each RDS instance.

Context

On the RDS Instances page, you can view the information of all RDS instances in Apsara Stack to manage them in a unified manner and locate problems quickly.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Assets Monitoring** > **RDS Instances**.
3. Set the search condition, such as **Department**, **Region**, and **Time Range**, and click **Search**.
4. In the RDS instance list, view the information of the RDS instances.

   You can view the basic information, whitelist policy, and encryption information of each RDS instance.
5. Click **Details** for an RDS instance in the **Operation** column to view the basic information and whitelisted IP addresses of the RDS instance.
6. Click **Export Data** to export the RDS instance list to your local disks.

4.2.5.4 View OSS instances

This topic describes how to view the information of OSS instances in Apsara Stack.

Context

On the OSS Instances page, you can view the information of all OSS instances in Apsara Stack to manage them in a unified manner and locate problems quickly.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Assets Monitoring** > **OSS**.
3. Set the search condition, such as **Department**, **Region**, and **Time Range**, and click **Search**.
4. In the OSS instance list, view the information of the OSS instances.

   You can view the basic information, usage, and whitelist of each OSS instance.
5. Click **Export Data** to export the OSS instance list to your local disks.

4.2.5.5 View SLB instances

This topic describes how to view the information of SLB instances in Apsara Stack.

Context

On the SLB Instances page, you can view the information of all SLB instances in Apsara Stack to manage them in a unified manner and locate problems quickly.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Assets Monitoring** > **SLB Instances**.

3. Set the search condition, such as **Department**, **Region**, and **Time Range**, and click **Search**.
4. In the SLB instance list, view the information of the SLB instances.
5. Click **Export Data** to export the SLB instance list to your local disks.

4.2.5.6 View EIP instances

This topic describes how to view the information of EIP instances in Apsara Stack.

Context

On the Elastic IP Addresses page, you can view the information of all EIP instances in Apsara Stack to manage them in a unified manner and locate problems quickly.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Monitoring Center** > **User Monitoring** > **Assets Monitoring** > **Elastic IP Addresses**.
3. Set the search condition, such as **Department**, **Region**, and **Time Range**, and click **Search**.
4. In the EIP instance list, view the information of the EIP instances.
5. Click **Export Data** to export the EIP instance list to your local disks.

5 Services

5.1 Traffic monitoring and management

5.1.1 Manage the detection threshold list

5.1.1.1 Add a traffic protection policy

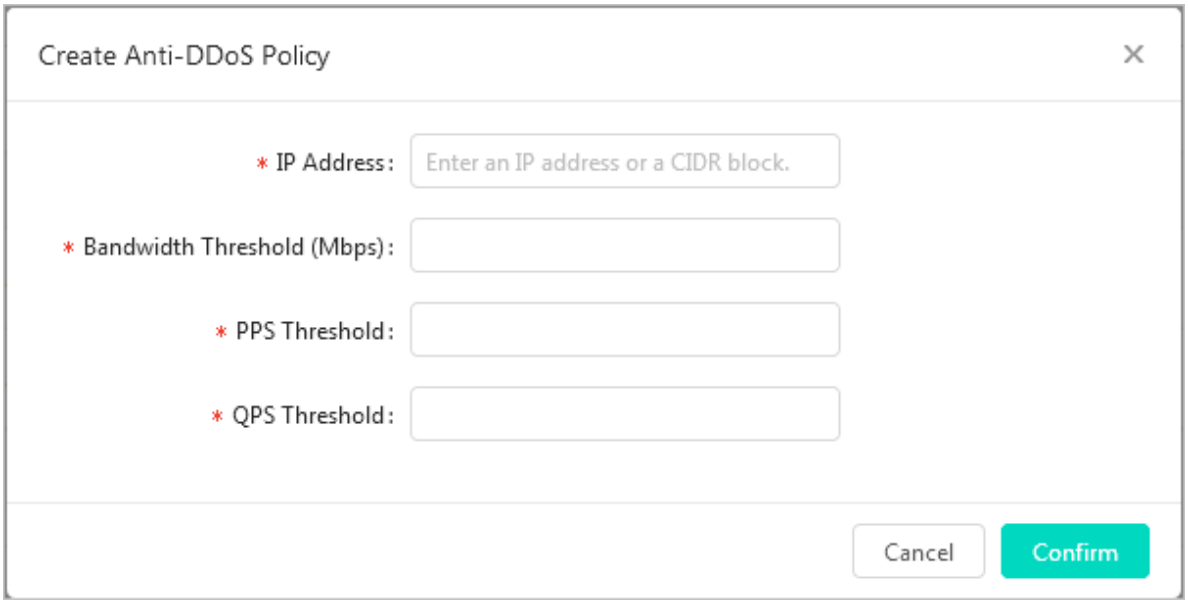
This topic describes how to add a traffic protection policy to set the traffic rate threshold, threshold number of packets per second, and threshold number of HTTP requests per second for an IP address.

Context

When any of the metrics reaches the threshold, the system generates an alert. In addition, if the DDoS traffic scrubbing module has been deployed in Apsara Stack, the traffic is routed to the DDoS traffic scrubbing device for scrubbing.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Traffic Monitoring** > **Alarm Thresholds**.
3. Click **Create Anti-DDos Rule**.
4. In the **Create Anti-DDos Rule** dialog box that appears, set the rule parameters.



5. Click **OK**.

5.1.1.2 Manage traffic protection policies

This topic describes how to view, modify, and delete the traffic protection policies that have been configured.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose**Services** > **Traffic Monitoring** > **Alarm Thresholds**. In the threshold list, you can view the protection policies that have been configured.
3. Modify a protection policy.
   a) In the threshold list, select the protection policy to be modified and click **Modify**.
   b) In the **Modify Anti-DDoS Rule** dialog box, modify the policy parameters.
   c) Click **OK**.
4. Delete a protection policy.

   Select the protection policy to be deleted and click **Delete**. In the dialog box that appears, click **OK**.

5.1.2 Configure traffic collection

5.1.2.1 Set a traffic collection CIDR block

This topic describes how to add and view a CIDR block to be monitored by the traffic security monitoring module of Apsara Stack Security.

Context

The security administrator can change or delete a monitored CIDR block as needed. A monitored CIDR block is valid only for a data center that is deployed in the region to which the CIDR block belongs.

Note:

If you set the same CIDR block on the traffic collection CIDR block setting page and region setting page, ensure that the CIDR block belongs to the same region.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Traffic Monitoring** > **Traffic Collection Settings**.

3. On the **Traffic Collection IP Range** tab page, view the traffic collection CIDR blocks that have been set.
4. Click **Add**.
5. In the **Enter Network Segment** dialog box that appears, set the traffic collection CIDR block and region.

   You must enter a valid CIDR block. You cannot set a CIDR block that already exists in the system.
6. Click **OK**.

   The new CIDR block is displayed in the CIDR block list.

What's next

You can click **Modify** or **Delete** in the **Operation** column to modify or delete a CIDR block.

5.1.2.2 Set a region

This topic describes how to add a CIDR block protected by Server Guard.

Context

When the Server Guard client installed on a server belonging to the specified region and CIDR block reports logon information to the Server Guard server, the Server Guard server automatically detects the data center where the server is located.

 **Note:**

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Traffic Monitoring** > **Traffic Collection Settings**.
3. On the **Region** tab page, view the list of regions that have been set.
4. Click **Add**.
5. In the **Enter Network Segment** dialog box that appears, set the CIDR block and region.

   You must enter a valid CIDR block. You cannot set a CIDR block that already exists in the system.
6. Click **OK**.

   The new region is displayed in the region list.

What's next

You can click **Modify** or **Delete** in the **Operation** column to change or delete a region.

5.1.2.3 Set a whitelist

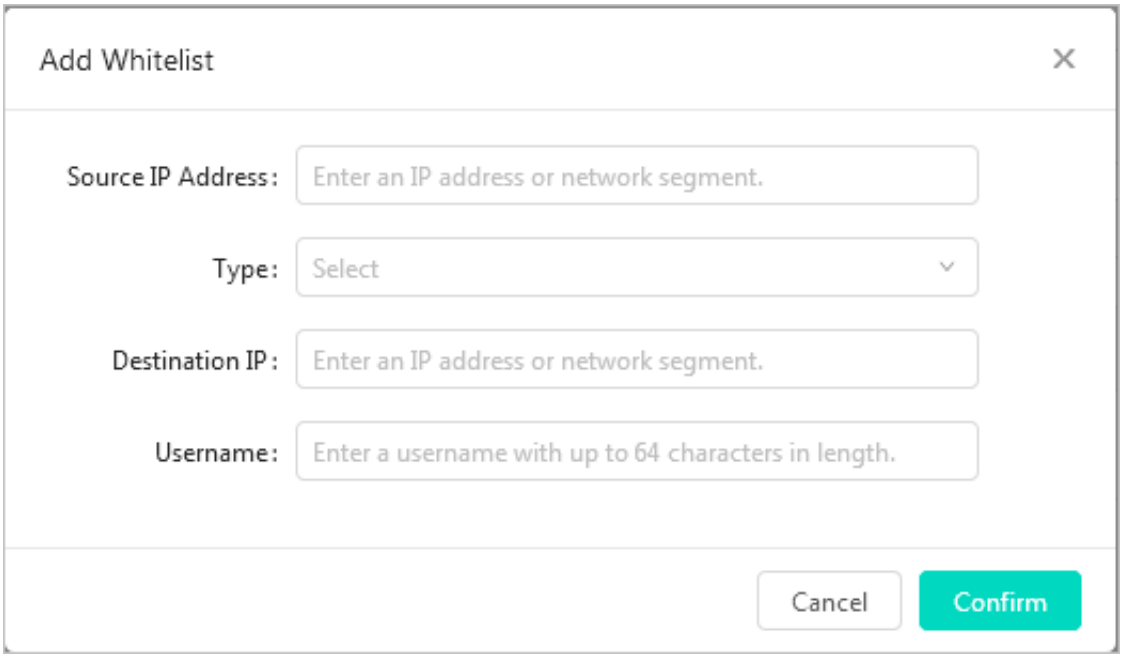
This topic describes how to whitelist WAF origin IP addresses and IP addresses that are exempt from brute-force attack detection or Web application attack detection.

Context

When scanning for various suspicious attacks, Apsara Stack Security permits the traffic from the IP addresses in the whitelist.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Traffic Monitoring** > **Traffic Collection Settings**.
3. Click **Whitelist Settings** and view the whitelists that have been configured.
4. Click **Add**.
5. In the **Add Whitelist** dialog box that appears, set the parameters to add a whitelist.



Parameter	Description
Source IP Address	The source IP address or CIDR block.
Destination IP	The destination IP address or CIDR block.
Username	The name of the user for adding the whitelist.
Type	• `BWAF Whitelist`: The traffic from the IP addresses in the whitelist is permitted.

Parameter	Description
	• `Brute-Force Attack Whitelist`: Logon requests from the IP addresses in the whitelist are not detected as brute-force attacks. • `Application Attack Whitelist`: The traffic from the IP addresses in the whitelist is not detected as suspicious web application attack traffic.

6. Click **OK**.

   The new whitelist is displayed in the list of whitelists.

What's next

You can click **Delete** in the **Operation** column to delete a whitelist.

5.1.3 Enable attack blocking

This topic describes how to enable the brute-force attack blocking and web-based attack blocking features.

Context

If the **Brute-force Attack Blocking** and **Web-based Attack Blocking** functions are disabled, the system only provides the alerting feature. After the two functions are enabled, the system can block any brute-force attacks or web-based attacks to ensure the security of Apsara Stack.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Traffic Monitoring** > **Attack Blocking Details**.
3. In the **Brute-force Attack Blocking** column and the **Web-based Attack Blocking** column, click the **on/off** toggle to enable the blocking functions.

   When the **on/off** toggle for a blocking feature is displayed as 

in green, this feature is enabled.

   You can enable or disable the blocking functions by clicking the **on/off** toggle. To ensure the security of Apsara Stack, we recommend that you enable the blocking functions.

5.2 Anti-DDoS management

5.2.1 Manage the DDoS console

5.2.1.1 Set the traffic scrubbing threshold for a single IP address

This topic describes how to view and set the traffic scrubbing threshold for a single IP address.

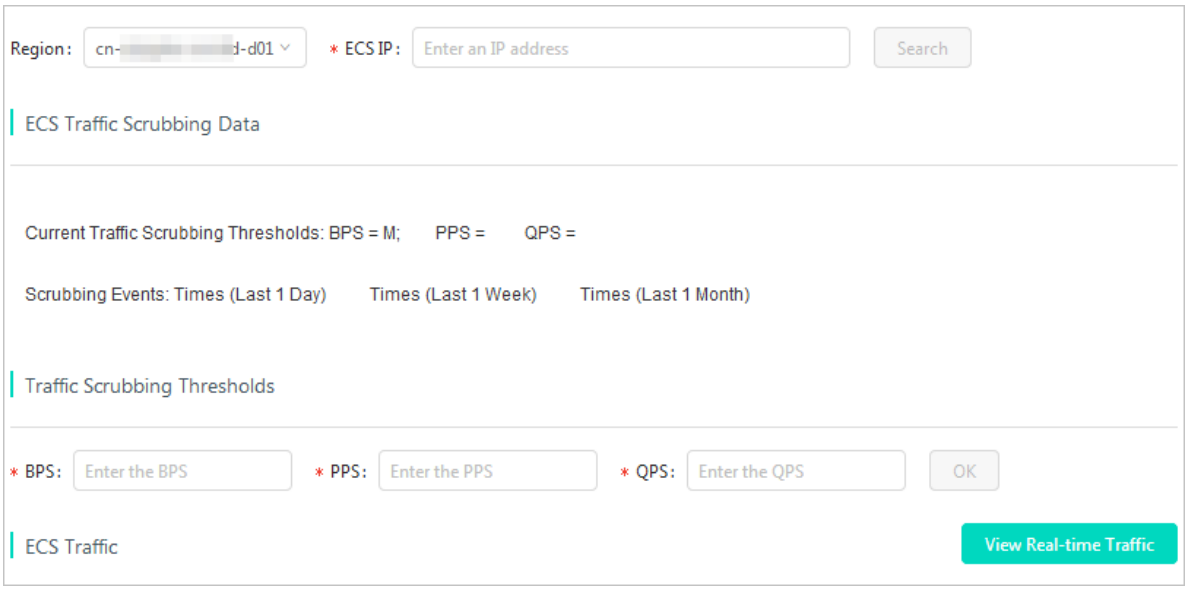
Context

Once the traffic flowing into a server with a specified IP address exceeds the preset traffic scrubbing threshold, the system automatically scrubs the traffic based on the configured traffic scrubbing policy. The system scrubs the unusual traffic until the network traffic falls below the scrubbing threshold.

Note:
You can also set the traffic scrubbing threshold by referring to *Add a traffic protection policy*.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Anti-DDoS** > **Console**.
3. In the **Scrubbing Policies** area, click **Query and Set Thresholds**.
4. Set the IP address of the server and the traffic scrubbing threshold.



Parameter		Description
Search	Region	The region to which the server belongs.
	ECS IP	The IP address of the server.
ECS Traffic Scrubbing Data		The current traffic scrubbing threshold and scrubbing events for the IP address of the server.

Parameter	Description
Traffic Scrubbing Thresholds	The traffic scrubbing threshold configured for the IP address. If the inbound traffic of the IP address exceeds the threshold, the system automatically scrubs the traffic until the traffic falls below the threshold. • BPS: bits per second, which is specified as the sum of the inbound and outbound traffic rates. • PPS: packets per second, which is specified as the sum of the inbound and outbound packet rates. • QPS: queries per second.

Note:

By entering the IP address of the server and clicking **Search**, you can view the scrubbing threshold configured for the IP address and the scrubbing events in the **ECS Traffic Scrubbing Data** area. You can also view the traffic of the IP address in the **ECS Traffic** area.

5. Click **OK**.

5.2.1.2 Set the traffic scrubbing threshold for multiple IP addresses

This topic describes how to set the traffic scrubbing threshold for multiple IP addresses.

Context

Once the traffic flowing into a server with a specified IP address exceeds the preset traffic scrubbing threshold, the system automatically scrubs the traffic based on the configured traffic scrubbing policy. The system scrubs the unusual traffic until the network traffic falls below the scrubbing threshold.

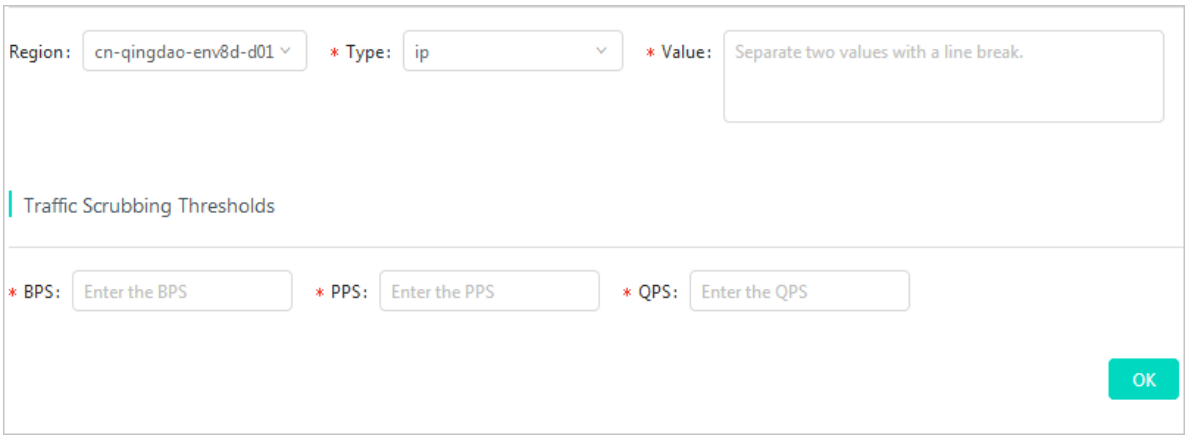
Note:

You can also set the traffic scrubbing threshold by referring to *Add a traffic protection policy*.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Anti-DDoS** > **Console**.
3. In the **Scrubbing Policies** area, click **Set Thresholds**.

4. Set the traffic scrubbing threshold.



Parameter		Description
Search	Region	The region to which the server belongs.
	Type	The condition used to filter servers. Here, IP is used.
	Value	The IP address of the server. If the IP addresses of multiple servers are set, enter each IP address in a separate line.
Traffic Scrubbing Thresholds		The traffic scrubbing threshold configured for the IP address. If the inbound traffic of the IP address exceeds the threshold, the system automatically scrubs the traffic until the traffic falls below the threshold. • BPS: bits per second, which is specified as the sum of the inbound and outbound traffic rates. • PPS: packets per second, which is specified as the sum of the inbound and outbound packet rates. • QPS: queries per second.

5. Click **OK**.

5.2.1.3 Customize a traffic scrubbing policy

To reduce the chance of incorrect traffic scrubbing, you can customize a traffic scrubbing policy, allowing the system to analyze attacks based on the actual situations and scrub unusual traffic accordingly.

Context

When detecting that the traffic exceeds the preset traffic scrubbing threshold, the system analyzes the traffic composition based on the traffic scrubbing policy. If the traffic matches a rule in the traffic scrubbing policy, the system determines whether the traffic is DDoS traffic or normal traffic and permits normal traffic or blocks DDoS traffic.

In **Version Information**, you can view the version number, creator, creation time, and version description of an advanced rule.

You can also click **Previous Versions** to view the historical versions of an advanced rule.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Anti-DDoS** > **Console**.
3. In the **Scrubbing Policies** area, click **Advanced Rules**.
4. In **Rule Content**, configure an advanced rule for the traffic scrubbing policy.

Note:

For the online help of rule configuration, click **Rule Format**.

- **Rule format**

  You can configure multiple sub-rules in an advanced rule, with each sub-rule in the following format:

```
id=int
note=string
cmd=string
rule=short
```

Parameter	Type	Required	Description
id	int	Required	The unique identifier for the DDoS rule.
note	string	Optional	The description of the DDoS rule.
cmd	string	Required	Whether the traffic is identified as DDoS traffic or normal traffic after it matches the DDoS rule. The options are ddos and normal.
rule	short	Required	The DDoS matching formula.

- **Notes**

An advanced rule must end with the following configuration and a blank line:

```
id=900
note=checksum
cmd=normal
rule=(2)>(1)
```

- **Rule matching formula**

  A rule matching formula supports basic arithmetic operations and logical expressions.

  - Logical expression: Basic expression + Logical operator + Basic expression
  - Basic expression: (Elementary arithmetic) + (Relational operator) + (Elementary arithmetic)
  - Logical operators: || and &&
  - Relational operators: >=, >, <=, <, ==, and ! =

  Pay attention to the following when configuring a rule matching formula:

  - Custom variables are supported in elementary arithmetic operations.
  - All operations use integer computation.
  - Division by zero is supported and yields 0x7FFFFFFF.
  - All expressions enclosed in parentheses can be prioritized in computation.
  - Each basic expression must contain a relational operator.

  The internal variables of a rule matching formula are as follows:

Internal variable	Description
sync	The number of new connections.
synack	The number of the SYN/ACK packets.
qps	The number of HTTP queries per second.
rqps	The number of responses sent by the server for the HTTP queries per second.
finrst	The number of FIN and RST packets.
dns	The number of DNS packets.
udpr	The number of packets from a high-risk UDP port.
udpu	The number of UDP unicast packets.
icmp	The number of ping packets.
ack	The number of HTTP ACK packets.

Internal variable	Description
bps	The packet size in Mbit.
pps	The number of packets.
tbps	The BPS threshold in Mbit.
tpps	The PPS threshold.
tqps	The QPS threshold.
tnewcon	The threshold for the number of new connections.
flowmax	The maximum sample value of the traffic.
flowall	The total sample value of the traffic.
product	The product to which the IP address belongs: — 1: ECS — 2: OSS

5. Click **Submit**.

5.2.1.4 Manually scrub traffic

In addition to configuring a protection policy to trigger an automatic traffic scrubbing, you can manually scrub the traffic of an IP address or cancel the scrubbing.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Anti-DDoS** > **Console**.
3. Manually scrub traffic.
   a) In the **Traffic Scrubbing Operations** area, enter the server information.

Parameter	Description
Region	The region to which the server belongs.
Traffic Scrubbing	The IP address of the server.

> **Note:**
> You can click **Query Traffic** to view the network traffic of the server.

   b) Click **Add**.
4. Stop traffic scrubbing.

If the unusual network traffic of a server whose traffic is being scrubbed is not caused by DDoS attacks, for example, an activity or a promotion is held on the official website, you can manually cancel the traffic scrubbing.

a) Click **Query Traffic Scrubbing Tasks** and record the IP address in the list.
b) In the **Traffic Scrubbing Operations** area, specify the server for which traffic scrubbing needs to be cancelled.
c) Click **Cancel** .

5.2.2 Manage DDoS events

This topic describes how to query DDoS events, analyze the traffic related to the DDoS events, and specify whether to cancel traffic scrubbing for the DDoS events as required.

Context

DDoS events include events triggered by the traffic protection policy and events generated by manual traffic scrubbing.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **Anti-DDoS** > **Events**.
3. Set the search criteria and click **Search** to query anti-DDoS events.

   The following table lists the search conditions.

Parameter	Description
Region	The region to which the server belongs.
IP address	The IP address of the server.
Trigger	The reason why traffic scrubbing is triggered, namely, the variable that exceeds the preconfigured threshold.
Status	The scrubbing status. • All • Scrubbing • Scrubbed
Duration	The time range in which the anti-DDoS event is triggered.

4. View the anti-DDoS events in **Search Result**.

Note:

You can click **Export** to export the anti-DDoS events.

You can perform the following operations for an anti-DDoS event:

- Click **Cancel** to cancel traffic scrubbing for the anti-DDoS event.

  Traffic scrubbing can be cancelled in the following scenarios:

  — The unusual network traffic was not caused by DDoS attacks.

  — The traffic scrubbing brings a severe impact on normal business accesses.
- Click **Traffic Analysis** to view the distribution of protocols used in DDoS attacks and the IP addresses of the top 10 servers that suffer the most DDoS attacks.
- Click **View Traffic**. On the *Traffic Query* page, view the traffic of the IP address.

5.3 WAF management

5.3.1 Manage domain names

This topic describes how to modify and delete domain names in WAF.

Context

On the **Domain Names** page, maintenance engineers can view the overall WAF information, such as the protected websites, status of WAF features, and rule groups in use. Maintenance engineers can also modify and delete each domain name.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose**Services** > **WAF Management** > **Domain Names**.
3. View the domain name-related information.

Column name	Description
Domain Name	The domain name.
Protocol	The web protocol type: • htttp • https
Port Number	The communication port: • htttp: 80 • htttps: 443
UID	The UID.

Column name	Description
IP	The IP address of the domain name.
WAF Status	Whether the WAF feature is enabled for the domain name.
CC Attack Protection	Whether the CC attack protection is enabled for the domain name.
ACL Status	Whether ACL is enabled for the domain name.
Rule Group	The rule group applicable to WAF. For more information, see *Manage rule groups*.

4. Select the target domain name, and click **Modify** to modify the domain name or click **Delete** to delete it.

5.3.2 Rules

5.3.2.1 Manage rules

This topic describes how to view and modify rules.

Context

A protection rule consists of multiple rule conditions, including the attack types and HTTP methods, and protection modes. A rule group consists of multiple rules and is used for domain name protection in WAF.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **WAF Management** > **Rules**.
3. Click the **Rule Group** tab and view the rule details in the list.

Column name	Description
Rule ID	The unique ID of the rule.
Rule Name	The custom name of the rule.
Protection Mode	The protection mode of the rule: • `Block`: blocks attacks. • `Observe`: detects attacks but does not block the attacks.
Attack Type	The type of web attacks detected by the rule.
Method	The HTTP method to which the rule takes effect.

4. Click **Modify** for the target rule to modify the rule information.

5.3.2.2 Manage rule groups

This topic describes how to modify rule groups.

Context

A rule group contains multiple rules. Rule groups are used for the domain name protection in WAF .

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **WAF Management** > **Rules**.
3. Click the **Rule Groups** tab to view the rule groups.
4. Select the target rule group and click **Modify**.
5. Select the check boxes in the **Select** column for the applicable rules.
6. Click **Save**.

5.3.2.3 Publish a rule

This topic describes how to publish a rule.

Context

After a rule is modified, you can perform this operation for the rule to take effect. After the rule list has taken effect, WAF blocks attacks based on the new rule.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Services** > **WAF Management** > **Rules**.
3. Click the **Rule Releases** tab and click **Release**.

6 Tasks

6.1 Add operation logs

This topic describes how to add an operation log in the Tasks module.

Context

After performing an operation in Cloud Security Operations Center, the IT administrator can add an operation log on the **Operation Logs** page.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Tasks** > **Operation Logs**.
3. Click the **Operation Logs** tab.
4. Enter the operation log in the textbox.
   - We recommend that you enter the error, cause, solution, and result for future analysis.
   - You can click **Upload Attachment** to upload files related to this operation.
5. Click **Save**.

6.2 View the operation calendar

This topic describes how to view the operation calendar and operation logs.

Context

After adding operation logs, the IT administrator can review the logs on the **Operation Calendar** tab page.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Tasks** > **Operation Logs**.
3. Click the **Operation Calendar** tab.
4. Specify the year and the month to view the operation logs of the specified month.
5. Click a day on the calendar. You can view the operation logs added on the specified day in **Previous Logs**.
   - To search for a log, you can enter a keyword in the search box and click **Search**.
   - To modify a log, you can click the Modify button on the right.

- To delete a log, you can click the Delete button on the right.

7 Reports

7.1 Create a report task

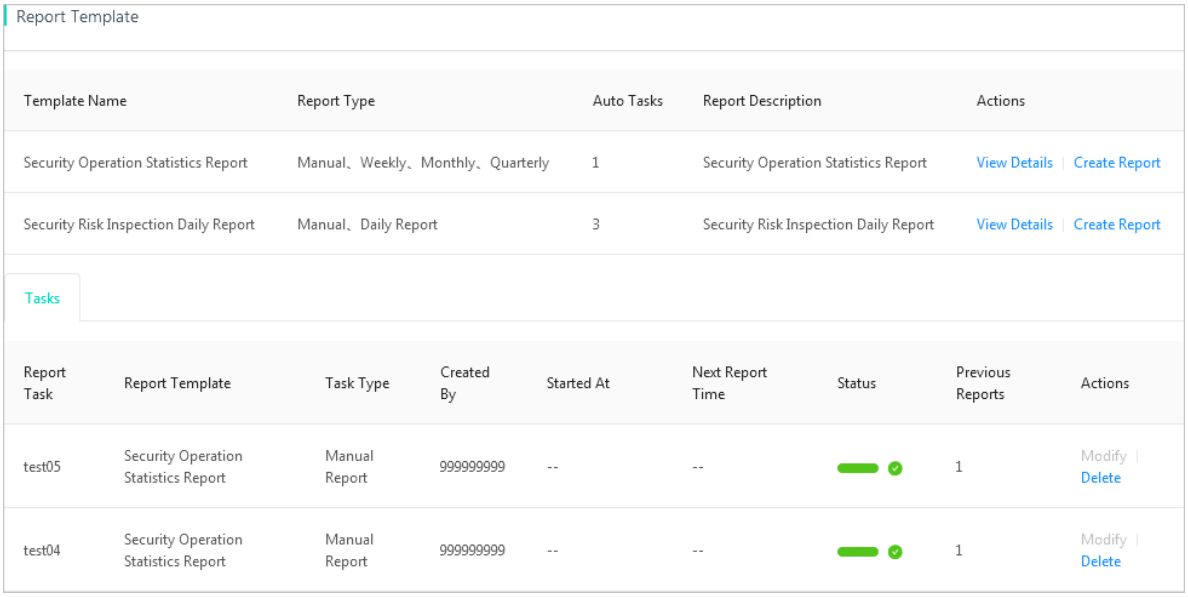
This topic describes how to create a report task using a report template.

Context

You can use report templates to create report tasks on security operation statistics or security risk inspection. Then the system generates statistical reports to help IT administrators analyze the security status of Apsara Stack and detect security issues.

Procedure

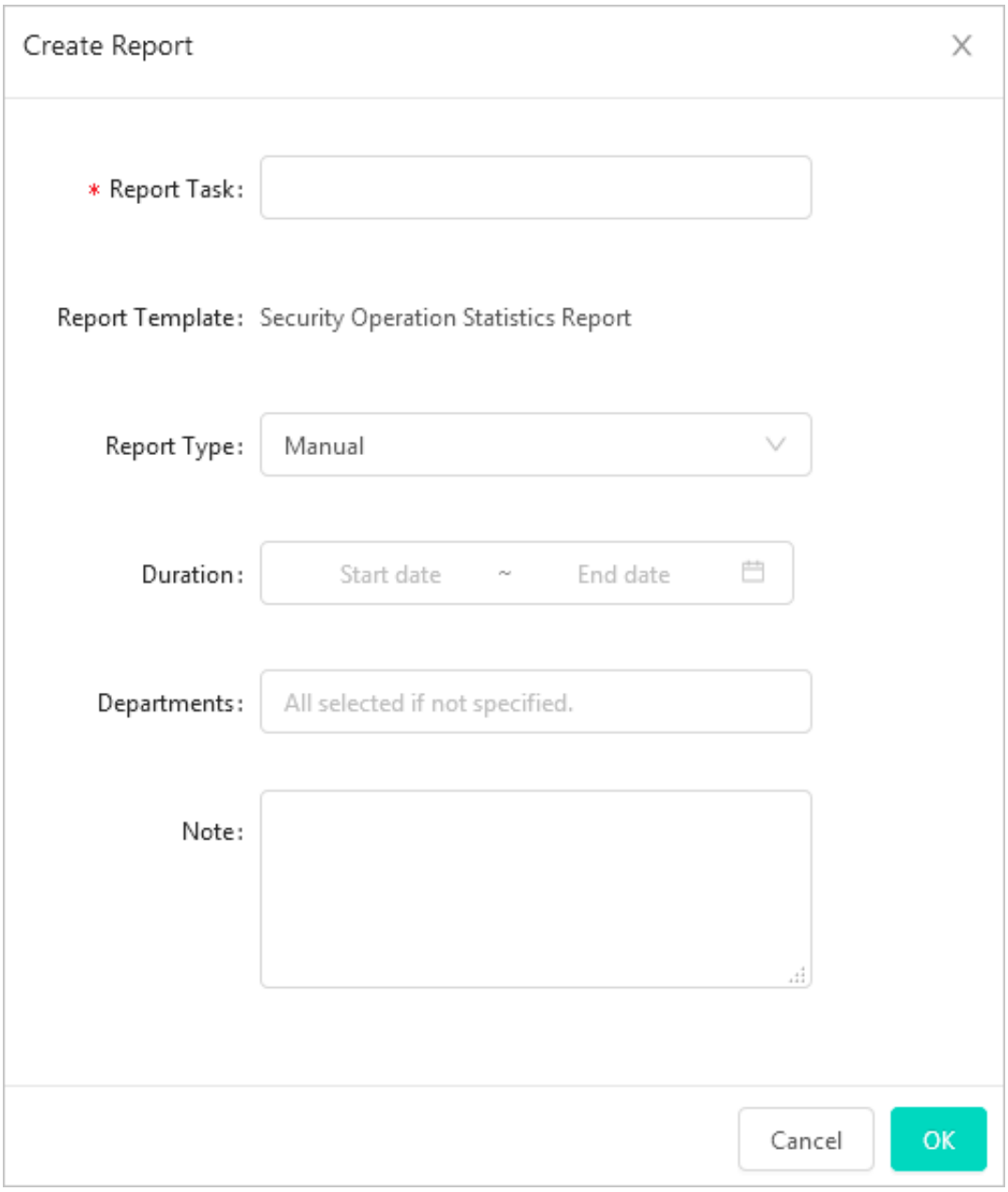
1. *Log on to Cloud Security Operations Center.*
2. Choose **Reports** > **Report Template**.



3. In the **Actions** column of a report template, click **Create Report**.

   You can click **View Details** to view the created report tasks in **Tasks**.

4. In the **Create Report** dialog box, specify the task parameters.



You can specify **Report Type** as `Manual` or `Auto`.

- `Manual`: A report is generated right after a report task is created.
- `Auto`: After a report task is created, reports are generated periodically based on the specified period.

5. Click **OK**.

   You can check the new task in **Tasks**.

   - To modify a report task, click **Modify** in the **Actions** column of a task.
   - To delete a report task, click **Delete** in the **Actions** column of a task.

7.2 View reports

This topic describes how to view reports.

Context

IT administrators can periodically view the reports to learn the overall security status of Apsara Stack and detect security issues.

Procedure

1. *Log on to Cloud Security Operations Center.*
2. Choose **Reports** > **Reports**.
3. Specify the year and the month to view the reports of the specified month.
4. Click a day on the calendar to view the report tasks on this day.

   To search for a report task, enter a keyword in the **Search Reports** search box, and click **Search**.
5. In the **Actions** column of a report task, click **View** to view the report details.

   Note:
   You can click **Delete** to delete a report.