ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

Apsara Stack Security

User Guide

Product Version: v3.16.2

Document Version: 20220916

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is Apsara Stack Security

Apsara Stack Security is a solution that provides a full suite of security features, such as network, server, application, data, and security management to protect Apsara Stack assets.

Background information

Traditional security solutions for IT services use hardware products such as firewalls and intrusion prevention systems (IPSs) to detect attacks on network perimeters and protect networks against attacks.

Cloud computing features low costs, on-demand flexible configuration, and high resource utilization. As cloud computing develops, an increasing number of enterprises and organizations use cloud computing services instead of traditional IT services. Cloud computing environments do not have definite network perimeters. As a result, traditional security solutions cannot effectively safeguard cloud assets.

With the powerful data analysis capabilities and professional security operations team of Alibaba Cloud, Apsara Stack Security provides integrated security protection services for networks, applications, and servers.

Complete security solution

Security domain	Service name	Description
Security management	Threat Detection Service	Monitors traffic and overall security status to audit and centrally manage assets.
	Cloud Security Scanner	Uses AI technologies to help enterprises identify security risks at the earliest opportunity.
	Security Operations Center (SOC)	Manages the overall security operations of the cloud environment. You can build a closed-loop security operations system that features risk prediction and discovery, defense control, detection and analysis, and response management. SOC is a cloud-native solution.
Server security	Server Guard	Protects Elastic Compute Service (ECS) instances against intrusions and malicious code.
	Server Security	Protects physical servers against intrusions.
	Container Protection	Protects containers and runtime environments against intrusions.
Application security	Web Application Firewall (WAF)	Protects web applications against attacks and ensures that mobile and PC users can securely access web applications over the Internet.
Network security	Anti-DDoS	Ensures the availability of network links and improves business continuity.

Security domain	Service name	Description
	Network Detection and Response	Detects and responds to network attacks at the Internet border and internal network border based on a variety of threat detection engines and threat intelligence data.
Data security	Sensitive Data Discovery and Protection (SDDP)	Prevents data leaks and helps your business system meet compliance requirements.
O&M audit	Security Audit	Summarizes and analyzes logs so that security auditors can detect and eliminate risks in time.
Security O&M service	On-premises security service	Helps you establish and optimize the cloud security system to protect your business system against attacks by using security features of Apsara Stack Security and other Apsara Stack services.

2.Usage notes

Before you log on to Apsara Stack Security Center, you must verify that your computer meets the configuration requirements.

For more information about the configuration requirements, see .

Configuration requirements

Item	Requirement
Browser	• Internet Explorer: V11 or later • Google Chrome (recommended): V42.0.0 or later • Mozilla Firefox: V30 or later • Safari: V9.0.2 or later • GmSSL browser that runs the Chrome kernel: V69.0.0 or later
Operating system	• Windows XP • Windows 7 or later • macOS

3.Quick start

3.1. User roles and permissions

This topic describes the user roles involved in Apsara Stack Security.

All roles in Apsara Stack Security Center are provided by default. You cannot create custom roles. Before you log on to Apsara Stack Security Center, make sure that your account is assigned the required role. For more information, see .

Default roles in Apsara Stack Security

Role name	Description
System administrator of Apsara Stack Security Center	Manages and configures system settings for Apsara Stack Security Center. The system administrator has permissions to manage Apsara Stack accounts, synchronize data, configure alerts, and configure global settings.
Security administrator of Apsara Stack Security Center	Monitors the security status across Apsara Stack and configures security policies for each functional module of Apsara Stack Security. The security administrator has permissions on all features under Threat Detection, Network Security, Application Security, Server Security, Physical Server Security, and Asset Management. **Note** The permissions on Web Application Firewall (WAF) must be separately granted.
Department security administrator	Monitors the security status of cloud resources in a specific department and configures security policies for each functional module of Apsara Stack Security for this department. The department security administrator has permissions on all features under Threat Detection, Network Security, Application Security, Server Security, Physical Server Security, and Asset Management. In addition, the department security administrator can specify alert notification methods and alert contacts in the department. **Note** The permissions on WAF must be separately assigned.
Auditor of Apsara Stack Security Center	Conducts security audits across Apsara Stack. The auditor can view audit events and raw logs, configure audit policies, and access all features under Security Audit.

If you do not have an account that assumes the required role, contact the administrator to create an account and assign the role to the account. For more information, see the **Create a user** topic in *Apsara Uni-manager Management Console User Guide*.

3.2. Log on to Apsara Stack Security Center

This topic describes how to log on to Apsara Stack Security Center.

Prerequisites

.

- Before you log on to the Apsara Uni-manager Management Console, the endpoint of the console is obtained from the deployment staff.
- We recommend that you use Google Chrome.

Procedure

1. Enter the URL of the Apsara Uni-manager Management Console in the address bar and press the Enter key.
2. Enter your username and password.

   Obtain the username and password that you use to log on to the Apsara Uni-manager Management Console from the operations administrator.

   > **Note** The first time that you log on to the Apsara Uni-manager Management Console, you must change the password of your account. For security purposes, your password must meet the minimum complexity requirements. The password must be 10 to 32 characters in length and must contain at least two of the following character types:
   >
   > - Uppercase or lowercase letters
   > - Digits
   > - Special characters, including exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%)

3. Click **Log On**.
4. If your account has multi-factor authentication (MFA) enabled, perform corresponding operations in the following scenarios:
   - You log on to the Apsara Uni-manager Management Console for the first time after MFA is enabled by the administrator:
     a. On the Bind Virtual MFA Device page, bind an MFA device.
     b. Enter the username and password again as in Step 2 and click **Log On**.
     c. Enter a six-digit MFA verification code and click **Authenticate**.
   - You have enabled MFA and bound an MFA device:

     Enter a six-digit MFA verification code and click **Authenticate**.

     > **Note** For more information, see the *Bind a virtual MFA device to enable MFA* topic in *Apsara Uni-manager Management Console User Guide*.

5. In the top navigation bar, choose **Security > Alibaba Cloud Security**.
6. On the **Apsara Stack Security Center** page, select a value for **Region**.
7. Click **Access with Authorized Role** to access Apsara Stack Security Center.

4.Threat Detection Service

4.1. Overview

This topic introduces the basic concepts related to Threat Detection Service (TDS).

TDS provides comprehensive protection for enterprises. It can monitor vulnerabilities, intrusions, web attacks, DDoS attacks, threat intelligence, and public opinions. TDS uses modeling and analysis to obtain key information based on traffic characteristics, host behavior, and host operation logs. In addition, TDS identifies intrusions that cannot be detected by traffic inspection or file scan. You can use the input of cloud analysis models and intelligence data to discover sources and behavior of attacks and assess threats.

TDS provides the following features:

- Overview: provides a security situation overview and information about security screens.
- Security Alerts: displays security alerts that occur in your business system.
- Attack Analysis: displays application attacks and brute-force attacks that occur in your system.
- Cloud Service Check: checks whether risks exist in the configurations of Apsara Stack services.
- Application Whitelist: allows you to create and apply application whitelist policies to your servers that require special protection. After you create the policies, Apsara Stack Security identifies trusted, suspicious, and malicious programs based on intelligent learning. This prevents unauthorized programs from running.
- Assets: manages servers and cloud services on Apsara Stack.
- Security Reports: allows you to configure security report tasks on Apsara Stack.

4.2. Security overview

4.2.1. View security overview information

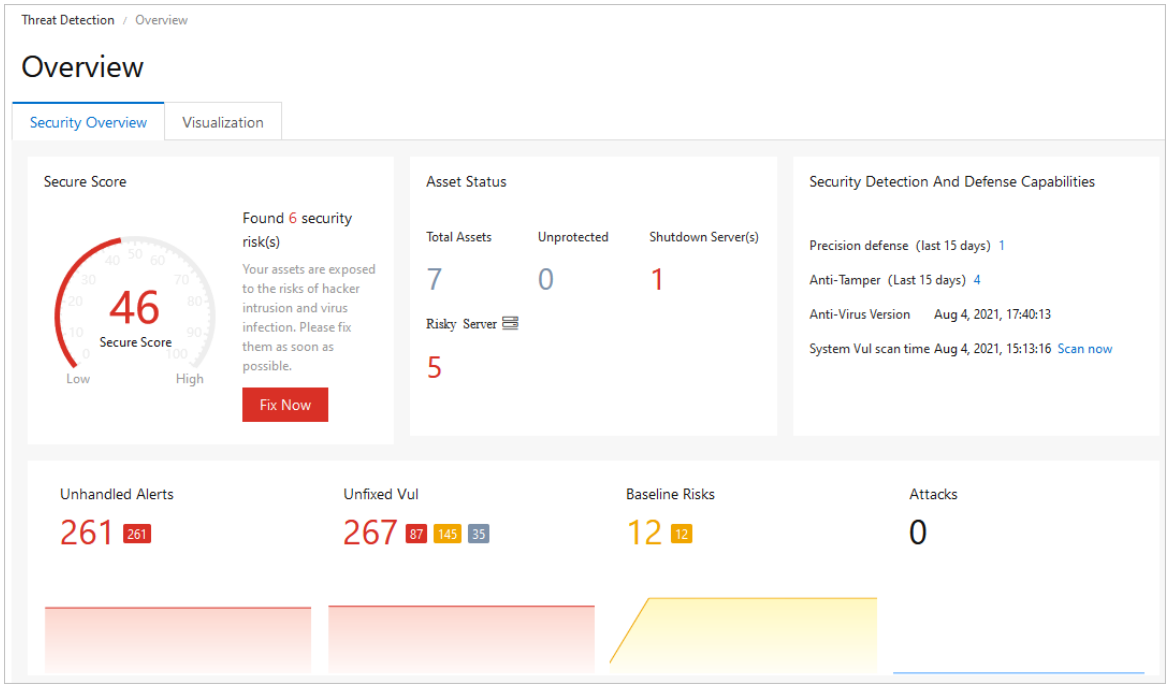
This topic describes how to view security statistics, attack trends, and network traffic information on the Apsara Stack platform.

Context

The **Security Overview** tab provides an overview of detected security events, the latest threats, and inherent vulnerabilities of the system. A security administrator can view information on the **Security Overview** tab to better understand the security posture of the system.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Overview**.
4. On the **Security Overview** tab, view the security posture of the Apsara Stack platform.



Sections on the Security Overview tab

Section	Description
Secure Score	The security score of assets and the number of detected security risks.
Asset Status	The total number of assets and the numbers of servers that are not protected, servers that are stopped, and servers that are at risk.
Security Detection And Defense Capabilities	The numbers of precise defense events and anti-tampering events over the last 15 days, the time when the antivirus database was last updated, and the time when vulnerability scanning was last performed. This allows you to obtain the defense situation and security status of your assets in real time.
Threat statistics	The numbers of alerts that are not handled, vulnerabilities that are not fixed, baseline risks, and attacks.
Configuration Assessment Risks	The risks in the baseline configurations of cloud services.
Issue Resolved	Statistics on alerts, vulnerabilities, and baseline risks that have been processed over the last 15 days. The statistics are displayed in a bar and trend chart.

4.3. Security alerts

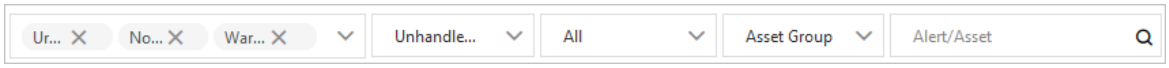
4.3.1. View security alerts

This topic describes how to view security alerts on the Security Alerts page.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Security Alerts**.
4. (Optional)Specify filter conditions to search for security alerts.

   > **Note** If you want to view all alerts, do not specify the conditions.

Filter condition	Description
Alert level	The alert level. You can select one or more levels. Valid values: ○ Urgent ○ Warning ○ Notice
Alert status	The alert status. Valid values: ○ Unhandled Alerts ○ Handled
Alert type	The alert type. Select **All** or a specific type.
Affected asset group	The affected asset group. Select **Asset Group** or a specific group.
Alert name or asset keyword	The alert name or the keywords of affected assets.

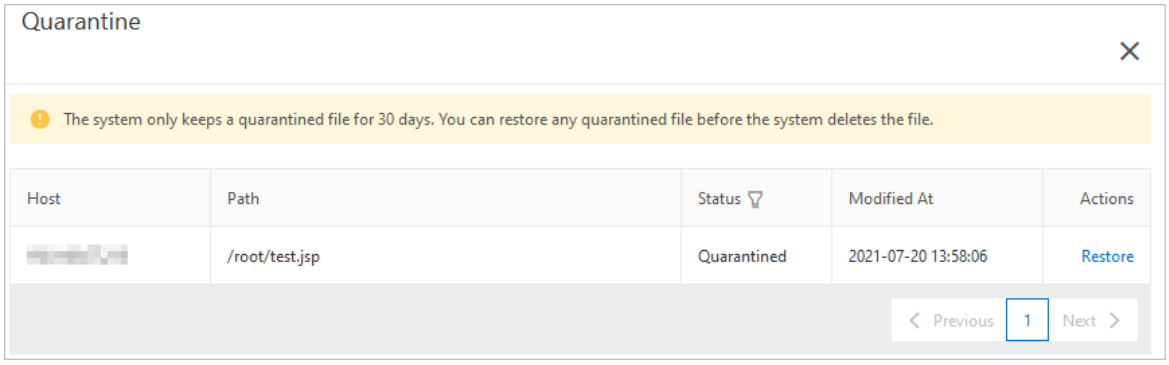
5. View security alerts and their details in the alert list.

4.3.2. Manage quarantined files

This topic describes how to manage threat files that are quarantined by the system. The system deletes a quarantined file 30 days after the file is quarantined. You can restore the file before it is deleted.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Security Alerts**.
4. In the upper-right corner of the **Alerts** page, click **Quarantine**.
5. In the **Quarantine** panel, view the information about a quarantined file, such as the IP address of the host, path, status, and operation time.



6. (Optional)If a file is incorrectly quarantined, click **Restore** in the **Actions** column to restore the file.

   > **Notice** Before you restore a quarantined file, make sure that the file is normal and does not bring risks.

   The restored file is removed from the Quarantine panel and is displayed in the security alert list again.

4.3.3. Configure security alerts

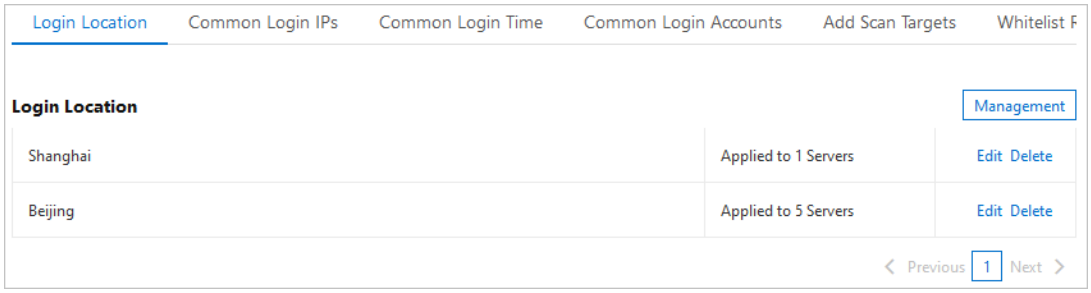
This topic describes how to configure security alerts, which allow you to specify approved logon locations and web directories to scan.

Procedure

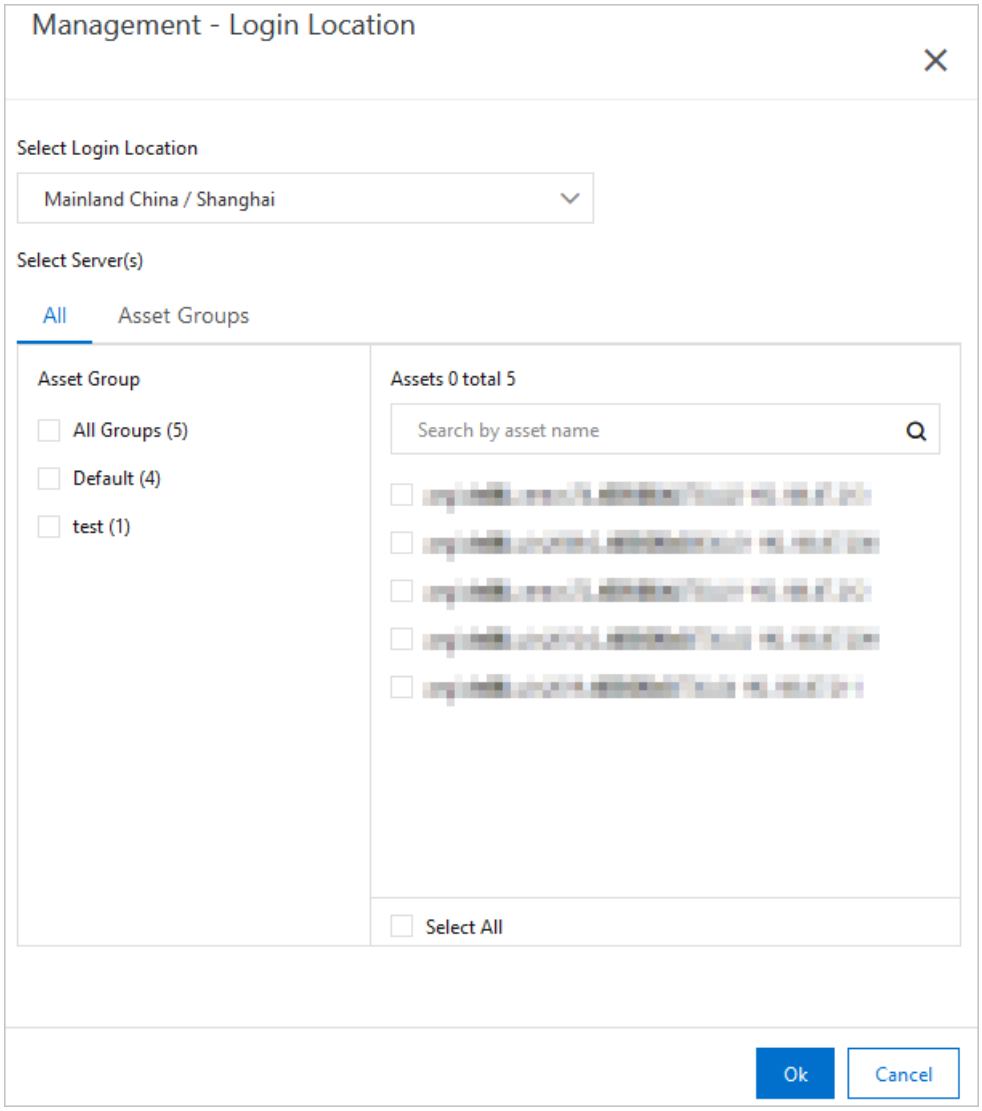
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Security Alerts**.
4. In the upper-right corner of the **Alerts** page, click **Settings**.

   In the **Settings** panel, you can perform the following operations:

   - **Add an approved logon location**
     a. Click **Management** to the right of **Login Location**.



b. In the **Management - Login Location** panel, select the logon location that you want to add and select the servers that allow logons from the added location.



c. Click **Ok**.

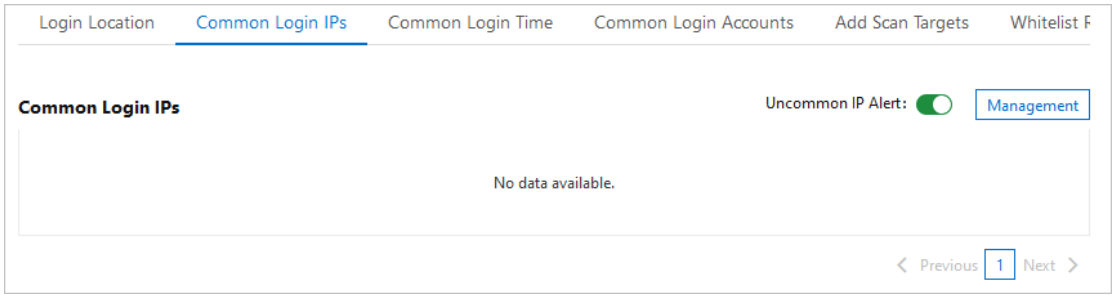
Threat Detection Service (TDS) allows you to **edit** and **delete** added logon locations.

- Find the required logon location and click **Edit** on the right to change the servers that allow logons from this location.
- Find the required logon location and click **Delete** on the right to delete the logon location.

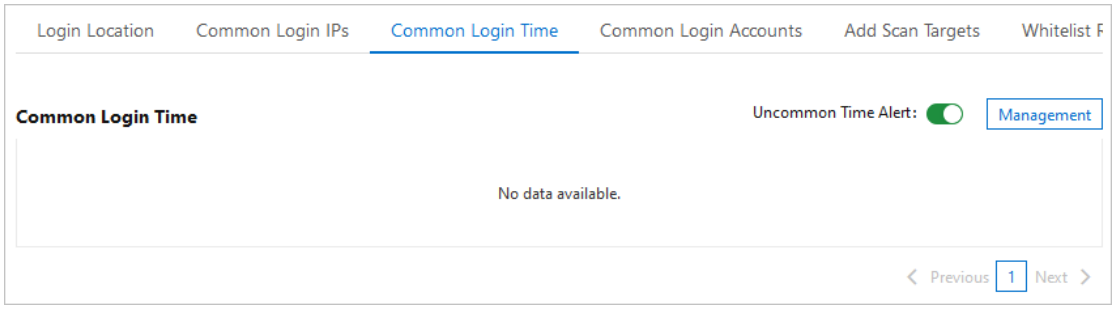
- **Configure advanced logon settings**

> **Note** When you configure advanced logon settings, you can specify the IP addresses, accounts, and time ranges that are allowed for logons to your assets. After you configure these settings, alerts are triggered if your assets receive logon requests that do not meet the requirements. The procedure to configure advanced logon settings is similar to that to configure **approved logon locations**. You can follow the preceding procedure to **add**, **edit**, or **delete** advanced logon settings.

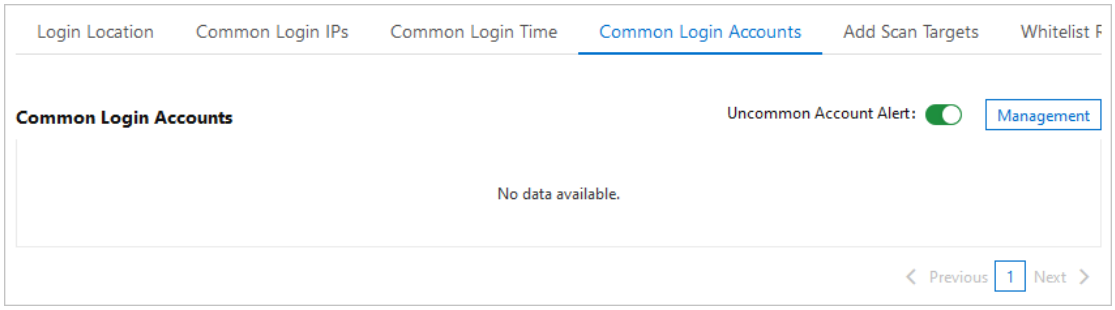
- On the right of **Common Login IPs**, turn on or off Uncommon IP Alert. After the switch is turned on, alerts are triggered if your assets receive logon requests from unapproved IP addresses.



- On the right of **Common Login Time**, turn on or off Uncommon Time Alert. After the switch is turned on, alerts are triggered if your assets receive logon requests at unapproved time.

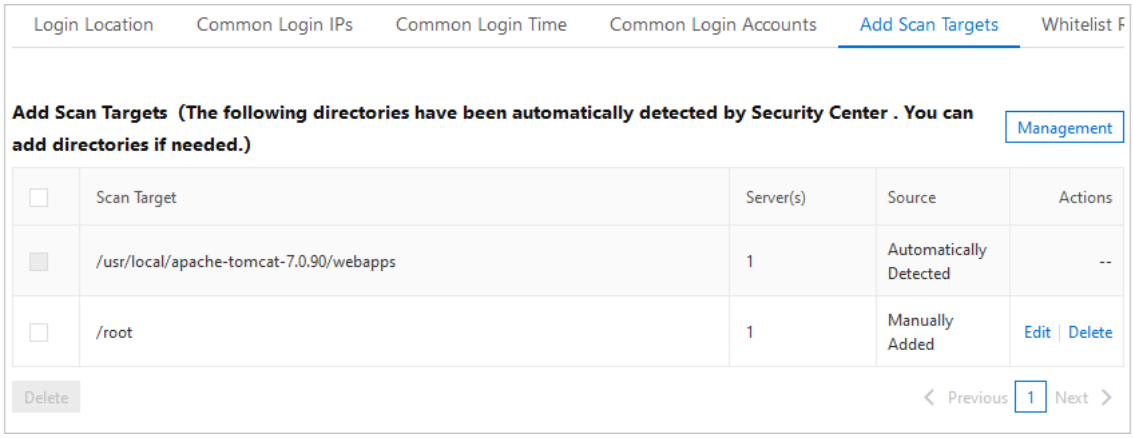


- On the right of **Common Login Accounts**, turn on or off Uncommon Account Alert. After the switch is turned on, alerts are triggered if your assets receive logon requests from unapproved accounts.



- **Add a web directory to scan**

Apsara Stack Security automatically scans web directories of your servers and runs dynamic and static scan tasks. You can also manually add other web directories of your servers.



a. On the right of **Add Scan Targets**, click **Management**.

b. Enter a valid web directory and select the servers on which the directory is scanned. The web directory is added to the scan list.

> **Note** Root directories are not allowed. This ensures performance and efficiency.

c. Click **Ok**.

4.4. Attack analysis

This topic describes the statistics provided by the attack analysis feature. The statistics include the total number of attacks, distribution of attack types, top five attack sources, top five attacked assets, and an attack list.

Background information

The attack analysis feature provides basic attack detection and prevention capabilities in Apsara Stack Security Center. We recommend that you optimize firewalls and enhance business security to develop a more fine-grained and in-depth defense system.

On the **Attack Awareness** page, you can specify a time range to view these attack details. You can view the attack analysis statistics of the current day, last 7 days, or last 15 days. You can also set Time Range to **Custom** to view the statistics of a time range within the last 30 days.

- **Attacks**: the total number of attacks detected in your assets within a specified time range.
- **Attack Type Distribution**: the attack types and the number of attacks for each type.
- **Top 5 Attack Sources**: the top five IP addresses from which the most attacks are launched.
- **Top 5 Attack Assets**: the top five assets that are attacked the most frequently.
- **Attack list**: the details about each attack. The details include the attack time, source IP address, attacked asset, attack type, and total number of attacks.

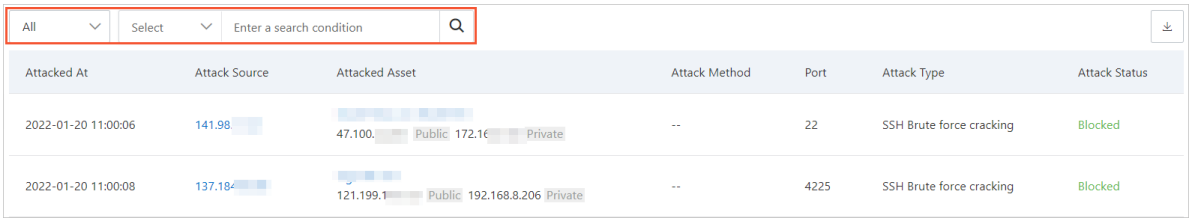
> **Note** The attack list displays a maximum of 10,000 attacks. You can specify **Time Range** to view details about the attacks that occur over the specified time range.

Parameters in the attack list

Parameter	Description
Attacked At	The time at which an attack occurs.
Attack Source	The source IP address of an attack.
Attacked Asset	The name, public IP address, and private IP address of an attacked asset.
Attacks	The total number of times that an attack is launched.
Attack Type	The type of an attack. The types of attacks that can be detected include SSH brute-force attacks and remote code execution attacks.

- Search for an attack.

  To search for an attack and view the details about the attack, specify search conditions above the attack list. Search conditions include the attack type, attacked asset, source IP address, and port number.



- View the details of an attacked asset.

  To view the details about an attacked asset, move the pointer over the name of the attacked asset.

- Export the attack list.

  To export and save the attack list to your computer, click the icon in the upper-left corner above the attack list. The attack list is exported to an Excel file.

4.5. Cloud service check

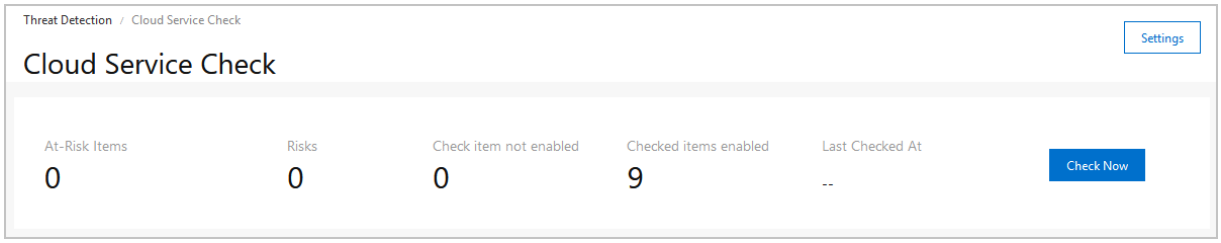
4.5.1. Overview

Threat Detection Service (TDS) provides the cloud service check feature. This feature allows you to check for the configuration risks of your Apsara Stack services. This topic describes the features and check items that are supported by the cloud service check feature.

Background information

The cloud service check feature allows you to perform network access control and data security checks. The checks help you detect configuration risks of your Apsara Stack services and provide repair solutions.

You can view the number of **Checked items enabled** on the **Cloud Service Check** page.



Cloud service check list

The following table describes the check items.

Type	Supported item	Description
	PolarDB - Backup configurations	Checks whether the automatic backup feature is enabled for PolarDB. Regular backups help you improve database security. You can restore data if an error occurs in your database. PolarDB supports automatic backup. We recommend that you enable automatic backup to create a backup on a daily basis.
	Container Registry - Repository permission configurations	Checks whether a Container Registry repository is set to private. Container Registry supports public and private repositories. Public repositories allow users to anonymously download images over the Internet. If images in a repository contain sensitive information, we recommend that you set the repository to private. If images in a repository do not contain sensitive information, ignore related alerts.
	OSS - Server-side encryption	Checks whether the data encryption feature is enabled for Object Storage Service (OSS) buckets. OSS supports server-side encryption to secure data that is persistently stored in OSS. We recommend that you enable server-side encryption to protect sensitive data.
	OSS - Sensitive information leakage scans	Checks whether access permissions on sensitive files in OSS buckets are required.
	ApsaraDB RDS - Cross-region backup configurations	Checks whether the cross-region backup feature is enabled for ApsaraDB RDS instances. ApsaraDB RDS for MySQL provides the cross-region backup feature that automatically synchronizes local backup files to OSS buckets in another region. This implements geo-disaster recovery. We recommend that you enable the cross-region backup feature.
	KVStore for Redis - Backup configurations	Checks whether the data backup feature is enabled for KVStore for Redis instances.

Type	Supported item	Description
Data security	ApsaraDB for MongoDB - SSL encryption	Checks whether SSL encryption is enabled for ApsaraDB for MongoDB databases. We recommend that you enable the SSL encryption feature to improve the security of data links in ApsaraDB for MongoDB databases.
	ApsaraDB for MongoDB - Backup configurations	Checks whether the automatic backup feature is enabled for ApsaraDB for MongoDB databases. Regular backups help you improve database security. You can restore data if an error occurs in your database. ApsaraDB for MongoDB provides automatic backup policies. We recommend that you enable automatic backup to create a backup on a daily basis.
	ECS - Disk encryption	Checks whether encryption is enabled for disks on Elastic Compute Service (ECS) instances.
	ECS - Automatic snapshot policies	Checks whether the automatic snapshot feature is enabled for the disks on ECS instances. The automatic snapshot feature improves the security of ECS instances and supports disaster recovery.
	OSS - Bucket permissions	Checks whether the OSS bucket ACL is set to *private*.
	OSS - Logging	Checks whether the logging feature is enabled for OSS.
	OSS - Cross-region replication	Checks whether the cross-region replication feature is enabled for OSS.
	ApsaraDB RDS - Database security policies	Checks whether the SQL audit, SSL encrypted transmission, and transparent database encryption features are enabled for ApsaraDB RDS databases.
	ApsaraDB RDS - Backup configurations	Checks whether the data backup feature is enabled for ApsaraDB RDS instances.
	SSL Certificates Service - Expiration check	Checks whether your SSL certificate expires. If your SSL certificate expires, you are not allowed to use SSL Certificates Service.
	ECS - Security group policies	Checks the security group policies of ECS. We recommend that you grant permissions to users based on the principle of least privilege. We also recommend that you specify 0.0.0.0/0 only for the ports that must be open to all services, such as port 80, 443, 22, or 3389.
	OSS - Bucket hotlink protection	Checks whether the hotlink protection feature is enabled for OSS buckets. The OSS hotlink protection feature checks the Referer header to deny access from unauthorized users. We recommend that you enable this feature.

Type	Supported item	Description
Network access control	VPC - DNAT rules	Checks whether a port is open to the Internet. When you create a DNAT rule for a NAT gateway that is deployed in a virtual private cloud (VPC), we recommend that you do not open internal management ports to the Internet. Do not open all ports or an important port, for example, ports 22, 3389, 1433, or 3306, to the Internet.
	Apsara Stack Security - Back-to-origin configuration for Anti-DDoS	Checks whether Anti-DDoS is configured to allow the requests from only Web Application Firewall (WAF) back-to-origin IP addresses. After you set up Anti-DDoS or WAF, you must hide the IP addresses of the backend servers to prevent attacks on the cloud assets.
	Apsara Stack Security - WAF back-to-origin configurations	Checks whether WAF allows requests from only WAF back-to-origin IP addresses. After you set up Anti-DDoS or WAF, you must hide the IP addresses of the backend servers to prevent attacks on the cloud assets.
	SLB - IP address whitelist configurations	Checks the access control configurations of Server Load Balancer (SLB) instances. Checks whether access control is enabled for HTTP and HTTPS services and checks whether 0.0.0.0/0 is added to the IP address whitelist.
	SLB - Open ports	Checks whether SLB opens ports to the Internet for forwarding unnecessary public services.
	ApsaraDB RDS - IP address whitelist configurations	Checks whether a whitelist is configured for ApsaraDB RDS and whether the whitelist contains 0.0.0.0/0. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.
	KVStore for Redis - IP address whitelist configurations	Checks whether a whitelist is configured for KVStore for Redis and whether the whitelist contains 0.0.0.0/0. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.
	AnalyticDB for PostgreSQL - IP address whitelist configurations	Checks whether a whitelist is configured for AnalyticDB for PostgreSQL and whether the whitelist contains 0.0.0.0/0. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.
	PolarDB - IP address whitelist configurations	Checks whether a whitelist is configured for PolarDB and whether the whitelist contains `0.0.0.0/0`. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.

Type	Supported item	Description
	ApsaraDB for MongoDB - IP address whitelist configurations	Checks whether a whitelist is configured for ApsaraDB for MongoDB and whether the whitelist contains `0.0.0.0/0`. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.

4.5.2. Run cloud service checks

Threat Detection Service (TDS) provides the cloud service check feature. This feature allows you to check for security risks in the configurations of your cloud services. This topic describes how to manually run cloud service checks on your cloud services. This topic also describes how to specify a detection interval for periodic automatic checks.

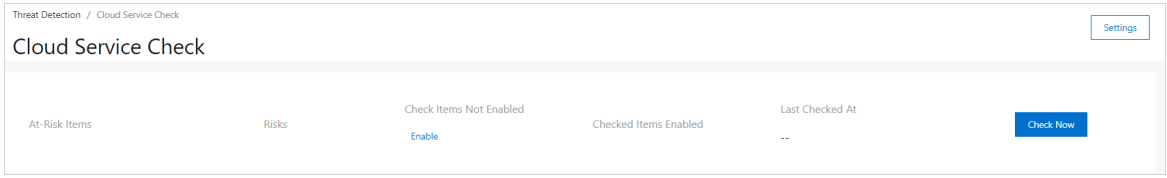
Context

Apsara Stack Security supports manual checks and periodic automatic checks to scan for security risks in the configurations of cloud services.

- Manual checks: On the **Cloud Service Check** page, you can click **Check Now** to check for security risks in the configurations of your cloud services.
- Periodic automatic checks: By default, Apsara Stack Security automatically runs checks during the time range `00:00 - 06:00` every other day. You can also customize a time range for periodic automatic checks. This way, you can detect and handle the security risks in the configurations of your cloud services at the earliest opportunity.

Manual checks

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Cloud Service Check**.
4. On the **Cloud Service Check** page, click **Check Now** to check whether the configurations of all your cloud services contain risks and the number of affected assets.



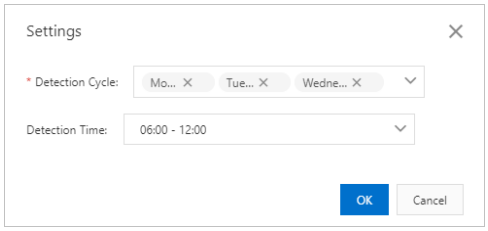
> **Note** Do not perform other operations until the check is complete.

After the check is complete, the detected risks are listed based on risk severities in descending order.

Automatic checks

1. Log on to Apsara Stack Security Center.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Cloud Service Check**.
4. In the upper-right corner of the **Cloud Platform Configuration Assessment** page, click **Settings**.
5. In the **Settings** dialog box, configure the **Detection Cycle** and **Detection Time** parameters.



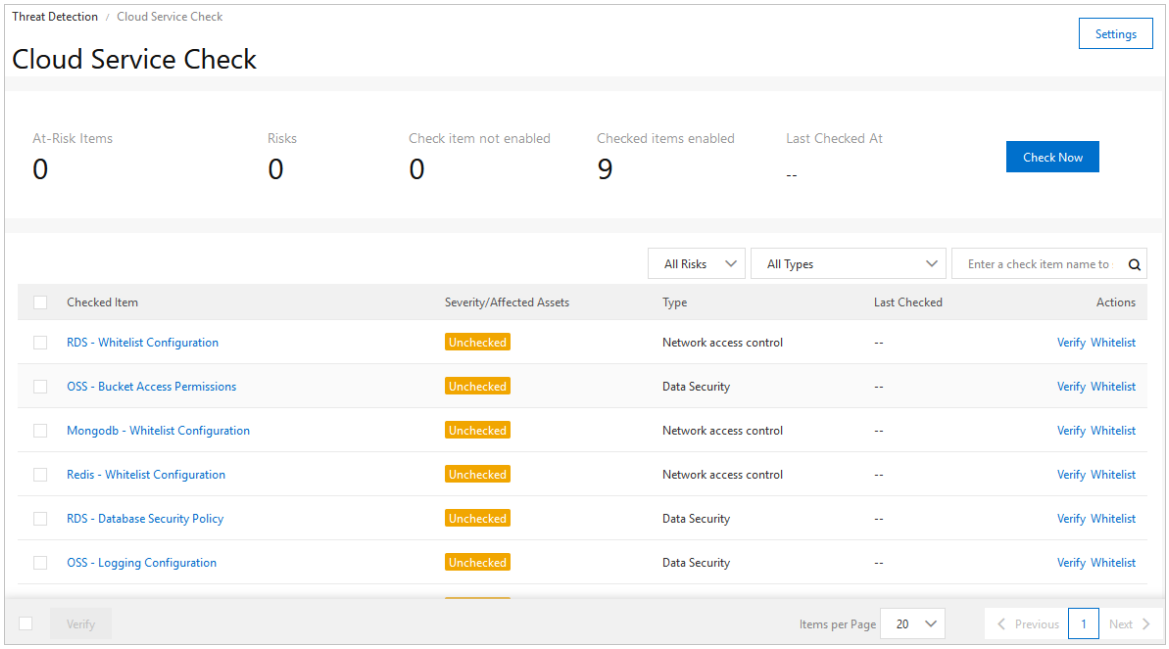
   - **Detection Cycle**: Valid values are Monday to Sunday. You can select multiple values.
   - **Detection Time**: Valid values are `24:00 - 06:00`, `06:00 - 12:00`, `12:00 - 18:00`, and `18:00 - 24:00`. You can select only one time range.
6. Click **Ok**.
   During the selected time range, Apsara Stack Security automatically runs checks based on all check items.

4.5.3. View the check results of configuration assessment for your cloud services and handle the detected risks

This topic describes how to view the check results of configuration assessment for your cloud services and handle the detected configuration risks in Apsara Stack Security. You can view the check items, details of check items, potential impacts caused by the detected configuration risks, and suggestions on how to handle the detected configuration risks. You can handle the detected configuration risks on the Cloud Service Check page in a centralized manner.

View check results

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Cloud Service Check**.
4. On the **Cloud Service Check** page, view the details of check results.



- **View the statistics of the last check**

  You can view the total number of at-risk items and the numbers of risks at different levels in the **At-Risk Items** section, and the number of assets on which risks are detected in the **Risks** section. You can also view the number of disabled check items in the Check Items Not Enabled section, the number of enabled check items in the Checked Items Enabled section, and the time when the check was last performed in the Last Checked At section.

- **View check items**

  You can view the information about the check items in the check item list. The information includes the risk severities of check items, the number of affected assets, the types of affected assets, the types of check items, and the time when the check was last performed.

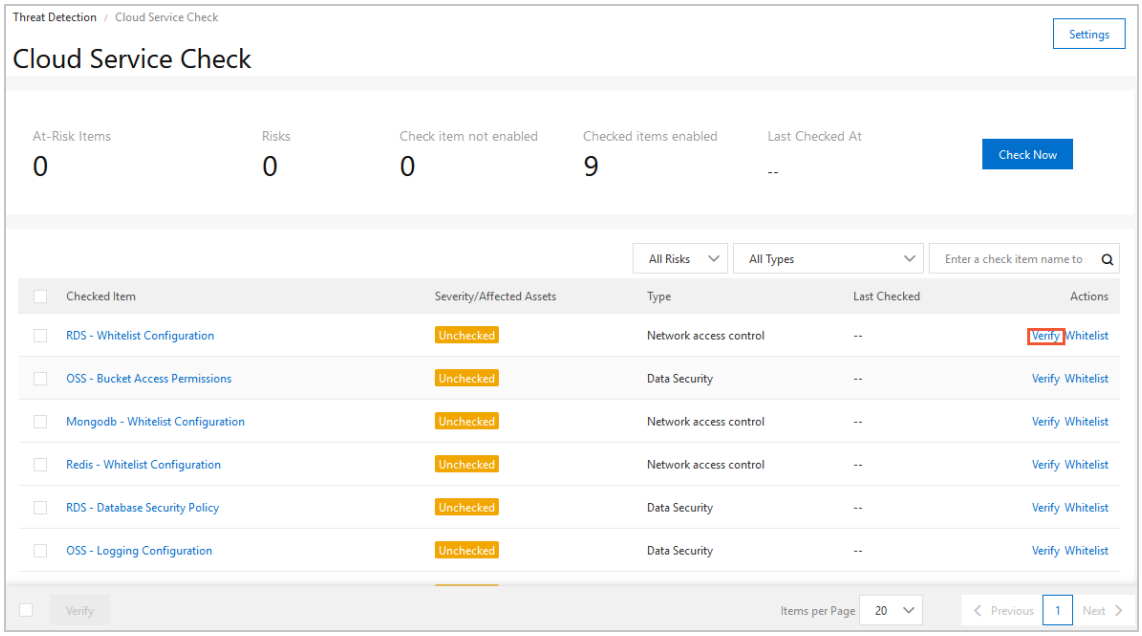
- **View the details of check results**

  You can click the name of a check item in the **Checked Item** column to go to the panel that displays the details of the check item. In the panel, you can view the description of the check item, potential impacts caused by the detected risks, and suggestions on how to handle the risks.

Handle the detected configuration risks of your cloud services

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Cloud Service Check**.
4. On the **Cloud Service Check** page, handle the configuration risks detected on your cloud services.
   - **Verify the configurations after modification**

If you have modified the configurations for which risks are detected, find the check item in the check item list and click **Verify** in the Actions column to check whether the new configurations are at risk.



- **Add check items to a whitelist**

  If you trust a check item for which risks are detected, find the check item in the check item list and click **Whitelist** in the Actions column to add the check item to a whitelist. Then, the state of the check item is displayed as **Ignored** in the Severity/Affected Assets column. **Ignored** check items are not counted in the total number of at-risk items in the **At-Risk Items** section.

  In the check item list, you can click **Remove** to remove the ignored check items from the whitelist.

  > Note After you add a check item to the whitelist, the risk that is detected for the check item is ignored only for this time. If the risk is detected again, Apsara Stack Security still displays the check result of this check item.

4.6. Assets

4.6.1. View the security status of a server

The Assets page displays security information about each protected server. The information includes the virtual private could (VPC) where each server resides, server status, and risk status. This topic describes how to search for specific servers and view the security status of these servers. This topic also describes how to specify search conditions and select the items that you want to display on the Assets page.

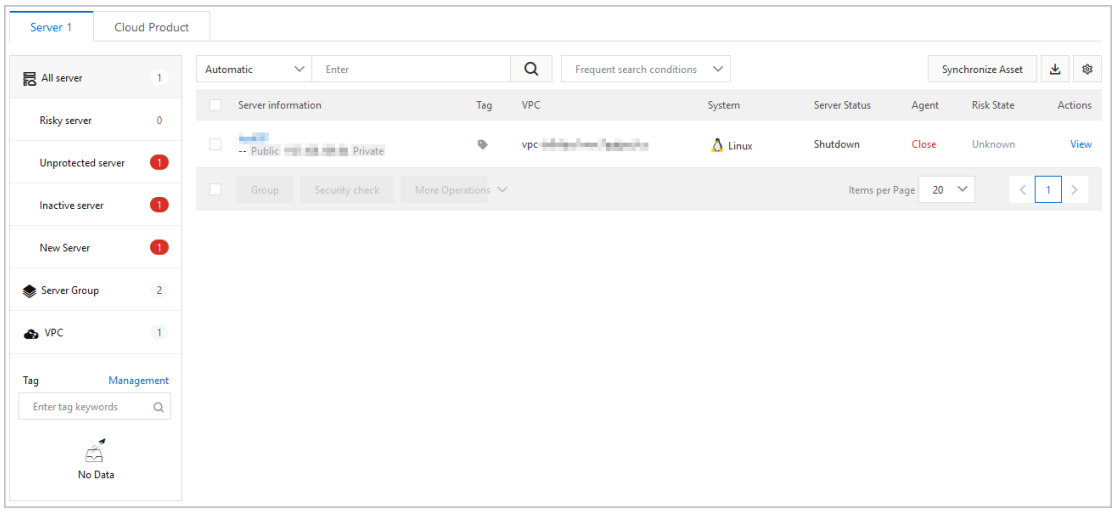
Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.

4. On the **Server(s)** tab of the Assets page, view the security status of each server.

   You can perform the following operations:

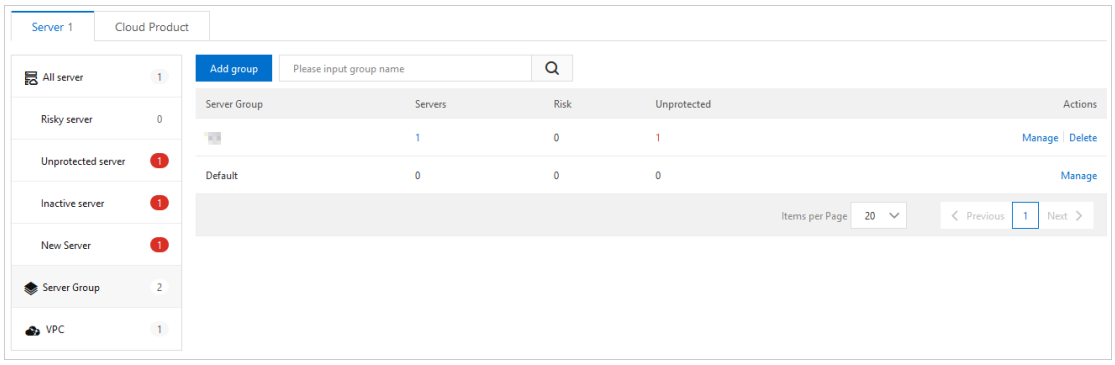
   - **Filter servers by status**
     - In **All Servers**, you can view the numbers of all servers, risky servers, unprotected servers, new servers, and servers that are shut down.



     To view the security information about a server, you must click the name of the server or click **Fix** in the **Actions** column. For more information, see View the details of a single asset.

     - You can click **Risk Servers**, **Unprotected Servers**, **Shutdown Server(s)**, or **New Server(s)** to view security information about specific servers.

   - **Filter servers by group**
     - You can click **Server Group** to view the numbers of all servers, servers that are at risk, and unprotected servers in each server group. You can also view the total number of server groups.

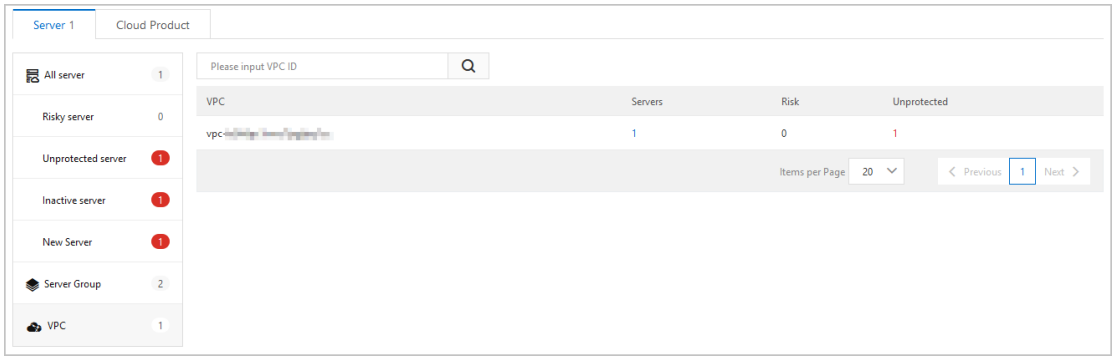


     To manage server groups, you can click **Manage** or **Delete** in the Actions column. For more information, see Manage asset groups.

     - You can find a server group and click the number in the **Servers**, **Risk**, or **Unprotected** column to view the security information about specific servers in this group.

   - **Filter servers by VPC ID**

- You can click **VPC** to view the numbers of all servers, servers that are at risk, and unprotected servers in each VPC. You can also view the total number of VPCs.



- You can find a VPC and click the number in the **Servers**, **Risk**, or **Unprotected** column to view the security information about specific servers in this VPC.

- **Filter servers by tag**

  In the navigation tree, you can click a tag to view the security information about servers to which the tag is added.

- **Filter servers by condition**

  If you click **All Servers**, **Server Group**, **VPC**, or a tag in the navigation tree, you can specify filter conditions above the right-side list to search for specific servers.

  - Use one filter condition to search for specific servers:

    You can select a filter condition and select or enter keywords to search for specific servers. The filter conditions include **Internet IP**, **Private IP**, **Instance name**, **System**, **Baseline problems**, **Vul problems**, **Alert problems**, **Risk Status**, **Online or Offline**, **Tag**, **Group name**, **OS**, and **Is there a snapshot risk**.

    > **Note**
    >
    > You can specify multiple filter conditions at a time and specify a Boolean operator for the conditions. The following list describes the Boolean operators:
    >
    > - Boolean operators:
    >   - **AND**: specifies the **AND** logical relation for the conditions.
    >   - **OR**: specifies the **OR** logical relation for the conditions.
    > - If you want to search for servers that meet at least one of the filter conditions, you must set the Boolean operator to **OR**.
    > - If a filter condition requires you to enter a keyword, you must enter the keyword and click the **Search** icon. Results are displayed only after you click the Search icon.

  - Use multiple filter conditions to search for specific servers:

    If you select multiple filter conditions, they are all applied to search for specific servers.

    You can also click **Server Group**, **VPC**, or a tag, and use the search box above the asset list to search for specific servers.

- **Save frequently used filter conditions**

You can save the filter conditions that are applied as frequently used search conditions. To save the conditions, click **Save** above the right-side list, and enter a name in the **Save condition** dialog box. Then, you can select the saved conditions from the **Frequently used search conditions** drop-down list on the right of the Search icon.

- **Customize displayed items**

  On the **Assets** page, you can click the icon in the upper-right corner. Then, you can select the items that you want to display on the Assets page.

4.6.2. View the security status of cloud services

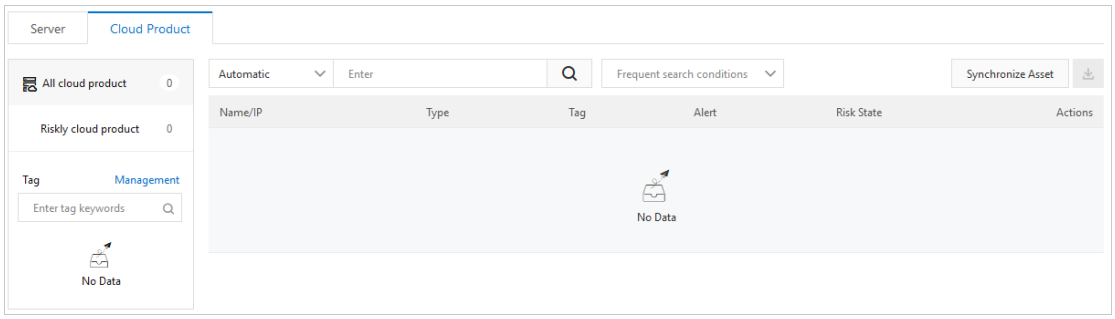
The Assets page displays the security information about each protected cloud service. The information includes the at-risk services and the types of services such as Server Load Balancer (SLB) and NAT Gateway. This topic describes how to configure search conditions to view the security status of cloud services.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the **Cloud Service** tab of the Assets page, view the security status of cloud services.

   You can perform the following operations based on your business requirements:

   - **Search by asset status**
     - In **All Cloud Services**, you can view the numbers of **all cloud services** and **risky cloud services**. You can also view the security status of all cloud services.

     - You can click **Risk Cloud Services** to view the cloud services that are at risk.

   You can click the name of the required cloud service or click **View** in the Actions column that corresponds to a service to view detailed information. For more information, see View the details of a single asset.

   - **Search by asset type**

     Cloud services are classified into two asset types:

     - **SLB**
     - **NAT**

In the navigation tree of the Cloud Service tab, you can view the number of cloud services of each type. You can click **SLB** or **NAT** to view the security status of the required cloud service.

- **Search by tag**

  In the **Tag** section of the navigation tree, you can view the number of cloud services to which each tag is added. You can click a tag to view the security status of cloud services to which the tag is added.

- **Filter by search condition**

  You can click **All Cloud Services**, **SLB**, or **NAT** in the navigation tree and configure search conditions in the search box above the **asset** list to search for specific assets.

  For example, you can click **All Cloud Services** and configure search conditions to search for specific assets.

  - Use multiple subconditions to search for specific assets:

    Select a condition from the drop-down list of the search box above the **asset** list, and select a subcondition or enter a keyword into the search box to search for specific assets. Supported search conditions are **Internet IP**, **Instance name**, **Alert problems**, **Risk Status**, **Tag**, and **Group name**.

  - Use multiple filter conditions to search for specific assets:

    Apply multiple search conditions.

    - You can click **SLB**, **NAT**, or a tag in the **Tag** section and configure conditions in the search box above the **asset** list to search for specific assets.
    - You can also click **All Cloud Services**, **SLB**, or **NAT**, and select a tag in the **Tag** section to search for specific assets.

- **Save frequently used search conditions**

  You can save the filter conditions that are applied as frequently used search conditions. Click **Save** below the search box and enter a name in the **Save condition** dialog box. Then, you can select the saved search condition from the Frequently used search conditions drop-down list on the right of the search box.

4.6.3. View the details of a single asset

The Assets page provides details about all assets. These details include basic information, alert management status, baseline check analysis, and asset fingerprints. This topic describes how to view the details of a server or a cloud service.

Context

The **Assets** page provides basic information about all assets. Different types of assets, such as servers and cloud services, are managed in different ways.

The following table lists the features that are supported for servers and cloud services on the **Assets** page. The following list describes the marks that are used to indicate whether a feature is supported for servers or cloud services:

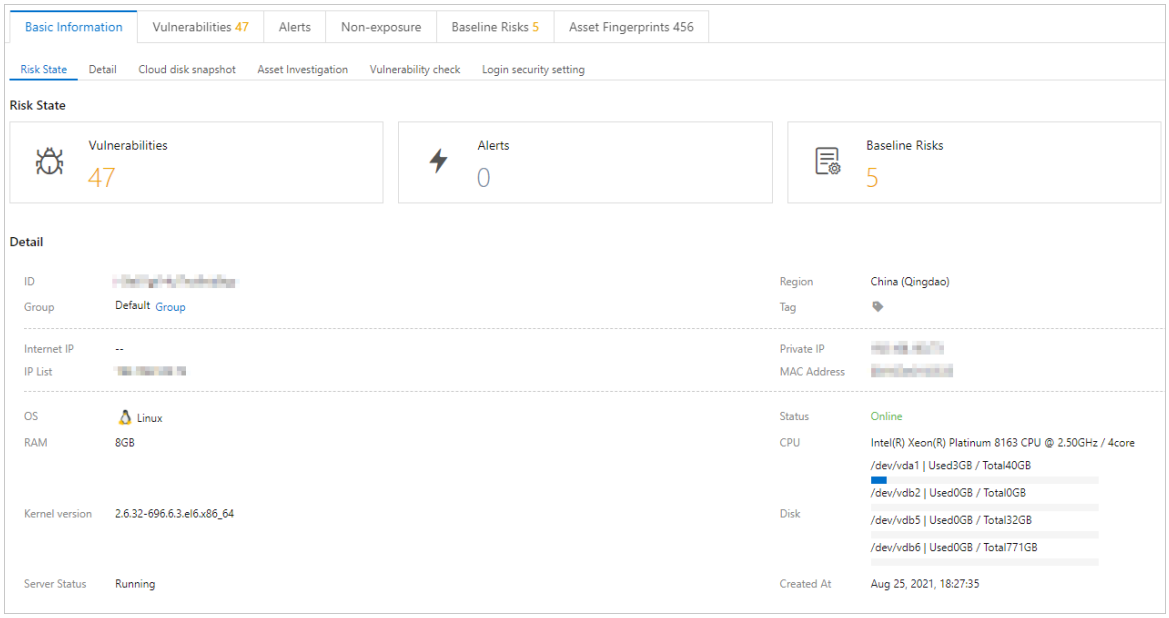
- Cross (×): not supported.
- Tick (√): supported.

Feature	Description	Server	Cloud service
Basic Information	Risk State: displays the number of risks detected on an asset. The following types of risks can be detected: • **Vulnerabilities** • **Alerts** • **Baseline Risks**	√	√ (Only alerts can be processed.)
	Detail: displays the configuration and protection status of an asset. You can specify a group and a tag for the asset.	√	√ (Asset grouping is not supported.)
	Asset Investigation: displays asset fingerprints, including ports, software, processes, and accounts.	√	X
	Vulnerability check: displays the types of vulnerabilities that can be detected. You can specify the types of vulnerabilities that you want to detect for an asset.	√	X
	Login security setting: displays the approved logon locations, IP addresses, time ranges, and accounts that are added. You can manage relevant alerts for an asset.	√	X
Vulnerabilities	Displays the results of vulnerability detection on an asset.	√	X
Alerts	Displays the alerts that are generated for an asset.	√	√
Baseline Risks	Displays the results of a baseline check on an asset.	√	X
Asset Fingerprints	Displays the details of asset fingerprints for an asset.	√	X

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the **Assets** page, click the **Server(s)** or **Cloud Service** tab.
5. On the **Server(s)** or **Cloud Service** tab, find the required asset and click its name.
6. View the details of the asset.

On the asset details page, click the **Basic Information**, **Vulnerabilities**, **Alerts**, **Non-exposure**, **Baseline Risks**, or **Asset Fingerprints** tab to view relevant details.

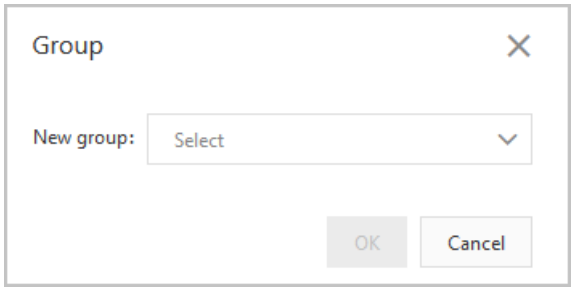


The following list describes the details of the asset:

- **Basic Information**: This tab consists of sections in which you can view asset details and manage the asset.
  - **Risk State**: This section displays the numbers of vulnerabilities, alerts, and baseline risks on the asset. You can click the number under Vulnerabilities, Alerts, or Baseline Risks to view the details.

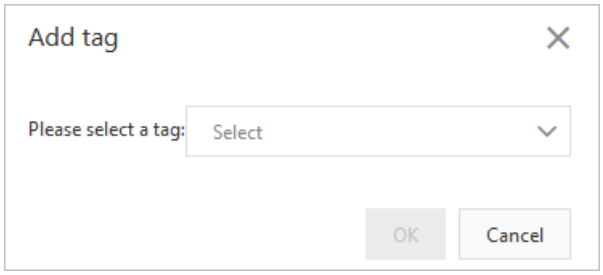
- **Detail**: This section displays information about the asset configuration and security protection settings, and allows you to manage asset tags and groups.
  - **Change asset groups**

    Click **Group**. In the **Group** dialog box, select a new group and click **OK**.

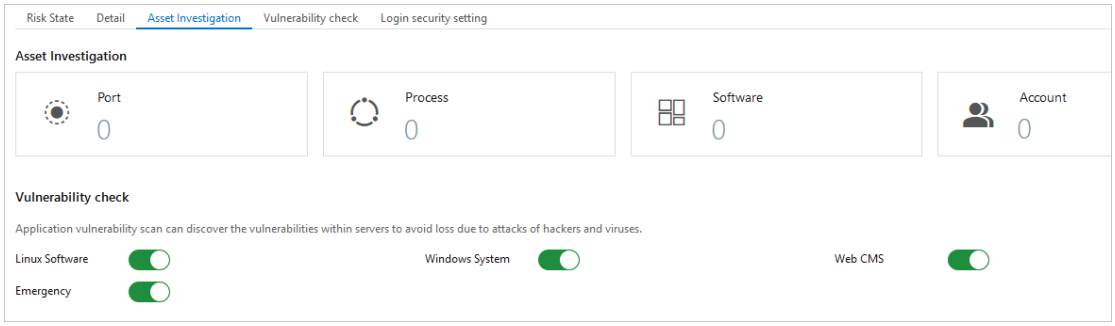
  - **Modify tags**

    Click the icon. In the **Add tag** dialog box, select a tag and click **OK**.

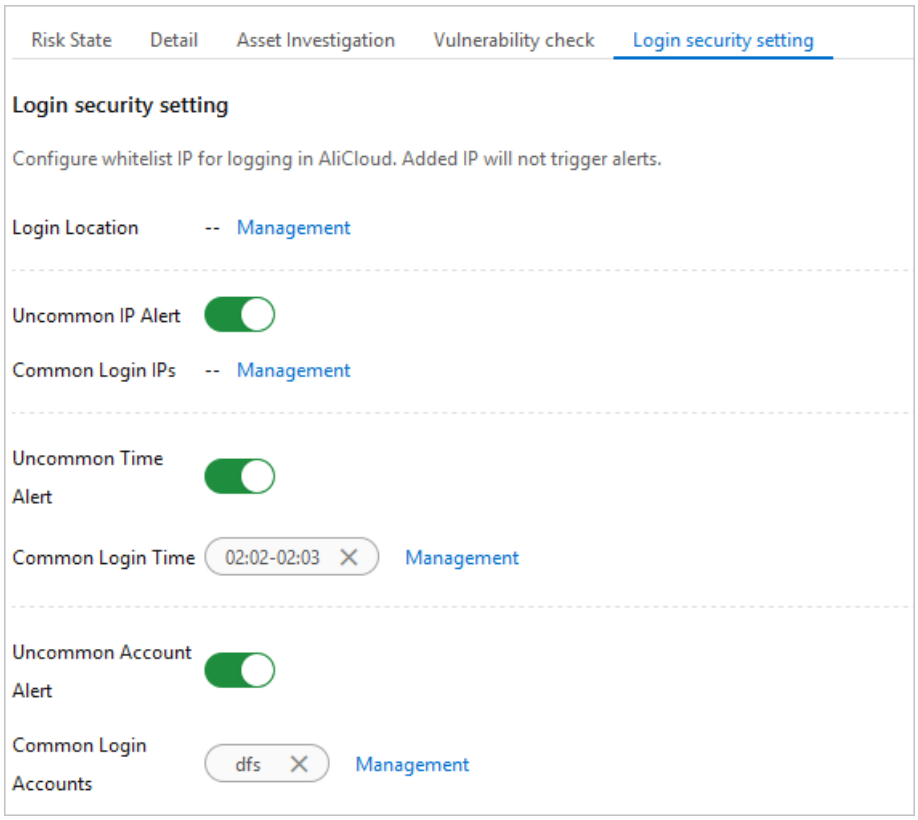
    You can click the icon on the right of a tag to delete the tag.

- **Asset Investigation**: This section displays the fingerprints of an asset. You can click the number under an item to go to the **Asset Fingerprints** tab to view the details.

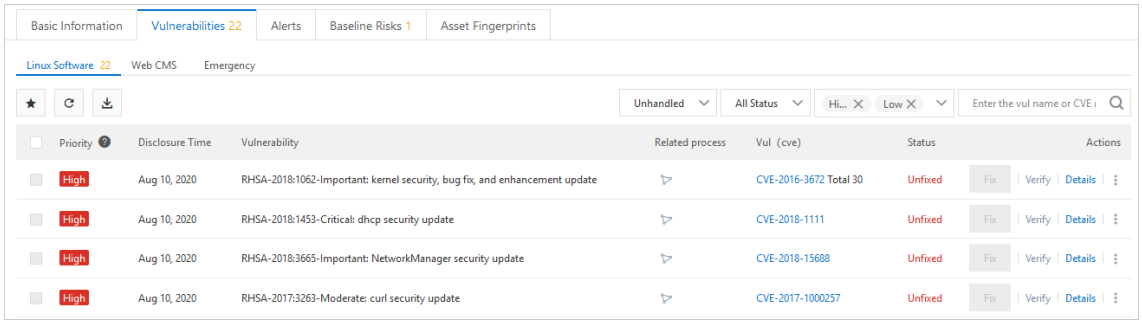
  

- **Vulnerability check**: This section displays vulnerability check items that are enabled or disabled for an asset. You can enable or disable different types of vulnerability checks for the asset. The vulnerabilities include Linux software vulnerabilities, Windows system vulnerabilities, Web CMS vulnerabilities, and urgent vulnerabilities.

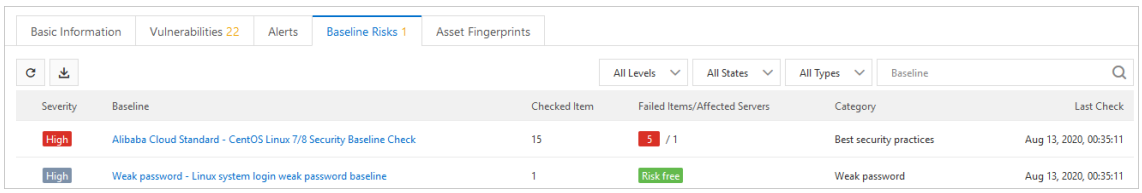
- **Login security setting**: This section allows you to specify approved logon locations, configure advanced logon settings, and turn on or turn off alerting for unapproved IP addresses, time, and accounts. The advanced logon settings include approved IP addresses, time ranges, and accounts. You can also specify approved IP addresses, time ranges, and accounts for a specific asset.



  - **Vulnerabilities**: This tab displays vulnerabilities detected on an asset.



  - **Alerts**: This tab displays alerts generated for an asset.
  - **Baseline Risks**: This tab displays baseline risks of an asset.

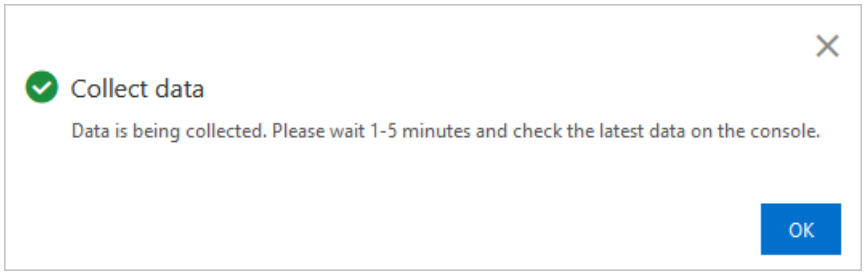


  - **Asset Fingerprints**: This tab displays the fingerprints, including ports, processes, software, and accounts of an asset.

You can manually collect the latest fingerprints of an asset.

a. You can click the **Port**, **Software**, **Process**, **Account**, or **Scheduled Tasks** tab. In the upper-right corner, click **Collect data now**.

b. In the **Collect data** message, click **OK**.



After the data collection task is submitted, it takes one to five minutes to collect the fingerprints of the required asset. After the data collection task is complete, you can view the latest fingerprints of the asset.

4.6.4. Enable and disable server protection

This topic describes how to enable and disable server protection.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the **Server(s)** tab of the page that appears, enable or disable server protection for specified servers.
   - **Enable server protection**

     Select one or more servers where the agent is in the **Close** state, and choose **More Operations > Turn on protection**.

     After server protection is enabled, the status in the Agent column changes to **Enable**.
   - **Disable server protection**

     If you confirm that a server does not require protection from Apsara Stack Security, you can disable protection for the server. Select one or more servers where the agent is in the **Enable** state, and choose **More Operations > Suspend Protection**.

     > **Note** After server protection is disabled, Apsara Stack Security stops protecting your servers. For example, Apsara Stack Security no longer detects vulnerabilities or generates alerts for detected risks. We recommend that you proceed with caution.

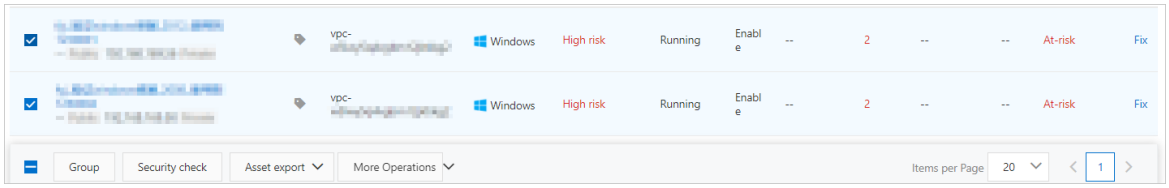
     After server protection is disabled, the status of the agent on your servers changes to **Close**.

4.6.5. Perform a quick security check

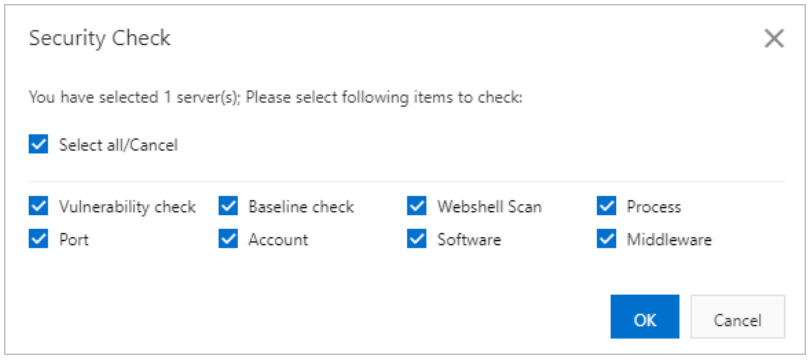
The Server(s) tab of the Assets page allows you to run security checks. You can dispatch security check tasks to scan for vulnerabilities, baseline risks, or webshells, and collect asset fingerprints on a specific server. The asset fingerprints are ports, software, processes, and accounts. This topic describes how to perform a security check on servers.

Procedure

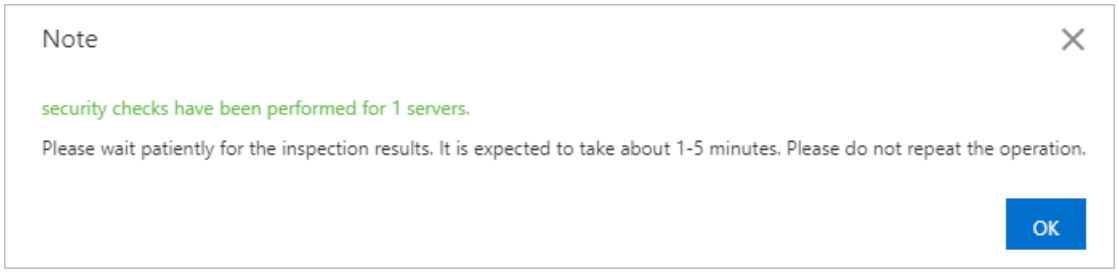
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the **Server(s)** tab, select one or more servers on which you want to perform a security check.
5. In the lower part of the page, click **Security check**.



6. In the **Security Check** dialog box, select check items.



7. Click **OK** to start the check.
8. In the message that appears, click **OK**.



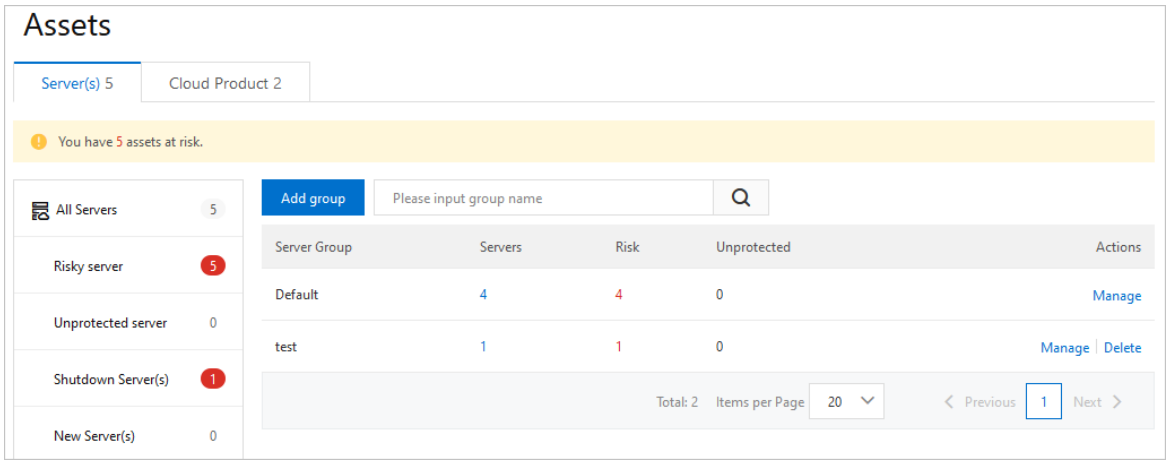
After the security check is complete, the check results are automatically displayed on the details pages of the selected servers.

4.6.6. Manage server groups

This topic describes how to create, modify, delete, and replace server groups.

Create a server group

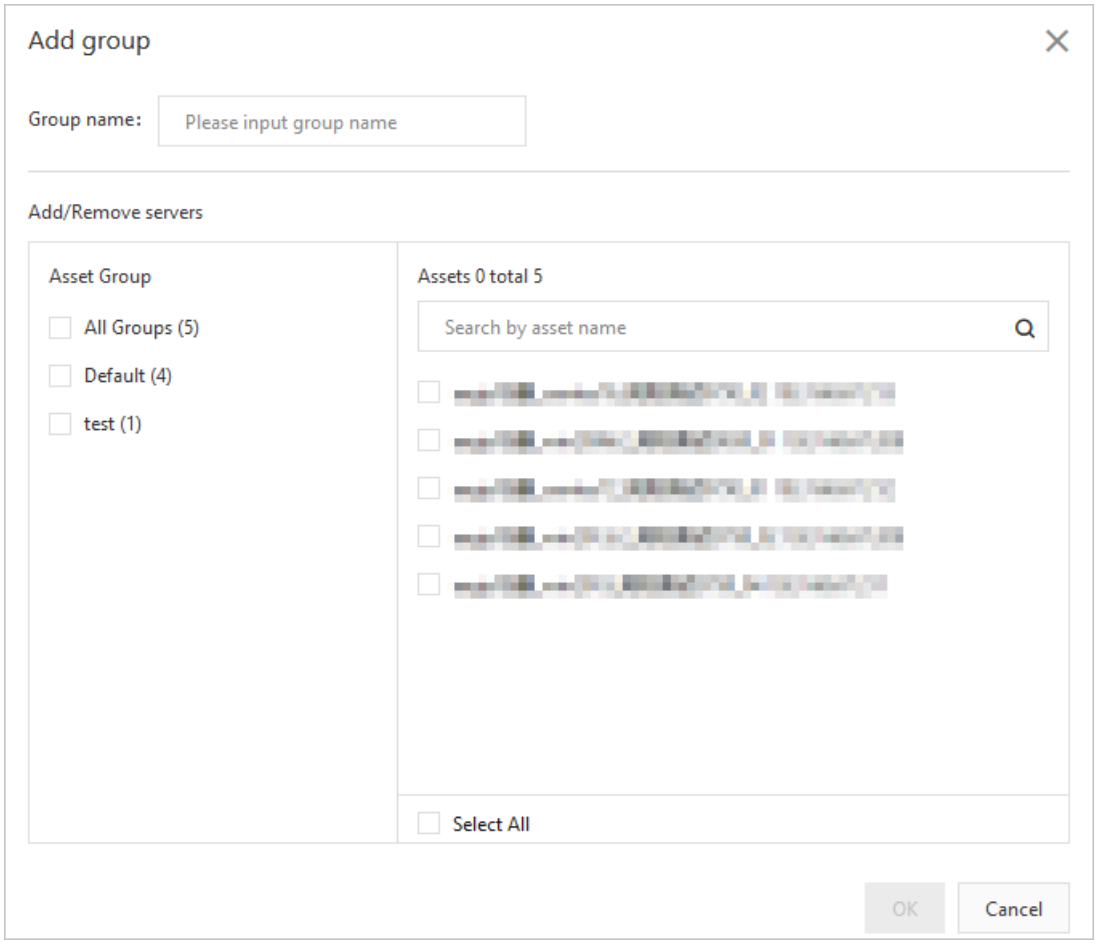
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the **Server(s)** tab of the page that appears, click **Server Group** in the navigation tree.



> **Note** By default, the assets that are not grouped are in the **Default** group.

5. Click **Add Group**.
6. In the **Add Group** dialog box, configure parameters for the new group.

   To configure the parameters, perform the following steps:



i. Enter a name for the new group in the **Group name** field.

ii. Add servers to the new group.

You can add servers in the Default group to the new group. You can also move servers from another group to the new group. To add or move servers, select **Default** or other groups in the **Asset Group** section, and select or clear the check boxes that correspond to the required servers in the asset list in the right area of the section.

7. Click **OK**.
In the server group list, you can view the new group.

Modify or delete a server group

The following procedure describes how to modify or delete a server group. When you modify a server group, you can rename the group or adjust the servers in the group.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the **Server(s)** tab of the page that appears, click **Server Group** in the navigation tree.
5. Find the server group that you want to modify or delete. In the Actions column, click **Manage** or **Delete**.

You can perform the following operations based on your business requirements:

- **Modify the group**
  a. In the Actions column, click **Manage**. The Group dialog box appears.
  b. In the **Group** dialog box, select the group in the **Asset Group** section.
  c. In the right area of the section, clear the check boxes that correspond to the required servers in the asset list.
  d. Click **OK**. The server group is modified.
- **Delete the group**

  In the Actions column, click **Delete**. In the message that appears, click **OK**.

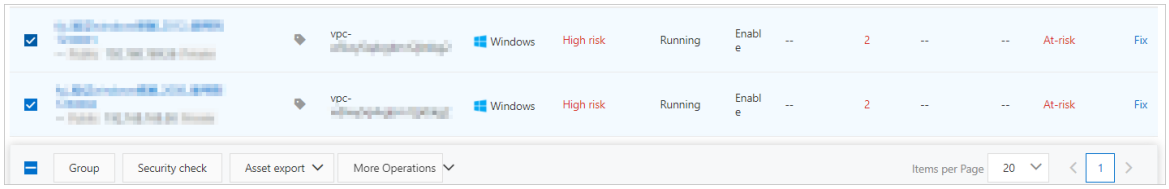
  > **Note** After you delete a group, servers in this group are moved to the **Default** group.

Replace a server group

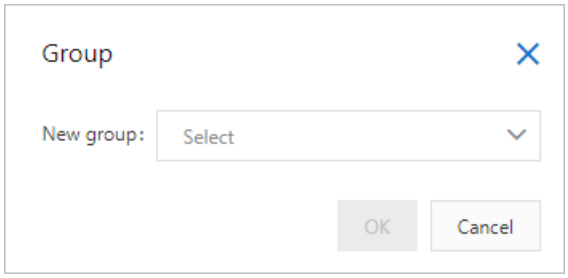
You can add servers to a server group to manage multiple servers at a time. We recommend that you add the same types of servers to a server group. For example, if you configure a baseline check template, you can specify a server group and apply the template to all servers in the group. You can also filter and view servers based on server groups.

To add servers to a specific server group, perform the following steps:

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the Server(s) tab of the page that appears, select one or more servers and click **Group** in the lower part of the page.



5. In the **Group** dialog box, select a new server group.



6. Click **OK**.

4.6.7. Manage asset tags

This topic introduces asset importance tags and describes how to create, modify, and delete custom tags.

Context

Apsara Stack Security provides the asset importance tags described in the following table to classify assets. You can select appropriate importance tags for your assets.

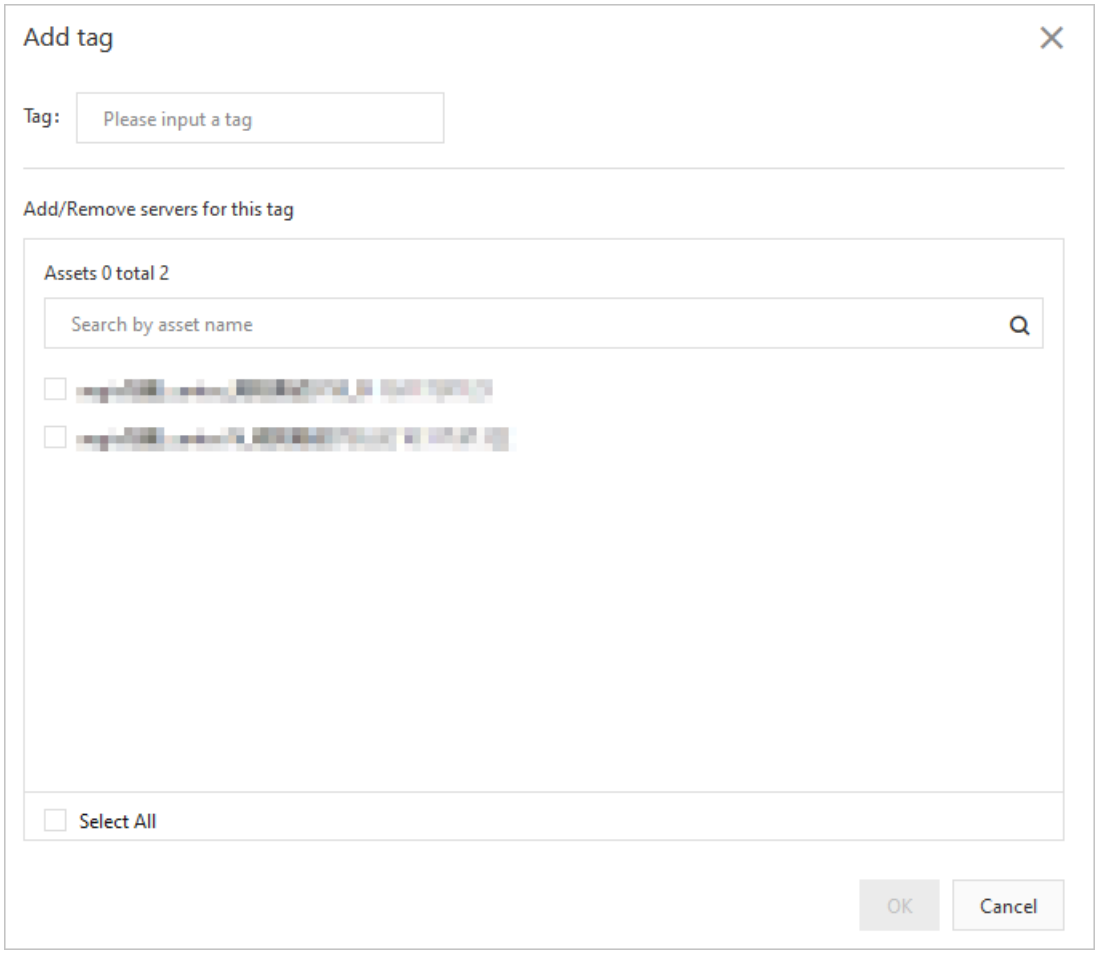
An asset importance tag is transformed to an **asset importance score**. An **asset importance score** is used to calculate a vulnerability priority score. You can determine whether to preferentially fix a vulnerability based on the vulnerability priority score. We recommend that you add importance asset tags to core assets. Apsara Stack Security prompts you to fix vulnerabilities based on the importance of each asset. The following table describes the relationships between asset importance tags and asset importance scores.

Asset importance tag	Asset importance score	Recommendation
Important Assets	1.5	Assets that are related to crucial business or store core business data. Virus intrusion into the assets adversely affects the system and causes major loss.
General Assets	1	Assets that are related to non-crucial business and are highly replaceable. Virus intrusion into the assets causes less impact on the system.
Test Assets	0.5	Assets for functional or performance tests, or assets that can cause less impact on the system.

Note If you do not add asset importance tags, the **General Assets** tag is automatically added to each asset. This tag indicates that the asset importance score is 1.

Create a custom tag

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the **Assets** page, click the **Server(s)** or **Cloud Service** tab.
5. In the navigation tree of the **Server(s)** or **Cloud Service** tab, click **Management** to the right of **Tag**.
6. In the **Add tag** dialog box, enter the tag name in the **Tag** field.



7. In the **Asset Group** section, select a server group. Then, select the required servers to add the new tag to the selected servers in the right area of the section.
8. Click **OK**.

   In the asset list of the Server(s) or Cloud Service tab, you can click the icon in the **Tag** column to add the new tag to an asset.

   > **Note** You can add multiple tags to one asset. All tags of an asset are displayed in the **Tag** column.

Modify or delete a custom tag

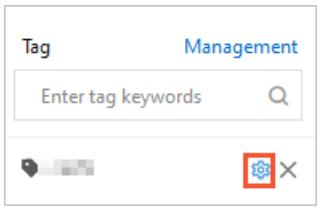
The following procedure describes how to modify or delete a custom tag. When you modify a tag, you can rename the tag or adjust the servers to which the tag is added.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Assets**.
4. On the **Assets** page, click the **Server(s)** or **Cloud Service** tab.
5. On the **Server(s)** or **Cloud Service** tab, modify or delete a tag.

   Perform the following operations to modify or delete a tag:

- **Modify a tag**

  a. Find the tag that you want to modify and move the pointer over the icon to the right of the tag. Then, click the icon.

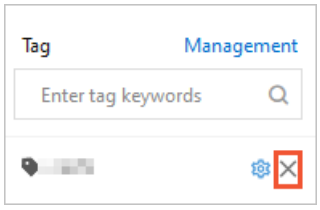
  

  b. In the **Tag** dialog box, enter a new name in the **Tag** field, add the tag to more servers, or remove the tag from specific servers.

  c. Click **OK**.

- **Delete a tag**

  Find the tag that you want to delete and move the pointer over the icon to the right of the tag. Then, click the icon. In the message that appears, click **OK**.

4.7. Application whitelist

The application whitelist feature prevents unauthorized programs from running on your servers and provides a trusted running environment for your servers.

Context

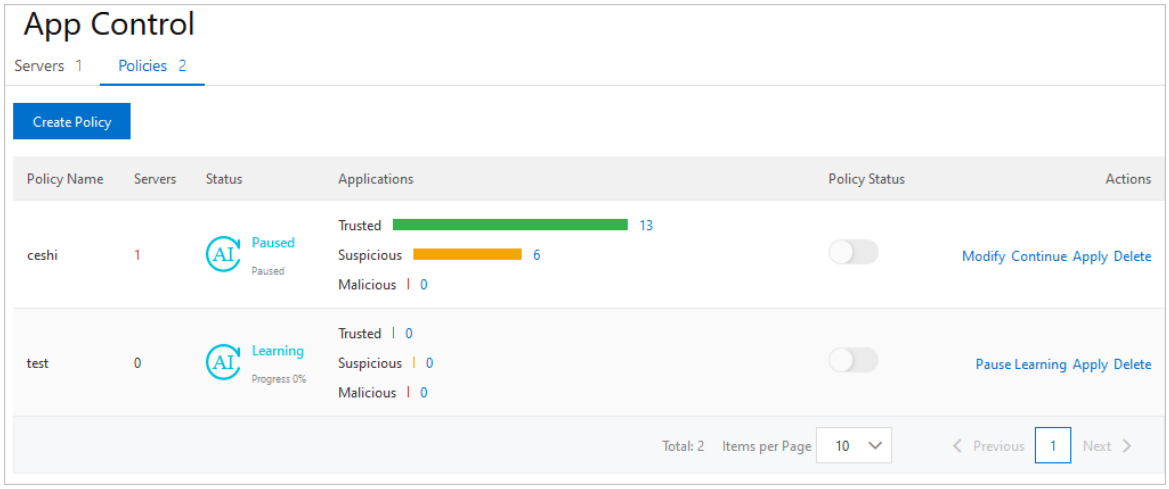
The application whitelist feature allows you to apply application whitelist policies to your servers that require special protection. Apsara Stack Security identifies trusted, suspicious, and malicious programs based on the policies. Then, you can add the identified programs to an application whitelist based on your business requirements. This prevents unauthorized programs from running. This feature protects your servers from untrusted and malicious programs and improves resource usage.

After you create an application whitelist policy, you can apply it to a server that requires special protection. Then, Apsara Stack Security scans for suspicious or malicious programs on the server and generates alerts for the programs that are not in the application whitelist.

> **Note** If a program that is not in the application whitelist starts, an alert is generated. The program may be a normal program that is newly started or a malicious program that is inserted into your compromised server. If the program is a normal program, a frequently used program, or a third-party program installed by you, we recommend that you add the program to the application whitelist. After you add the program to the application whitelist, Apsara Stack Security no longer generates alerts for this program the next time the program starts. If the program is malicious, we recommend that you immediately delete this program and check whether the configuration files such as cron tasks are tampered with.

Step 1: Create an application whitelist policy

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Application Whitelists**.
4. On the **Application Whitelist** page, click the **Policies** tab.
5. On the **Policies** page, click **Create Policy**.
6. In the Create Policy step of the **Create Whitelist Policy** panel, configure the following parameters:
   - **Policy Name**: the name of the application whitelist policy.
   - **Intelligent Learning Duration**: the duration for Apsara Stack Security to perform intelligent learning. Valid values: 1 Day, 3 Days, 7 Days, and 15 Days. The intelligent learning feature uses machine learning to automatically collect and categorize large amounts of alert data. Apsara Stack Security can identify suspicious or malicious programs based on the collected data.
   - **Servers for Intelligent Learning**: the servers to which you want to apply the application whitelist policy.
7. Click **Next**. The application whitelist policy is created.
   After the application whitelist policy is created, the policy details are displayed in the policy list on the Policies tab.



The following table describes the parameters in the list of application whitelist policies.

Parameter	Description
Policy Name	The name of the application whitelist policy.
Servers	The number of servers to which the application whitelist policy is applied.

Parameter	Description
Status	The status of the policy. Valid values: ○ **Applied**: Intelligent learning is complete. The policy has been applied to servers. ○ **Pending Confirmation**: Intelligent learning is complete. The policy needs to be confirmed and enabled. After intelligent learning is complete, you must turn on the switch in the **Policy Status** column to enable this policy. The policy takes effect only after it is enabled. Apsara Stack Security automatically identifies the programs on your servers as trusted, suspicious, or malicious programs. ○ **Paused**: Intelligent learning is manually paused. You can click **Continue** in the Actions column to resume intelligent learning. ○ **Learning**: Intelligent learning is in progress. After an application whitelist policy is created, Apsara Stack Security automatically performs intelligent learning based on the policy. The status of a new application whitelist policy is **Learning**.
Applications	The number of programs of each type on all servers to which the policy is applied. The program types include **trusted**, **suspicious**, and **malicious**.
Actions	The operations that you can perform on a policy. You can perform the following operations: ○ **Apply**: Add or remove servers to which the policy is applied in the **Apply Whitelist Policy** panel. ○ **Modify**: Modify the policy in the **Modify Whitelist Policy** panel. You can change the values of **Policy Name** and **Intelligent Learning Duration**, and add or remove the servers on which intelligent learning is automatically performed. ○ **Pause Learning**: Pause intelligent learning. ○ **Continue**: Resume intelligent learning. After you click **Continue**, the status of the policy changes to **Learning**. You can view the learning progress of the policy in the **Status** column. ○ **Delete**: Delete the policy. After the policy is deleted, the servers to which the policy is applied are no longer protected by the policy.

Step 2: Apply the created application whitelist policy to servers

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane, click **Application Whitelists**.
4. On the **Application Whitelist** page, click **Servers**
5. On the **Servers** tab, click **Add Server**.
6. In the **Add Server** panel, configure the parameters.

In the **Add Server** panel, configure the following parameters:

- **Whitelist Policy**: Select the created application whitelist policy from the drop-down list.
- **Event Handling**: The default value is **Alert**, which indicates that Apsara Stack Security generates an alert when a suspicious program is detected.

  If a program that is not in the application whitelist starts, Apsara Stack Security automatically generates an alert. You can click the number in the **Suspicious Events** column to go to the **Alerts** tab of the server details page and view the alert details.
- **Servers**: Select the server to which you want to apply the application whitelist policy. You can select multiple servers.

  To search for a server, enter the server name in the **Servers** search box and click the search icon. Fuzzy match is supported.

7. Click **OK**. The application whitelist policy is applied to the selected servers.
   After the application whitelist is created, you can view the protected servers and the name of the application whitelist policy in the server list on the **Servers** tab.

   The **Servers** tab displays the following information of a protected server:

   - **Server Name/IP**: the name and IP address of the server to which the application whitelist policy is applied.
   - **Whitelist Policy**: the name of the application whitelist policy that is applied to the server.
   - **Suspicious Events**: the number of programs that are not in the application whitelist and have started. If a suspicious program starts on the server, Apsara Stack Security detects the program and generates an alert.
   - **Event Handling**: The default value is **Alert**, which indicates that Apsara Stack Security generates an alert when a suspicious program is detected.

     If a program that is not in the application whitelist starts, Apsara Stack Security automatically generates an alert. You can click the number in the **Suspicious Events** column to go to the **Alerts** tab of the server details page and view the alert details.
   - **Actions**: After you click **Delete** in the **Actions** column, the server is removed from the application whitelist policy.

     After you click Delete in the Actions column, the application whitelist policy becomes invalid for the server. In this case, if a program that is added to the application whitelist starts on this server, Apsara Stack Security generates an alert.

Add a program to or remove a program from an application whitelist

After you configure an application whitelist policy for your server, you can view the detailed information in the server list on the **Servers** tab. The information includes the details of the protected server and the name of the application whitelist policy that is applied to the server. You can click a policy name in the **Whitelist Policy** column to view the programs running on the server. You can also view the numbers of trusted, suspicious, and malicious programs and their detailed information.

The following information about each program on the server is displayed:

- **Type**: the type of the program. Programs are classified into trusted, suspicious, and malicious programs.
- **Process Name**: the name of the program.
- **Hash**: the hash function of the program. A hash function is used to identify whether a program is

unique. This helps protect servers against malicious programs.

- **Path**: the file path of the program on the server.
- **Degree of Trustability**: the degree of trustability for the program. The value of this parameter is determined by Apsara Stack Security. Valid values: 0%, 60%, and 100%. The value 0% indicates malicious programs, 60% indicates suspicious programs, and 100% indicates trusted programs.

  > **Note** We recommend that you handle the program whose Degree of Trustability is 0% at the earliest opportunity.

- **Actions**: the operations that can be performed on the program. You can determine whether to add the program to the whitelist based on the services deployed on your server. You can perform the following operations:
  - **Add to Whitelist**: If you trust the program, add it to the whitelist.
  - **Remove from Whitelist**: After you remove the program from the whitelist, Apsara Stack Security identifies the program as untrusted. If this program starts, Apsara Stack Security generates an alert.

4.8. Vulnerability scan

4.8.1. Quick start

This topic describes how to get started with the vulnerability scan feature.

The following procedure shows how to use the vulnerability scan feature:

1. Configure the following detection items and the required cycles based on your environment requirements:
   - Overall Monitoring: Configure detection features and the monitoring cycle of each detection feature. For more information, see Configure overall monitoring.
   - Basic Monitoring: Configure Weak Password Vulnerability Monitoring, Operation Security Vulnerability Monitoring, CMS Application Vulnerability Monitoring, and Baseline Monitoring. For more information, see Configure basic monitoring.
   - Web Monitoring: Configure the monitoring cycle and the types of web vulnerabilities that you want to monitor. For more information, see Configure web monitoring.
   - Whitelist: Add the assets that do not require detection to the whitelist. For more information, see Configure a whitelist.
2. Import assets that require vulnerability scans.
   - Import internal assets: Configure a scan engine to import your internal assets in virtual private clouds (VPCs). For more information, see Configure a scan engine for internal assets.
   - Import Internet assets: Import your Internet assets. For more information, see Import assets.

     > **Note** The number of imported assets cannot exceed the specified upper limit.

3. View and confirm the results of vulnerability scans.
   - View the overall information to obtain the results of vulnerability scans. For more information, see View the information on the Overview page.

- View and confirm vulnerability risks. For more information, see Manage security vulnerabilities.
- View and confirm host compliance risks. For more information, see Manage host compliance risks.

4. Generate vulnerability scan reports.

   Generate reports to audit the vulnerabilities and baseline risks on assets on a regular basis. For more information, see Create a report.

4.8.2. View the information on the Overview page

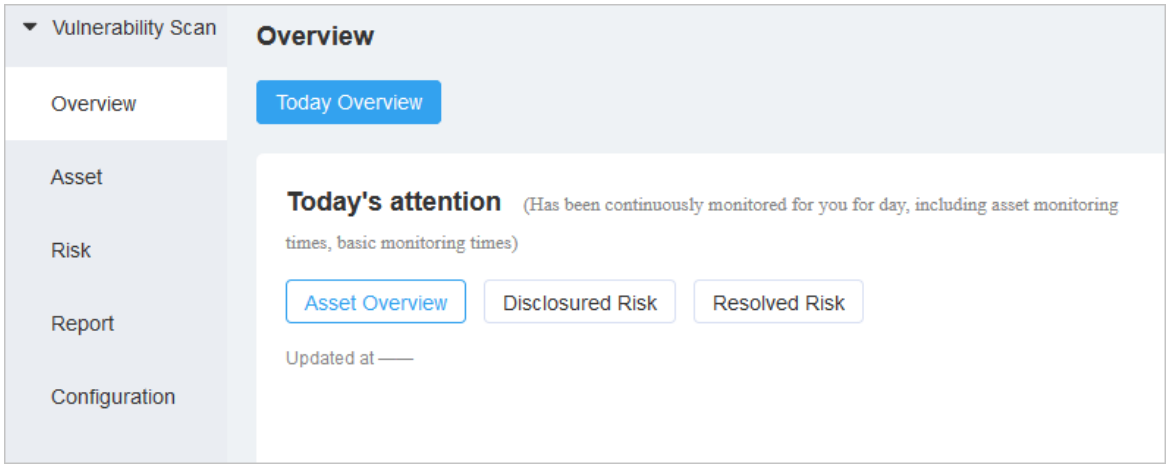
This topic describes the overall results of vulnerability scans. Security administrators can understand the vulnerability situation based on the overall results.

Context

The vulnerability scan feature can identify the following vulnerabilities: web security vulnerabilities, content management system (CMS) application vulnerabilities, weak password vulnerabilities, O&M security vulnerabilities, and baseline security vulnerabilities.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Overview**.
4. View the overall results of vulnerability scans.



Section	Description

Section	Description
Today's attention	View Asset Overview, Disclosured Risk, and Resolved Risk of the current day. ○ **Asset Overview**: displays the numbers of hosts, websites, and domain names for the current day and provides a security score for the current assets. The radar chart on the right shows the distribution of web security vulnerabilities, CMS application vulnerabilities, weak password vulnerabilities, O&M security vulnerabilities, and baseline security vulnerabilities. ○ **Disclosured Risk**: displays the numbers of high-risk vulnerabilities, medium-risk vulnerabilities, and low-risk vulnerabilities, and the total number of these vulnerabilities for the current day. These vulnerabilities are not fixed. The **Disclosured Risk Distribution** section on the right displays the distribution of unfixed vulnerabilities. ○ **Resolved Risk**: displays the numbers of high-risk vulnerabilities, medium-risk vulnerabilities, and low-risk vulnerabilities, and the total number of these vulnerabilities for the current day. These vulnerabilities are fixed. The **Resolved Risk Distribution** section on the right displays the distribution of fixed vulnerabilities.
Asset Risk Top 5	View the top five assets that are at risk on the **Security Vulnerabilities** and **Host Compliance** tabs. These assets are displayed by asset or group.
Risk Monitoring Trend	View the trend charts of vulnerabilities on the **Security Vulnerabilities** and **Host Compliance** tabs. Fixed and unfixed vulnerabilities are identified by lines in different colors. You can move the pointer over a line to view the numbers of unfixed vulnerabilities and fixed vulnerabilities for the specific day.
Asset Monitoring Trend	View the trends in the numbers of protected hosts and websites. Hosts and websites are identified by lines in different colors. You can move the pointer over a line to view the number of protected hosts and websites for the specific day.
Risk Asset Ranking List	View the rankings of assets that are at risk on the **Latest Risk** and **High Risk** tabs.
Port Service Statistics	View the statistics on the **Port** and **Host Service** tabs.

4.8.3. Asset management

4.8.3.1. View the results of asset analysis

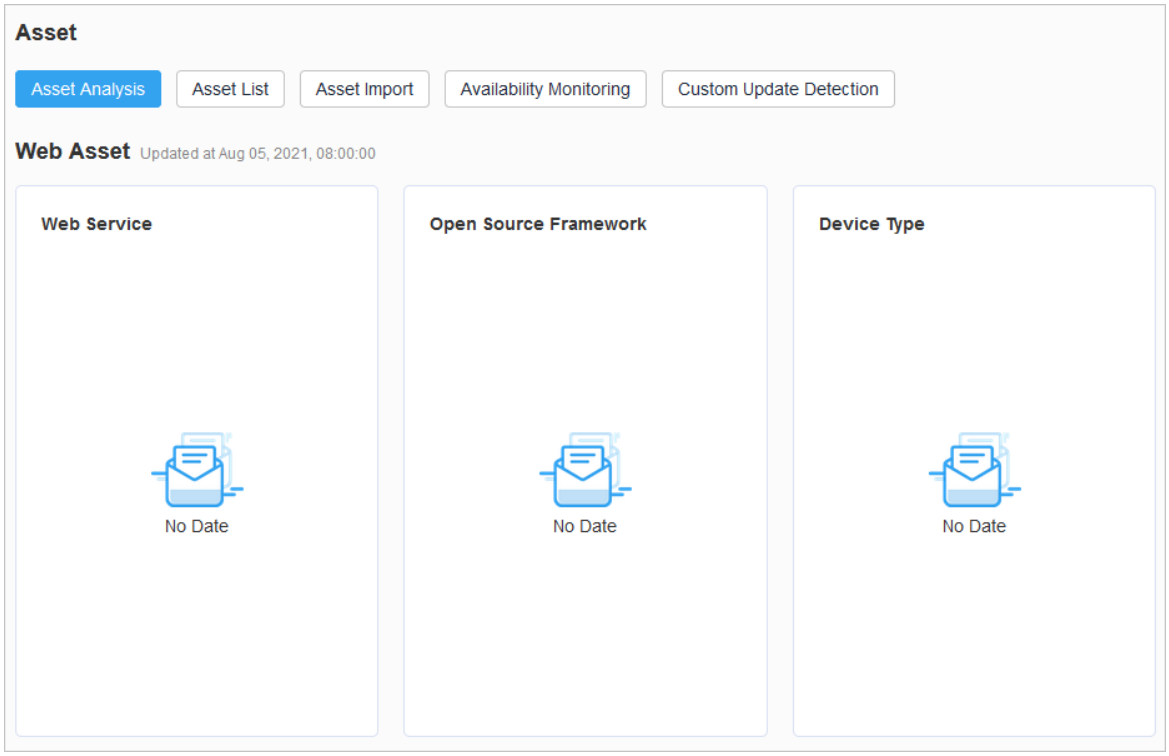
This topic describes how to view the analysis results of websites and hosts.

Context

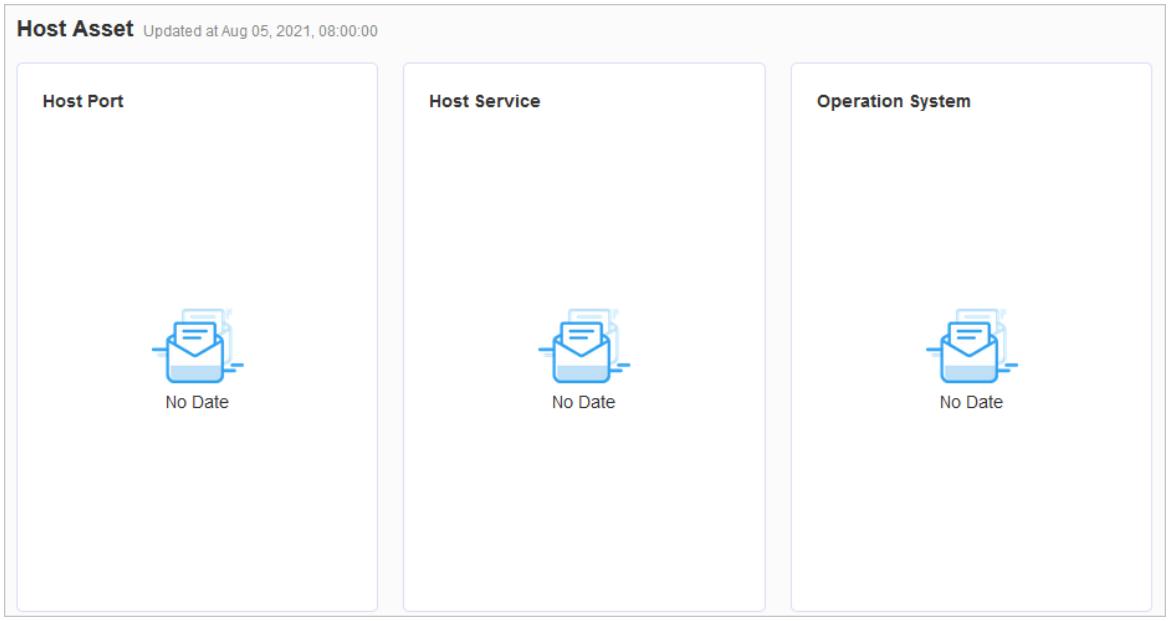
The asset analysis feature allows you to view the analysis results of websites and hosts. For the websites, you can view Web Service, Open Source Framework, and Device Type. For the hosts, you can view Host Port, Host Service, and Operation System.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the **Vulnerability Scan** pane, click **Asset**.
4. On the **Asset** page, click the **Asset Analysis** tab to view websites.



5. View hosts.



4.8.3.2. Import assets

This topic describes how to import Internet assets.

Context

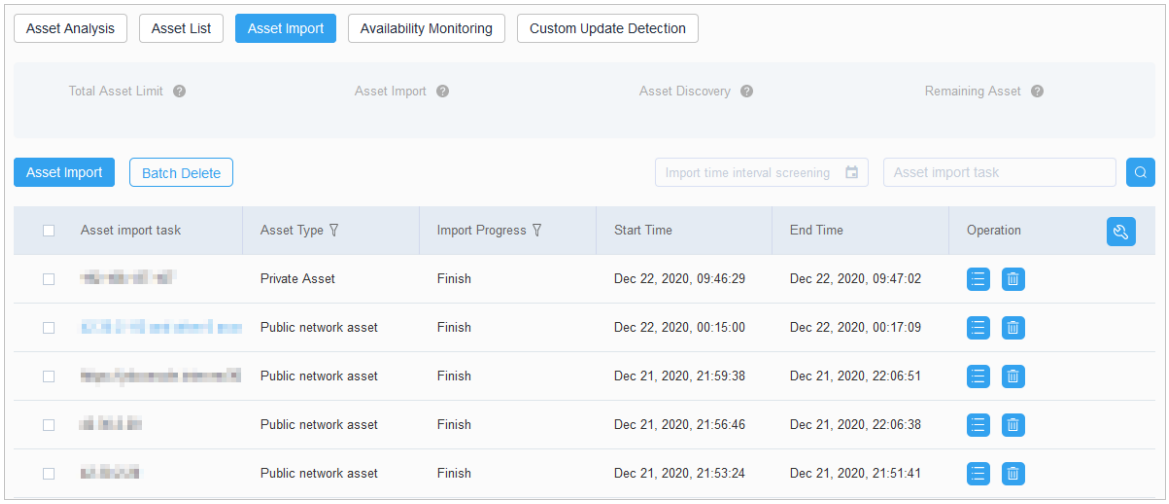
The vulnerability scan feature works only on imported assets. If you want to scan the vulnerabilities of your assets, you must import your assets.

The assets that the feature supports include Internet assets and internal assets. The internal assets refer to the assets in a virtual private cloud (VPC).

- To import internal assets, you must add a scan engine. For more information, see Configure a scan engine for internal assets.
- To import Internet assets, perform the operations provided in this topic.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the **Vulnerability Scan** pane, click **Asset**.
4. On the **Asset** page, click the **Asset Import** tab to view imported assets.



5. Click **Asset Import**. On the **Public network asset Import** page, create an asset import task.
   i. In the **Import Asset** section, select **Manual Import** and enter the required assets in the field. Then, read and select the disclaimer.
      - You can enter domain names, URLs, IP addresses, and CIDR blocks.
      - You can enter the information about multiple assets at a time. Press Enter after you enter the information about one asset.
      - You cannot enter the information about the assets in VPCs.
      - The number of imported assets must be less than the number of remaining assets supported by the platform.

        > **Note** For example, if the number of remaining assets supported by the platform is 100 and 90 assets are entered, all the assets can be scanned. If 110 assets are entered, only 100 assets can be scanned, and the 10 assets that remain cannot be scanned.

   ii. In the **Asset Info** section, group the imported assets and configure an owner and a tag for the assets.
      - **Asset Group**: Select a group from the drop-down list. You can click the icon to create, edit, or delete a group.
      - **Person in charge**: Select an owner from the drop-down list. You can click the icon to create, edit, or delete an owner.
      - **Asset Tag**: Click **Add Tag** to add a tag to the imported assets.

iii. In the **Import Set** section, select the operations that you want to perform after the assets are imported.

Operation		Description
Asset Discovery	*Auto Import subdomains*	Automatically queries the subdomain assets of the imported domain names.
	Auto import associated IP	Automatically adds IP address assets that are mapped to the domain names.
	Auto synchronize tags and groups	Applies the group and tag of the imported assets to the assets that are discovered by the system.
Web Asset	*Open WEB Monitoring*	Enables the web monitoring feature on the imported website assets. If you want to select the web monitoring rules to use, click the icon. In the dialog box that appears, select the required web monitoring rules. For more information about how to configure web monitoring rules, see Configure web monitoring.

iv. In the **Whitelist** section, add the assets that do not need to be scanned.

You can enter IP addresses and URLs. If you add more than one asset, you must press Enter after you enter the information about an asset.

v. Click **Save**.

6. Manage the created asset import task.

After the asset import task is created, you can view the task in the task list. You can also perform the following operations on the task.

Icon	Description
	View the details, result, and process of the asset import task.
	Delete the asset import task.

4.8.3.3. Manage assets

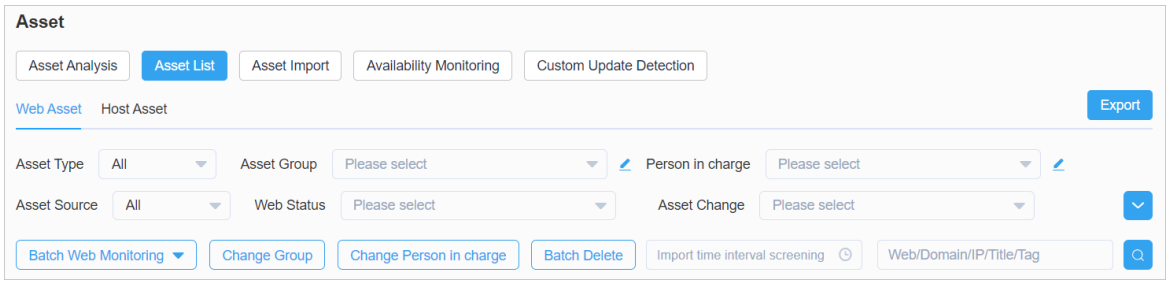
This topic describes how to view and manage assets.

Context

You can view the information about assets in the asset list. If the purpose or owner of an asset changes, security administrators can move the asset to another group or change the owner.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the Vulnerability Scan pane, click **Asset**.
4. On the **Asset** page, click the **Asset List** tab to view assets.



5. Click the **Web Asset** tab and manage websites.
   i. Specify filter conditions to search for websites.

   The filter feature allows you to search for websites in a more efficient manner.

Filter condition	Description
Asset Type	The type of the asset that you want to view.
Asset Source	The source from which the asset is imported. Valid values: **Manual** and **System Find**.
Asset Group	The group to which the asset belongs.
Web Status	The status of the website.
Person in charge	The owner of the website.
Asset Change	The change status of the asset. Valid values: **All**, **New**, **Update**, **No Update**, and **Offline**.
Web Monitoring	The monitoring status of the website.
Risk Level	The risk level of the asset.
Web Service	The service type and version of the website.
WAF Recognition	Specifies whether the asset is identified by Web Application Firewall (WAF).
Open Source Framework	The open source framework type of the asset.
Device Type	The type of the device.
Time range	The time range during which the asset is imported.
Key information	The key information of the asset. The key information includes the website, domain name, IP address, title, and tag.

ii. Click **Export** to export the asset list to an EXCEL file.

iii. Select one or more websites that you want to manage. The following table describes the operations that you can perform on the websites.

Operation	Description
Batch Web Monitoring	Allows you to enable or disable web monitoring for multiple websites. ■ **Batch Open Monitoring**: To enable web monitoring for multiple websites, select Batch Open Monitoring from the drop-down list of Batch Web Monitoring. ■ **Batch Stop Monitoring**: To disable web monitoring for multiple websites, select Batch Stop Monitoring from the drop-down list of Batch Web Monitoring
Change Group	Allows you to change the group of multiple assets at a time.
Change Person in charge	Allows you to change the owner of multiple assets at a time.
Batch Delete	Allows you to delete multiple assets at a time. After the assets are deleted, the assets are not scanned by the vulnerability scan feature.

6. Click the **Host Asset** tab and manage hosts.

i. Specify filter conditions to search for hosts.

The filter feature allows you to search for hosts in a more efficient manner.

Filter condition	Description
Asset Type	The asset type, such as Internet assets or a specific VPC.
Asset Source	The source from which the asset is imported. Valid values: **Manual** and **System Find**.
Asset Group	The group to which the asset belongs.
Person in charge	The owner of the asset.
Asset Change	The change status of the asset. Valid values: **All**, **New**, **Update**, **No Update**, and **Offline**.
Risk Level	The risk level of the asset. Valid values: **All**, **High**, **Middle**, **Low**, and **Security**.
SurviveStatus	The liveness status of the asset. Valid values: **Alive** and **Close**.
Operation System	The operating system of the host.
Host Port	The port of the host.
CDN Recognition	Specifies whether Content Delivery Network (CDN) is configured for the asset.
Host Service	The service of the host.
Time range	The time range during which the asset is imported.
Key information	The key information of the asset. The key information includes the IP address, host, tag, and domain name.

ii. Click **Export** to export the asset list to an EXCEL file.

iii. Select one or more hosts that you want to manage. The following table describes the operations that you can perform on the hosts.

Operation	Description
Change Group	Allows you to change the group of multiple assets at a time.
Change Person in charge	Allows you to change the owner of multiple assets at a time.
Batch Delete	Allows you to delete multiple assets at a time. After the assets are deleted, the assets are not scanned by the vulnerability scan feature.

4.8.3.4. Manage asset availability

This topic describes how to manage the availability of assets.

Context

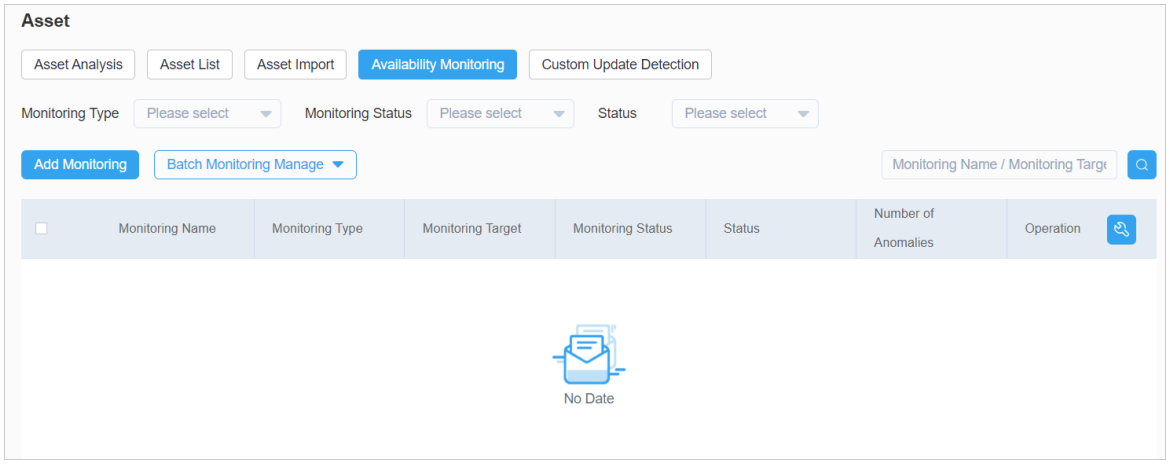
If hosts or websites are used for a long period of time, they may become unavailable due to errors. Availability monitoring allows a security administrator to discover unavailable assets. Then, the security administrator can troubleshoot the issues that cause the assets to become unavailable.

Availability monitoring supports the following methods:

- HTTP monitoring: This method is used to monitor websites.
- PING monitoring: This method is used to monitor hosts.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the **Vulnerability Scan** pane, click **Asset**.
4. On the **Asset** page, click the **Availability Monitoring** tab to view availability monitoring tasks.

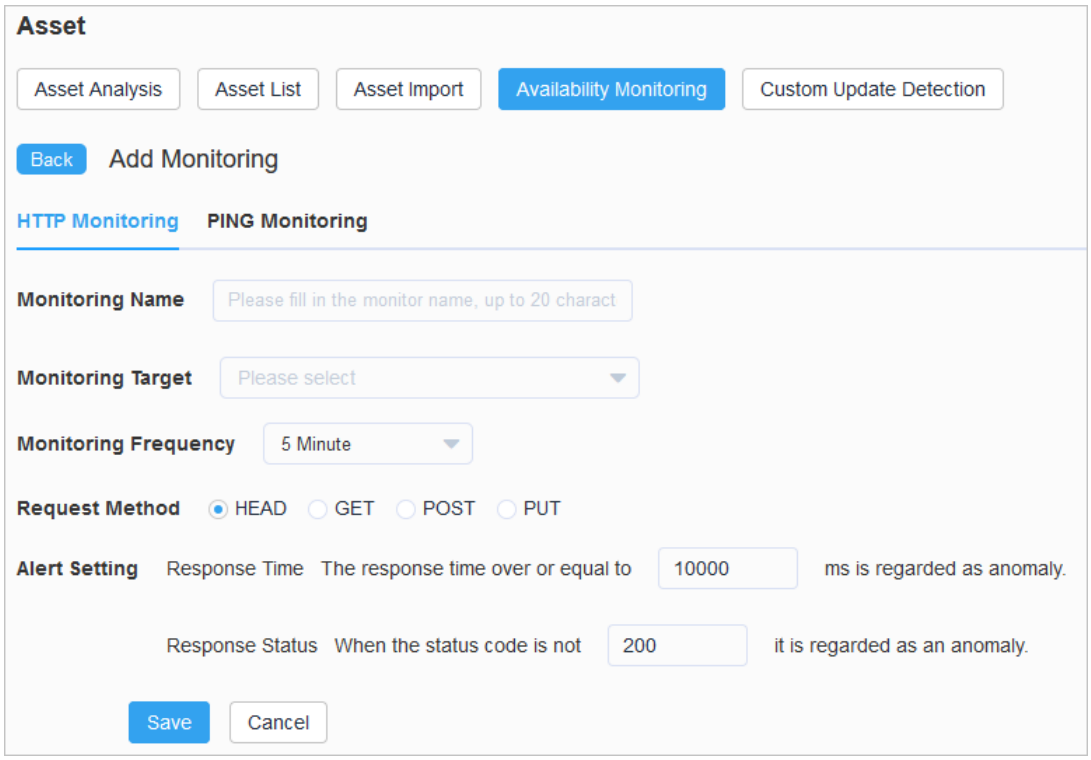


5. Create an availability monitoring task.

   Availability monitoring supports HTTP monitoring and PING monitoring.

   - To create an HTTP monitoring task, perform the following steps:
     a. Click **Add Monitoring**.

b. Click the **HTTP Monitoring** tab.



c. Configure the following parameters.

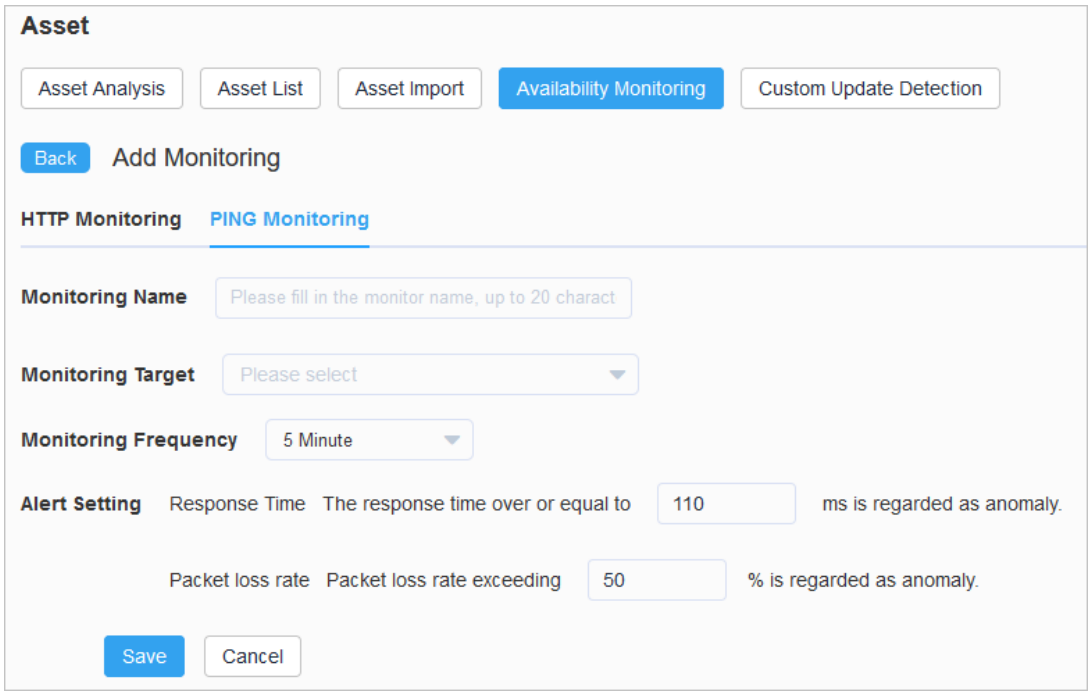
Parameter	Description
Monitoring Name	The name of the availability monitoring task.
Monitoring Target	The website that you want to monitor.
Monitoring Frequency	The interval at which you want to monitor the website. Valid values: **1 Minute**, **5 Minute**, **15 Minute**, and **30 Minute**.
Request Method	The request method that is used to send HTTP request packets. Valid values: **HEAD**, **GET**, **POST**, and **PUT**.
Alert Setting	The policy based on which Apsara Stack Security reports alerts. If one of the following conditions is met, the website is unavailable: ■ Response Time: If the actual response time is greater than the specified value, an exception occurs. ■ Response Status: If an unexpected status code is returned, an exception occurs.

d. Click **Save**.

- To create a PING monitoring task, perform the following steps:

a. Click **Add Monitoring**.

b. Click the **PING Monitoring** tab.



c. Configure the following parameters.

Parameter	Description
Monitoring Name	The name of the availability monitoring task.
Monitoring Target	The host that you want to monitor.
Monitoring Frequency	The interval at which you want to monitor the host. Valid values: **1 Minute**, **5 Minute**, **15 Minute**, and **30 Minute**.
Alert Setting	The policy based on which Apsara Stack Security reports alerts. If one of the following conditions is met, the host is unavailable: ■ Response Time: If the actual response time is greater than the specified value, an exception occurs. ■ Response Status: If an unexpected status code is returned, an exception occurs.

d. Click **Save**.

6. Manage more than one availability monitoring task at a time.

   You can manage more than one availability monitoring task in the monitoring task list at a time.

   - Start more than one availability monitoring task at a time.

     Select more than one availability monitoring task and choose **Batch Monitoring Manage > Batch Open Monitoring**.

   - Stop more than one availability monitoring task at a time.

     Select more than one availability monitoring task and choose **Batch Monitoring Manage > Batch Stop Monitoring**.

- Delete more than one availability monitoring task at a time.

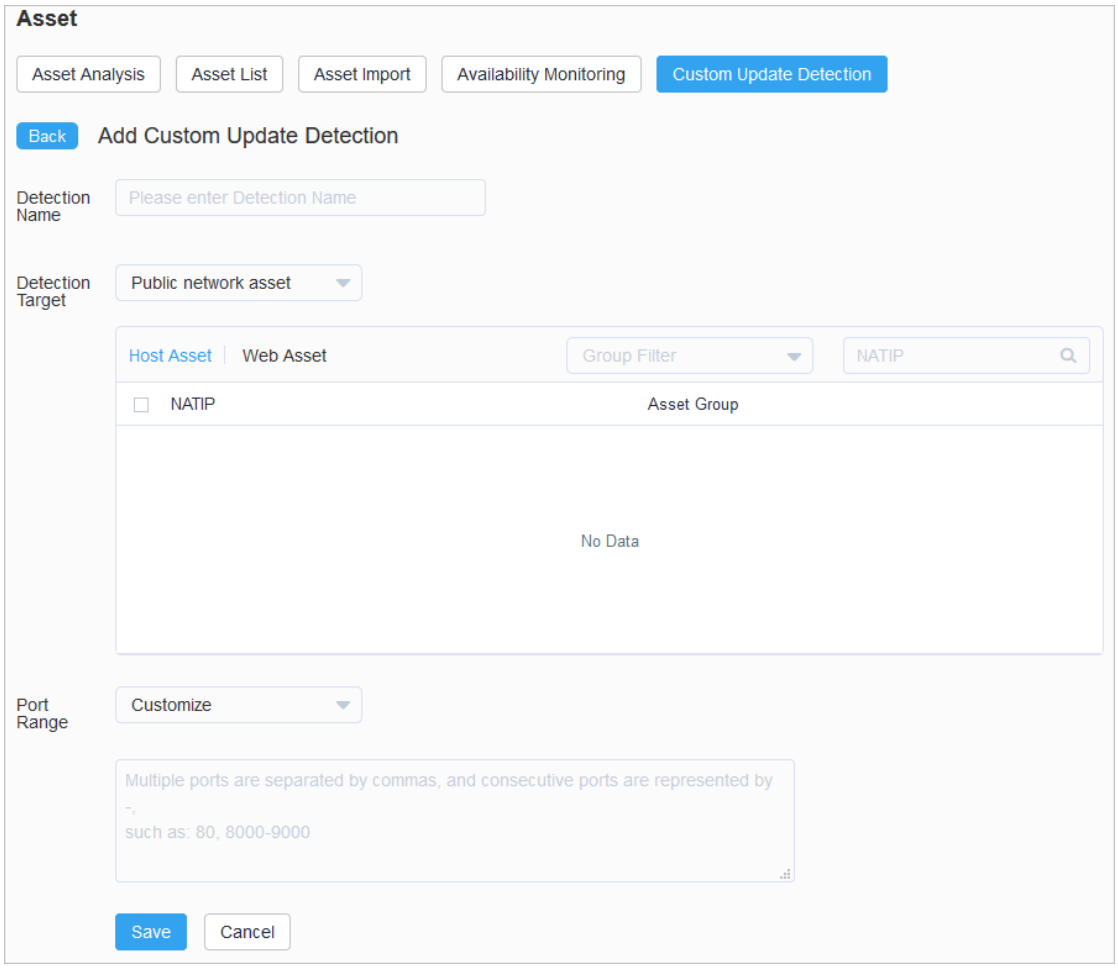
  Select more than one availability monitoring task and choose **Batch Monitoring Manage > Batch Delete Monitoring**.

4.8.3.5. Manage custom update detection tasks

This topic describes how to manage custom update detection tasks.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Asset**.
4. On the **Asset** page, click the **Custom Update Detection** tab to view custom update detection tasks.
5. Create a custom update detection task.
   i. Click **Add Detection**.
   ii. On the **Add Custom Update Detection** page, configure the parameters.



Parameter	Description
Detection Name	The name of the custom update detection task.
Detection Target	The asset that you want to detect. The value is fixed as **Public network asset**. a. Click **Host Asset** or **Web Asset** based on your business requirements. b. Select the assets that you want to detect from the asset list. **Note** You can search for assets by using **Group Filter** or NAT IP.
Port Range	The range of ports that you want to detect. Valid values: **Customize**, **Full Port**, **Top100**, and **Top1000**. **Note** The **Port Range** parameter appears only if you click Host Asset when you configure the **Detection Target** parameter. ■ **Customize**: You can specify custom ports to detect. ■ **Full Port**: All ports are detected. ■ **Top 100**: Top 100 ports are detected. ■ **Top 1000**: Top 1,000 ports are detected.

iii. Click **Save**.

4.8.4. Risk management

4.8.4.1. Manage vulnerabilities

This topic describes how to view and handle the vulnerabilities that are detected by the vulnerability scan feature.

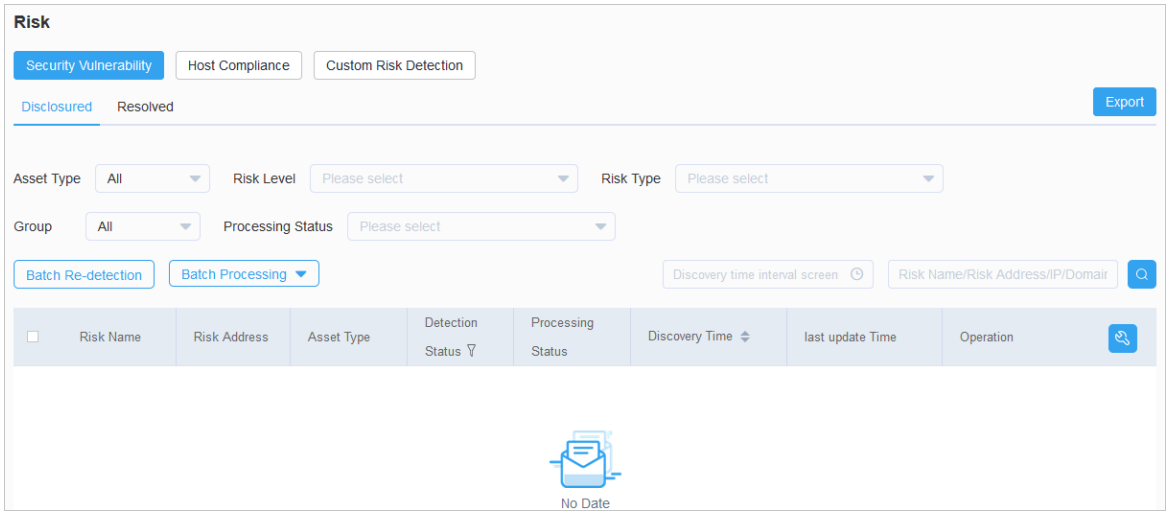
Context

On the **Security Vulnerability** tab, security administrators can view the vulnerabilities that are detected by the vulnerability scan feature.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Risk**.

4. On the **Risk** page, click the **Security Vulnerability** tab to view vulnerabilities.



   - Click the **Disclosured** or **Resolved** tab to view unfixed vulnerabilities or fixed vulnerabilities.
   - View risk statistics. The statistics include **Disclosured Risk**, **Resolved Risks**, **Unconfirmed Risk**, **Confirmed Risk**, and **Ignored Risk**.
5. Specify search conditions to view specific vulnerabilities. The conditions include **Asset Type** and **Risk Level**.
6. Handle vulnerabilities.

   Security administrators can analyze and confirm whether the vulnerabilities affect the security of assets based on the vulnerability information.

   - Confirm risks

     If a vulnerability affects the security of assets, confirm the risk after the security vulnerability is fixed.

     a. Find the vulnerability and click the icon in the **Operation** column.

     b. In the drop-down list, select **Confirm Risk**.

     c. In the dialog box that appears, click **OK**.
   - Ignore risks

     If a vulnerability is a false positive or does not affect the security of assets, ignore the risk.

     a. Find the vulnerability and click the icon in the **Operation** column.

     b. In the drop-down list, select **Ignore Risk**.

     c. In the dialog box that appears, click **OK**.
7. Click **Export** to export the list of vulnerabilities to your computer.

4.8.4.2. Manage host compliance risks

This topic describes how to view and confirm host compliance risks.

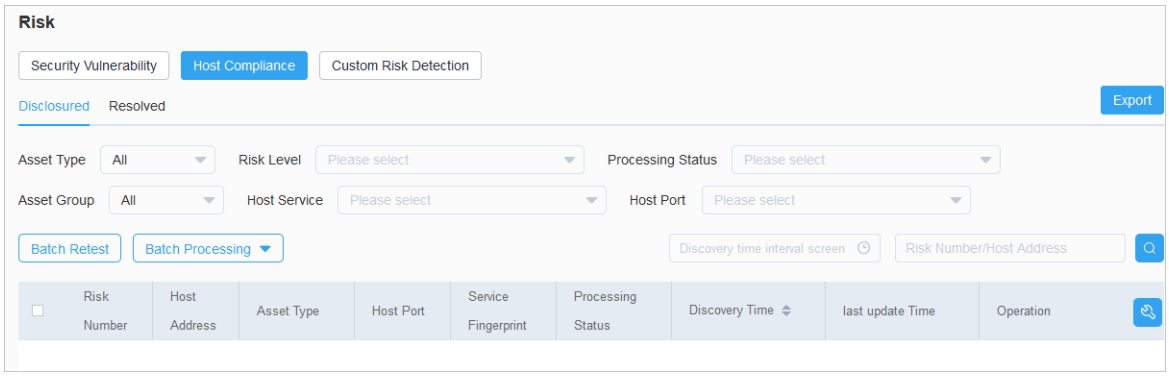
Context

On the **Host Compliance** tab, security administrators can view the host compliance issues that are detected by the vulnerability scan feature.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Risk**.
4. On the **Risk** page, click the **Host Compliance** tab to view host compliance risks.

   You can click the **Disclosured** or **Resolved** tab to view **unfixed vulnerabilities** or **fixed vulnerabilities**.



5. Specify conditions to search for host compliance risks. The conditions include **Asset Type** and **Risk Level**.
6. Handle host compliance risks.

   Security administrators can analyze and confirm whether host compliance risks affect the security of assets based on the risk information.

   - Confirm risks

     If a host compliance risk affects the security of assets, harden the security of hosts and confirm the risk.

     a. Find the risk and click the icon in the **Operation** column.

     b. In the drop-down list, select **Confirm Risk**.

     c. In the message that appears, click **Sure**.

   - Ignore risks

     If a host compliance risk proves to be a false positive or does not affect the security of assets, ignore the risk.

     a. Find the risk and click the icon in the **Operation** column.

     b. In the drop-down list, select **Ignore Risk**.

     c. In the message that appears, click **Sure**.
7. Click **Export** to export the list of host compliance risks to your computer.

4.8.4.3. Create a custom risk detection task

This topic describes how to create a custom risk detection task.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, choose **Risk > Custom Risk Detection**.
4. On the Custom Risk Detection tab, click **Add Detection**.
5. On the **Add Custom Risk Detection** page, configure the parameters.

Parameter	Description
Detection Name	The name of the custom risk detection task.
Detection Target	The asset on which you want to perform risk detection. The value is fixed as **Public network asset**.
Emergency Detection	The switch that is used to enable or disable the emergency detection feature. If you enable this feature, you can select emergency detection items from the detection item list.
Basic Risk Detection	The switch that is used to enable or disable the basic risk detection feature. For more information about how to configure this feature, see Configure basic monitoring.
WEB Risk Detection	The switch that is used to enable or disable the web risk detection feature. For more information about how to configure this feature, see Configure web monitoring.

6. Click **Save**.

4.8.5. Report management

4.8.5.1. Create a report

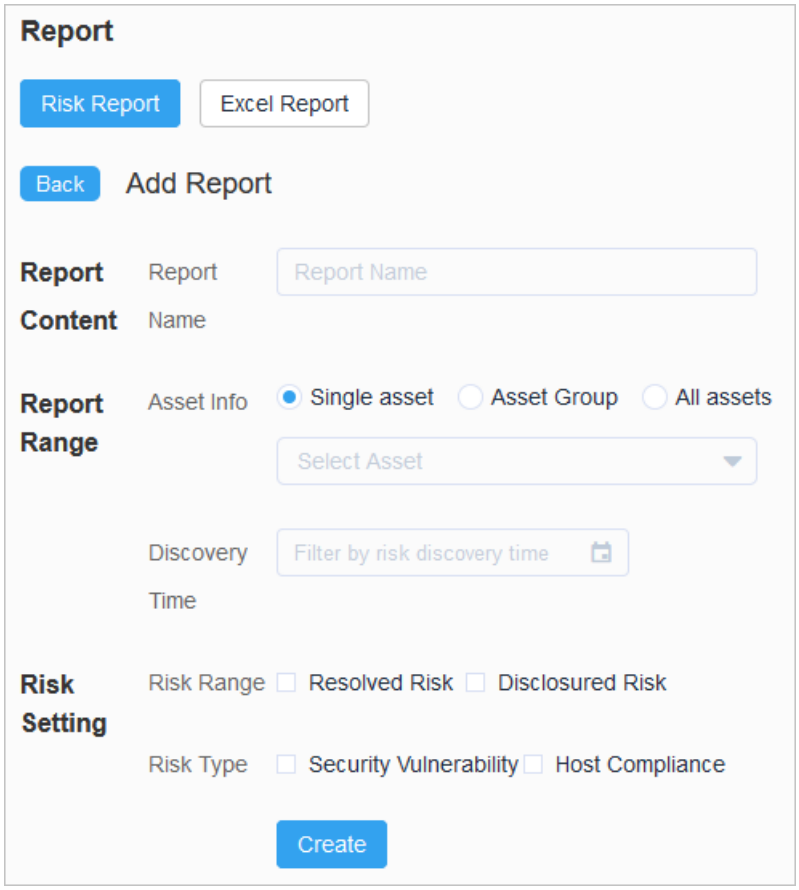
This topic describes how to create a report.

Context

A security administrator can create a report to view the security postures of specific assets during a period of time and implement security measures as required.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Report**.
4. On the **Risk Report** tab, click **Add Report**.
5. Configure the following parameters.



Parameter		Description
Report Content	**Report Name**	The name of the report that you want to create.
Report Range	**Asset Info**	The scope of assets that you want to include in the report. Valid values: **Single asset**, **Asset Group**, and **All assets**. ○ **Single asset**: Select an asset. ○ **Asset Group**: Select an asset group and a tag. **Note** After you select an asset group and a tag, the assets in the group that have the selected tag are included in the report. ○ **All assets**: Select assets by tag.
	Discovery Time	The time range in which you want to perform risk detection.

Parameter		Description
Risk Setting	Risk Range	The scope of risks that you want to include in the report. Valid values: **Resolved Risk** and **Disclosured Risk**.
	Risk Type	The types of risks that you want to include in the report. Valid values: **Security Vulnerability** and **Host Compliance**.

6. Click **Create**.

Result

After the report is created, it appears in the report list on the **Report** page.

4.8.5.2. Delete multiple reports at a time

This topic describes how to delete multiple reports at a time.

Context

You can delete multiple reports that you no longer need at a time to save storage space.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Report**.
4. Click **Risk Report**.
5. In the report list, select the reports that you want to delete.
6. Click **Batch Delete**.

4.8.6. Configuration management

4.8.6.1. Configure overall monitoring

This topic describes how to configure overall monitoring for the vulnerability scan feature. Overall monitoring includes Asset Monitoring Configuration, Base Risk Monitoring Configuration, External Risk Monitoring Configuration, and Scan Configuration.

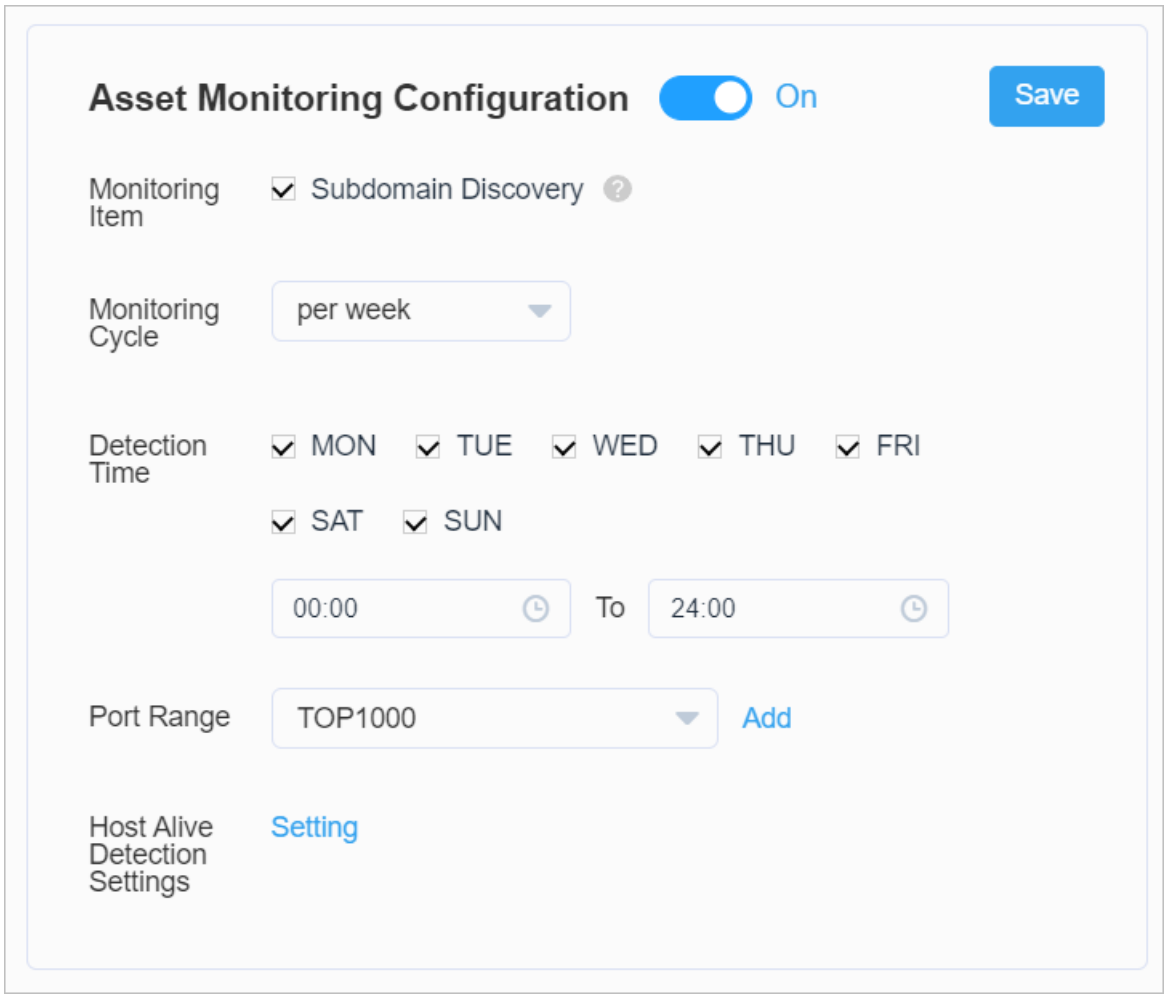
Context

Overall monitoring allows you to configure detection features and the monitoring cycle for each detection feature.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.

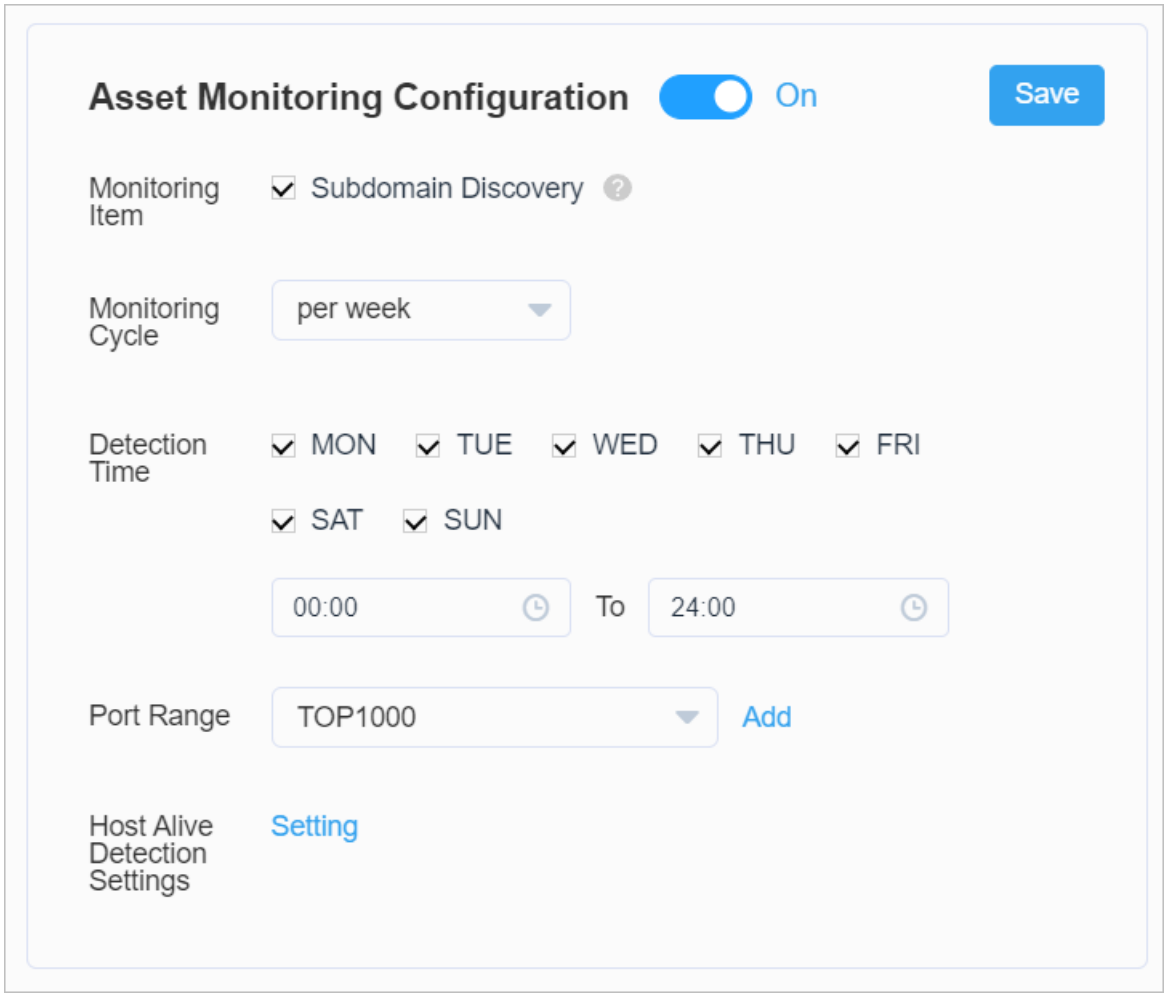
3. In the left-side navigation pane, click **Configuration**.
4. On the **Monitoring Configuration** tab, click **Overall Monitoring**.
5. In the **Monitoring Status** section, view the status of overall monitoring.



6. Configure detection features.

   Detection features include **Asset Monitoring Configuration**, **Base Risk Monitoring Configuration**, **External Risk Monitoring Configuration**, and **Scan Configuration**.

In this step, the **Asset Monitoring Configuration** detection feature is used as an example.



i. Turn on Asset Monitoring Configuration to enable the asset monitoring feature.

- After the switch is turned on, the switch is in the **On** state. In the On state, the switch is blue. After the switch is turned off, the switch is in the **Off** state. In the Off state, the switch is gray.
- You must turn on **Asset Monitoring Configuration** and **Base Risk Monitoring Configuration** to enable the two features. External Risk Monitoring Configuration and Scan Configuration are automatically enabled.

ii. Configure the following parameters.

Asset Monitoring Configuration

Parameter	Description

Parameter	Description
Monitoring Item	The item that you want to monitor. Valid value: **Subdomain Discovery**. If you want to import assets, you must set the Import Set parameter to **Auto Import subdomains**. Then, subdomains are automatically imported. If you select **Subdomain Discovery**, Apsara Stack Security regularly discovers subdomains for assets whose Import Set parameter is set to **Auto Import subdomains**.
Monitoring Cycle	The cycle based on which you want to perform detection. Valid values: **customization**, **per week**, and **per month**. ■ **customization**: Specify the interval at which you want to perform detection. Unit: days. ■ **per week**: Specify the days of each week on which you want to perform detection. ■ **per month**: Specify the days of each month on which you want to perform detection.
Detection Time	The time when you want to perform detection. The time varies based on the value of the **Monitoring Cycle** parameter. ■ If you set the **Monitoring Cycle** parameter to **customization**, select a time range of the day in which you want to perform detection. ■ If you set the **Monitoring Cycle** parameter to **per week**, select the days of each week and the time range in which you want to perform detection. ■ If you set the **Monitoring Cycle** parameter to **per month**, select the days of each month and the time range in which you want to perform detection. **Note** For example, if you set the **Monitoring Cycle** parameter to **per week** and select **Monday** to **Sunday** and 00:00:00 to 24:00:00 for the **Detection Time** parameter, Apsara Stack Security performs detection 24 hours a day, 7 days a week.
Port Range	The ports on which you want to perform detection. Valid values: **customization**, **Full port**, **TOP100**, and **TOP1000**. ■ **customization**: Specify the ports to scan. ■ **Full port**: Scan all ports. ■ **TOP100**: Scan top 100 ports. You can click **Add** to add more ports. ■ **TOP1000**: Scan top 1,000 ports. You can click **Add** to add more ports.

Parameter	Description
Host Alive Detection Settings	The option that is used to check whether a host is running. By default, the ping feature is used to check whether a host is running. If the host has the ping feature disabled, the status of the host is checked based on top 20 ports and custom ports. To specify custom ports, click **Settings**. In the Host Alive Detection Settings dialog box, specify the ports in the **Custom Port** field.

Base Risk Monitoring Configuration

Parameter	Description
Monitoring Item	The item that you want to monitor. Valid values: **Weak Password**, **Common Vulnerabilities**, **Baseline Monitoring**, and **Host Compliance**. ■ **Weak Password**: Attackers can guess passwords or launch brute-force attacks to crack passwords. Then, the attackers can obtain relevant permissions. If you select this item, weak password vulnerabilities can be identified. ■ **Common Vulnerabilities**: Web vulnerabilities and CMS application vulnerabilities are included. If you select this item, common vulnerabilities can be identified. This way, you can install patches at the earliest opportunity. ■ **Baseline Monitoring**: Risks in host configuration and account configuration are detected. ■ **Host Compliance**: Host compliance risks are detected.
Monitoring Cycle	The cycle based on which you want to perform detection. Valid values: **customization**, **per week**, and **per month**. ■ **customization**: Specify the interval at which you want to perform detection. Unit: days. ■ **per week**: Specify the days of each week on which you want to perform detection. ■ **per month**: Specify the days of each month on which you want to perform detection.

Parameter	Description
Detection Time	The time when you want to perform detection. The time varies based on the value of the **Monitoring Cycle** parameter. ■ If you set the **Monitoring Cycle** parameter to **customization**, select a time range of the day in which you want to perform detection. ■ If you set the **Monitoring Cycle** parameter to **per week**, select the days of each week and the time range in which you want to perform detection. ■ If you set the **Monitoring Cycle** parameter to **per month**, select the days of each month and the time range in which you want to perform detection. **Note** For example, if you set the **Monitoring Cycle** parameter to **per week** and select **Monday** to **Sunday** and 00:00:00 to 24:00:00 for the **Detection Time** parameter, Apsara Stack Security performs detection 24 hours a day, 7 days a week.

External Risk Monitoring Configuration

Parameter	Description
Monitoring Item	The item that you want to monitor. Valid value: **Code Disclosure**. If you select Code Disclosure, Apsara Stack Security detects leaked source code of your assets.
Monitoring Cycle	The cycle based on which you want to perform detection. Valid values: **customization**, **per week**, and **per month**. ■ **customization**: Specify the interval at which you want to perform detection. Unit: days. ■ **per week**: Specify the days of each week on which you want to perform detection. ■ **per month**: Specify the days of each month on which you want to perform detection.

Parameter	Description
Detection Time	The time when you want to perform detection. The time varies based on the value of the **Monitoring Cycle** parameter. ■ If you set the **Monitoring Cycle** parameter to **customization**, select a time range of the day in which you want to perform detection. ■ If you set the **Monitoring Cycle** parameter to **per week**, select the days of each week and the time range in which you want to perform detection. ■ If you set the **Monitoring Cycle** parameter to **per month**, select the days of each month and the time range in which you want to perform detection. **Note** For example, if you set the **Monitoring Cycle** parameter to **per week** and select **Monday** to **Sunday** and 00:00:00 to 24:00:00 for the **Detection Time** parameter, Apsara Stack Security performs detection 24 hours a day, 7 days a week.

Scan Configuration

Parameter	Description
Risk Re-detection	The time at which you want to perform detection again. If risks are detected in assets, Apsara Stack Security scans the assets again each day at the time you specify.
Asset Scanning Rate	The asset scan rate. Valid values: **Slow Mode**, **General Mode**, **Fast Mode**, and **Turbo Mode**.
Risk Scanning Rate	The risk scan rate. Valid values: **Slow Mode**, **General Mode**, and **Fast Mode**.
UserAgent Setting	The User-Agent property.

iii. Click **Save**.

4.8.6.2. Configure basic monitoring

This topic describes how to configure basic monitoring.

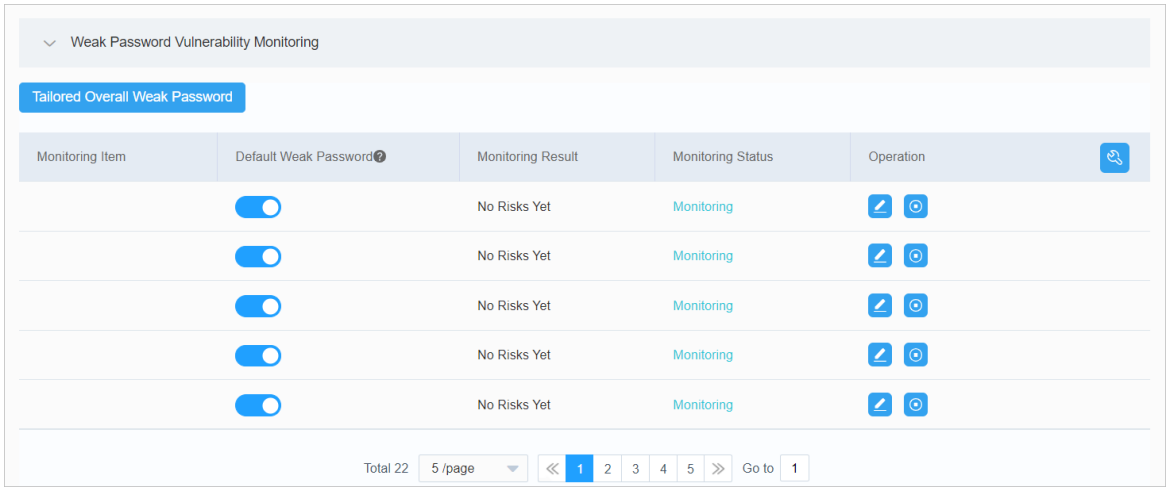
Context

Basic monitoring includes Weak Password Vulnerability Monitoring, Operation Security Vulnerability Monitoring, CMS Application Vulnerability Monitoring, and Baseline Monitoring.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.

3. In the left-side navigation pane, click **Configuration**.
4. On the **Configuration** page, click the **Monitoring Configuration** tab.
5. Click the **Basic Monitoring** tab. Then, click **Weak Password Vulnerability Monitoring** to configure rules to monitor weak passwords.



   - By default, all monitoring items on weak passwords use the default weak password library.
   - To disable a monitoring item, perform the following step:

     Find the monitoring item and click the icon in the **Operation** column.

   - To enable a monitoring item, perform the following step:

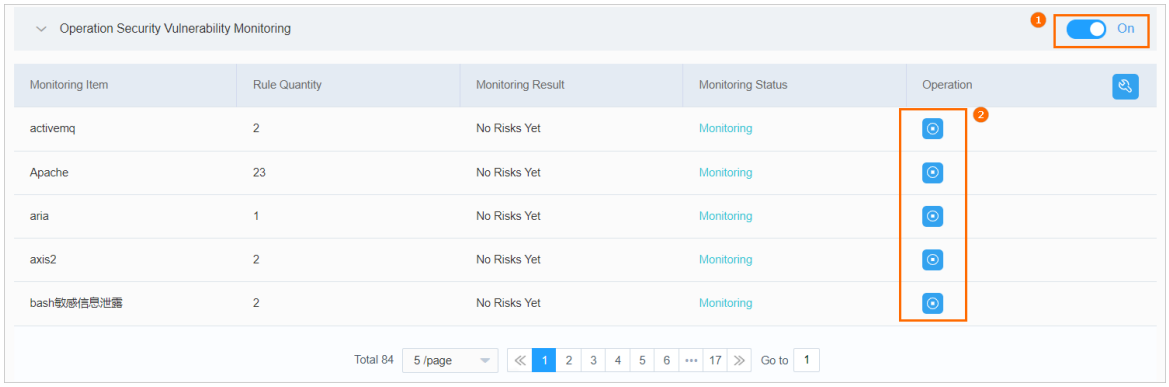
     Find the monitoring item and click the icon in the **Operation** column.

   - To specify custom weak passwords for a monitoring item, perform the following steps. In this example, **MySQL Weak Password Vulnerability** is used.
     a. In the **Default Weak Password** column, turn off the switch. The switch status changes to .
     b. In the **Operation** column, click the icon.
     c. In the **Customize MySQL Weak Password** dialog box, specify custom weak passwords.
     d. Click **Yes**.
   - To apply the same custom weak passwords to multiple monitoring items, perform the following steps:
     a. In the **Default Weak Password** column, turn off the switches for the monitoring items to which you want to apply the same custom weak passwords. The switch status changes to .

        > **Note** If you want to apply a custom weak password to a monitoring item, you must turn off the switch in the Default Weak Password column of the monitoring item.

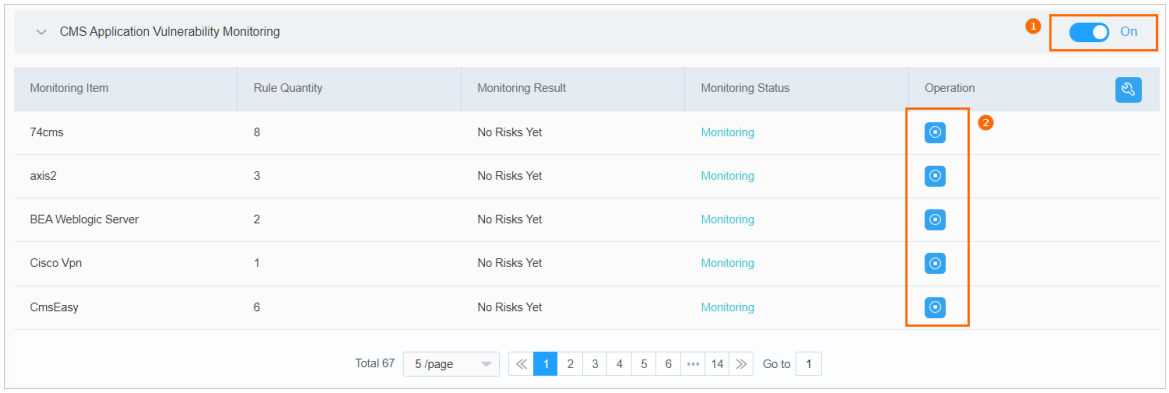
     b. Click **Tailored Overall Weak Password**.
     c. In the **Tailored Overall Weak Password** dialog box, specify custom weak passwords.
     d. Click **Yes**.

6. Click **Operation Security Vulnerability Monitoring** and configure O&M vulnerability monitoring.



No.	Description
1	The switch that is used to enable or disable the **Operation Security Vulnerability Monitoring** feature. We recommend that you enable this feature to enhance system security.
2	The switch that is used to enable or disable a monitoring item. You can disable monitoring items based on your business requirements.

7. Click **CMS Application Vulnerability Monitoring** and configure monitoring on content management system (CMS) application vulnerabilities.



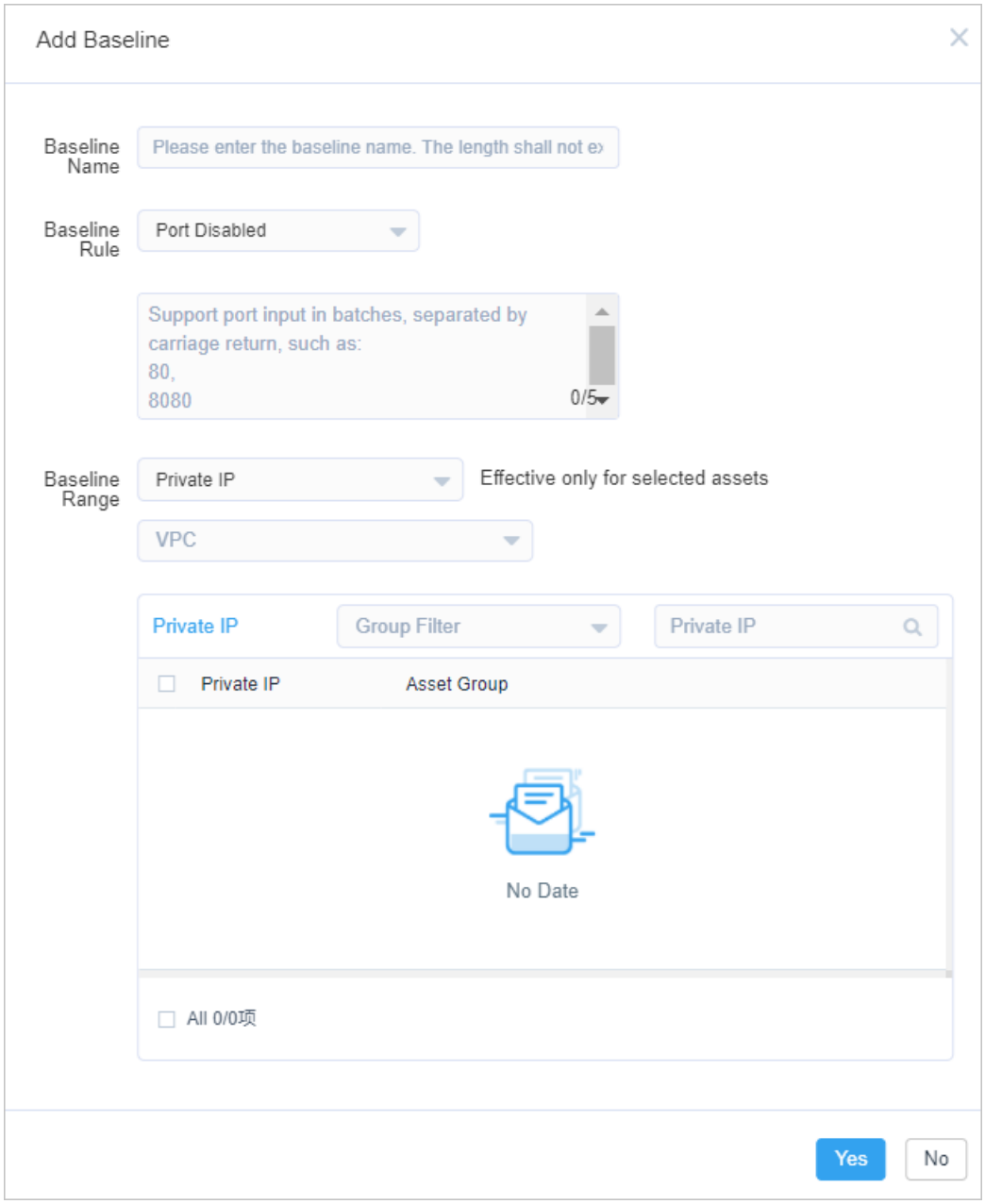
No.	Description
1	The switch that is used to enable or disable the **CMS Application Vulnerability Monitoring** feature. We recommend that you enable this feature to enhance system security.
2	The switch that is used to enable or disable a monitoring item. You can disable monitoring items based on your business requirements.

8. Click **Baseline Monitoring** and configure baseline monitoring.

   To add a baseline monitoring item, perform the following steps:

i. Click **Add**.

ii. In the **Add Baseline** dialog box, configure the baseline monitoring item.



In this example, a baseline monitoring item is added to block Telnet-based access.

Parameter	Description
Baseline Name	The name of the baseline monitoring item. Example: Block Telnet-based access.

Parameter	Description
Baseline Rule	The detection rule that is used by the baseline monitoring item. This rule checks whether hosts use disabled ports or run disabled services. Valid values: ■ **Port Disabled**: ports that you want to disable. Example: 23. ■ **Service Disabled**: services that you want to disable. Example: Telnet.
Baseline Range	The scope of assets to which the baseline monitoring item can be applied. Valid values: **Private IP** and **NatIP**. You must specify this parameter and select assets.

iii. Click **Yes**.

4.8.6.3. Configure web monitoring

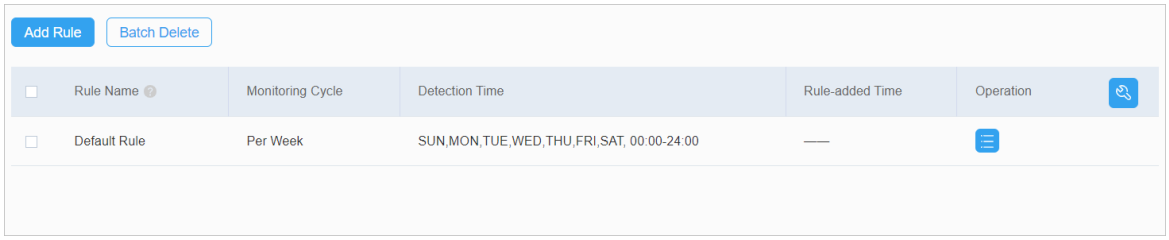
This topic describes how to configure web monitoring.

Context

Web monitoring allows you to configure monitoring items for monitoring web vulnerabilities. You can also configure conditions to block website crawlers.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Configuration**.
4. On the **Monitoring Configuration** tab, click the **Web Monitoring** tab to view existing rules.



> **Note** **Default rule** is created by the system. You can only view details of the default rule, but cannot modify or delete it.

5. Create a web monitoring rule.
   i. Click **Add Rule**.
   ii. On the **Add Web Monitoring Rule** page, configure the following parameters.

Parameter	Description
Rule Name	The name of the web monitoring rule.

Parameter	Description
Monitoring Cycle	The monitoring cycle. Valid values: **Customization**, **Per Week**, and **Per Month**. ■ **Customization**: Specify the interval at which you want to perform detection. ■ **Per Week**: Specify the days of each week on which you want to perform detection. ■ **Per Month**: Specify the days of each month on which you want to perform detection.
Detection Time	The time when you want to perform detection. The time varies based on the value of the **Monitoring Cycle** parameter. ■ If you set the **Monitoring Cycle** parameter to **Customization**, select a time range of the day in which you want to perform detection. ■ If you set the **Monitoring Cycle** parameter to **Per Week**, select the days of each week and the time range in which you want to perform detection. ■ If you set the **Monitoring Cycle** parameter to **Per Month**, select the days of each month and the time range in which you want to perform detection. **Note** For example, if you set the **Monitoring Cycle** parameter to **Per Week** and select **Monday** to **Sunday** and 00:00:00 to 24:00:00 for the **Detection Time** parameter, Apsara Stack Security performs detection 24 hours a day, 7 days a week.
Monitoring Options	The types of the web vulnerabilities that you want to monitor. Supported operations: **Select All**, **Inverse**, and **Clear**.
UserAgent	The User-Agent field of an HTTP request packet. The User-Agent field identifies the application type, operating system, software developer, and version number of the proxy software that initiates the request.
Cookies	The cookie parameters.
Key Page	The web directories or pages that you want to monitor.
Excluded Page	The web directories or pages that you do not want to monitor.
Crawler Depth	The capturing depth of crawlers. Valid values: **10**, **15**, and **30**.
URL Numbers	The number of URLs that are used for crawling. Valid values: **500**, **1000**, and **2000**.
scanning Frequency	The scan frequency of web monitoring. Valid values: **Request 10 Times Per Second** and **Request 15 Times Per Second**.

iii. Click **Yes**.

6. Manage the web monitoring rule.

Icon	Description
	Modify the rule.
	Delete the rule.
Batch Delete	If you want to delete multiple rules, select the rules and click **Batch Delete**.

4.8.6.4. Configure a whitelist

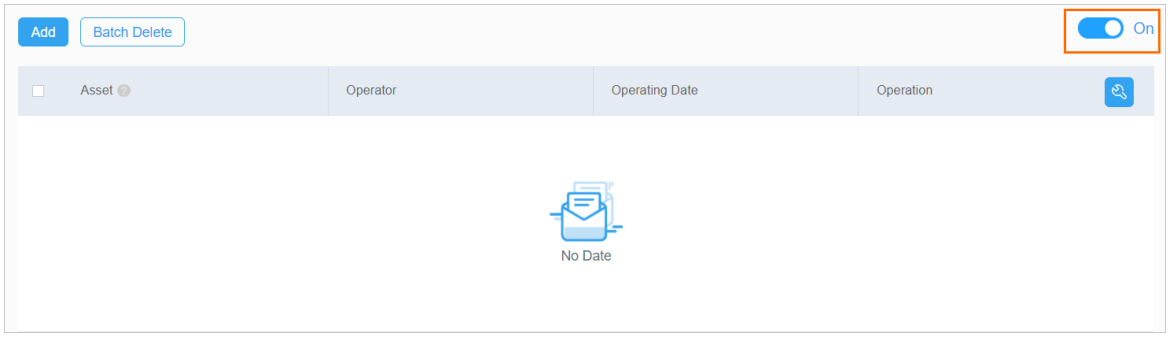
This topic describes how to configure a whitelist.

Context

Apsara Stack Security does not scan the assets that are added to a whitelist. Before you add assets to a whitelist, make sure that the assets are secure.

Procedure

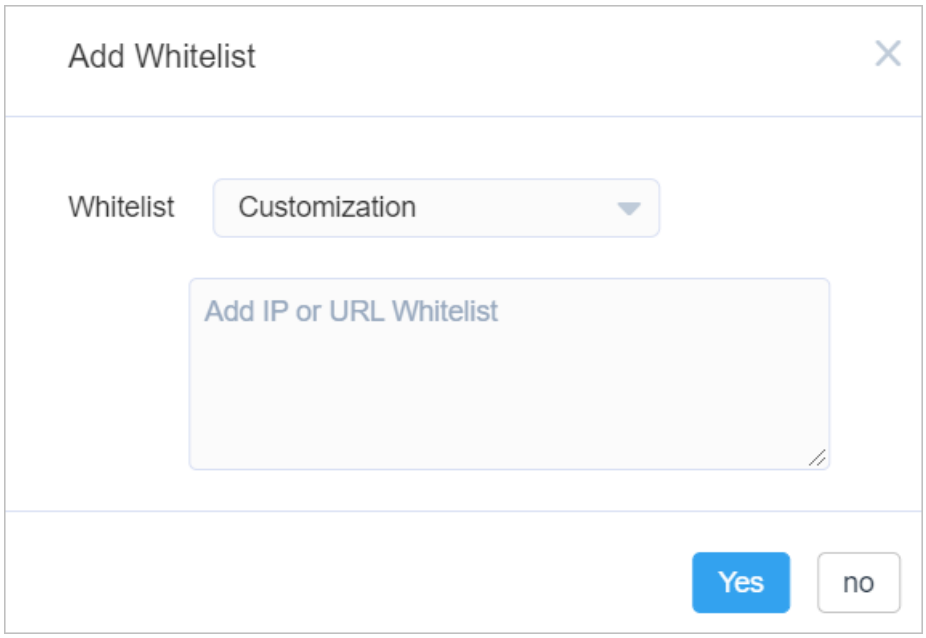
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Configuration**.
4. On the Configuration page, click the **Monitoring Configuration** tab. Then, click the **Whitelist** tab to view the assets that are added to a whitelist.



Note By default, the whitelist feature is enabled. If you do not want to use the whitelist feature, turn off the switch in the upper-right corner.

5. Add assets to a whitelist.
   i. Click **Add**.

ii. In the **Add Whitelist** dialog box, configure the parameters.



- If you select **Asset Group** for the **Whitelist** parameter, select a group from the second drop-down list. The assets in this group are added to the whitelist.
- If you select **Customization** for the **Whitelist** parameter, enter the IP addresses or URLs that you want to add to the whitelist in the field that appears.

iii. Click **Yes**.

6. Manage the assets that are added to a whitelist.
   - Remove an asset from a whitelist

     Find the asset and click the icon in the **Operation** column to delete the asset.
   - Remove multiple assets from a whitelist at a time

     Select the assets and click **Batch Delete** to remove the assets from a whitelist at a time.

4.8.6.5. Configure a scan engine for internal assets

This topic describes how to configure a scan engine for internal assets, such as the assets of a virtual private cloud (VPC).

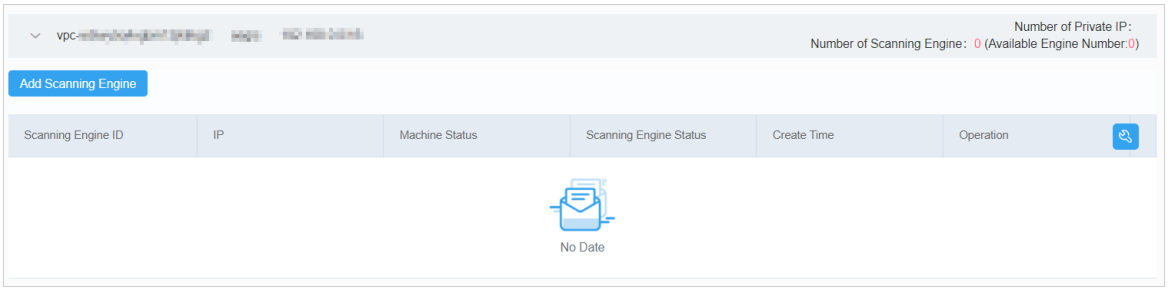
Context

You must add a scan engine for a VPC before you can scan for vulnerabilities on the assets of the VPC.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Security Management** section, click **Cloud Security Scanner**.
3. In the left-side navigation pane, click **Configuration**.
4. On the **Configuration** page, click the **Scan Engine Manage** tab.
5. Click the **Private-sector assets** tab.

6. Click the name of the VPC whose assets you want to scan.



7. Click **Add Scan Engine**.
8. In the **Add Scan Engine** dialog box, select a vSwitch for the VPC from the **vSwitch** drop-down list.
9. Click **OK**.

4.9. Create a security report

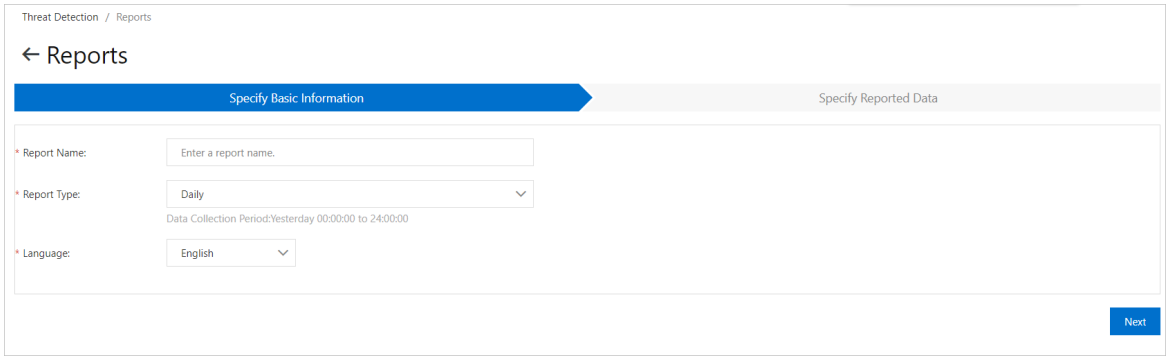
Security reports help monitor the security status of your assets. You can specify the content, types of statistics, and email addresses of recipients to create a security report. This topic describes how to create a security report.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Security Management** section, click **Threat Detection**.
3. In the left-side navigation pane,click **Security Reports**.
4. On the **Reports** page, click **Create Report**.

> **Notice** In addition to the default security report created by Apsara Stack Security, you can create a maximum of nine security reports.

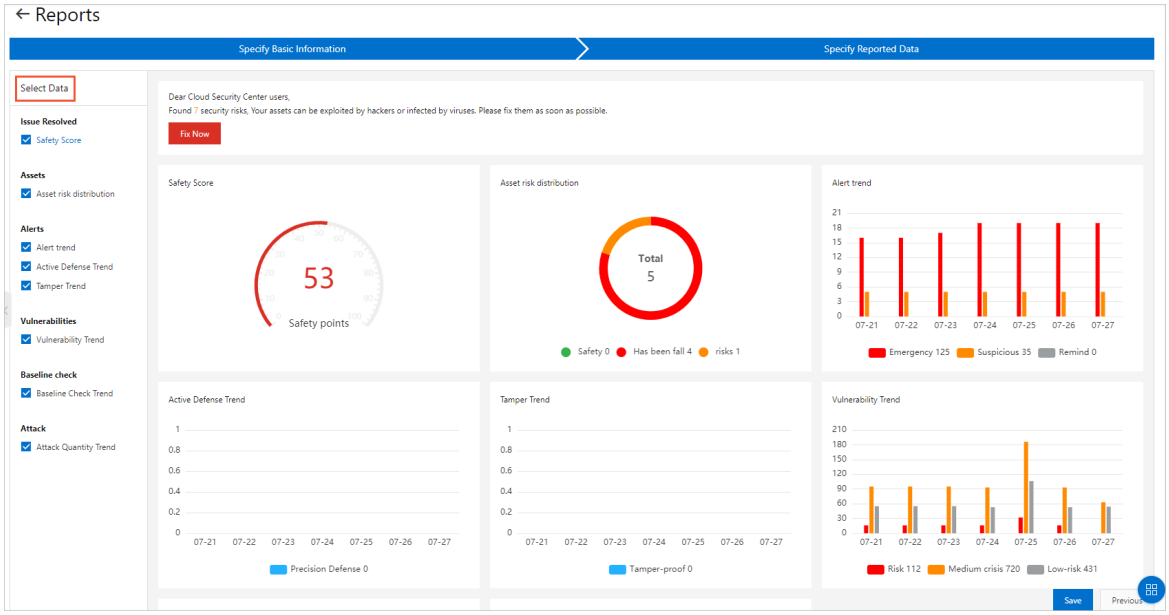
5. In the **Specify Basic Information** step, configure the parameters.



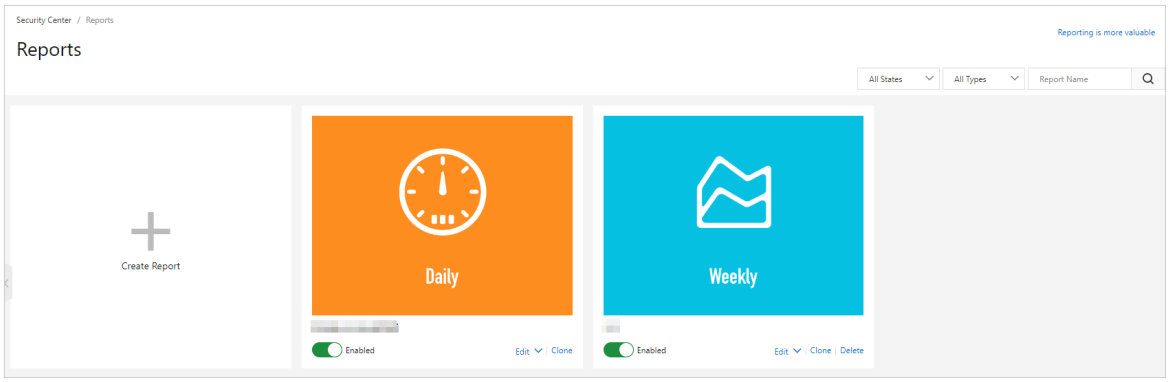
Configure the following parameters:

- **Report Name**: Enter a name for the security report.
- **Report Type**: Select a report type from the drop-down list. Valid values: *Daily*, *Weekly*, and *Monthly*.
- **Language**: Select a natural language for the report. Valid values: **简体中文** and **English**.

6. Click **Next**.
7. In the **Specify Reported Data** step, select the types of data that you want to view in the security report. You can select assets, alerts, vulnerabilities, baselines, attacks, and other data related to security operations.



8. Click **Save report content**. The security report is created.
   You can view the newly created security report on the **Reports** page.



5.Network Traffic Monitoring System

5.1. View traffic trends

This topic describes how to view the network traffic trends and the statistics about inbound and outbound traffic.

Context

The security administrator can analyze traffic trends and obtain the traffic rate, peaks, and troughs. The security administrator can also view the top five IP addresses that have the largest volume of traffic and identify malicious IP addresses.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Network Security > Network Traffic Monitoring**.
3. In the upper-right corner of the **Traffic Trends** page, select the time range, which can be **Last 1 Hour**, **Last 24 Hours**, or **Last 7 Days**.
4. View network traffic information.
   - Network traffic trends

     View the network traffic trends in the time range that you selected. The network traffic trends include the trend of inbound traffic and the trend of outbound traffic. The inbound and outbound traffic is measured in bit/s.
   - Inbound Traffic

     View the information about Inbound Sessions, Inbound Applications, and Destination IPs with Most Requests.
   - Outbound Traffic

     View the information about Outbound Sessions, Outbound Applications, and Source IPs with Most Requests.
5. (Optional)Click the icon to export traffic trends as a PDF file.

5.2. View traffic at the Internet border

This topic describes how to view traffic at the Internet border. You can obtain up-to-date information about network security.

Prerequisites

The Network Traffic Monitoring System module is purchased and deployed at the egress (ISW) of Apsara Stack. **This module is used to audit, analyze, and manage both inbound and outbound traffic at Internet borders.**

Context

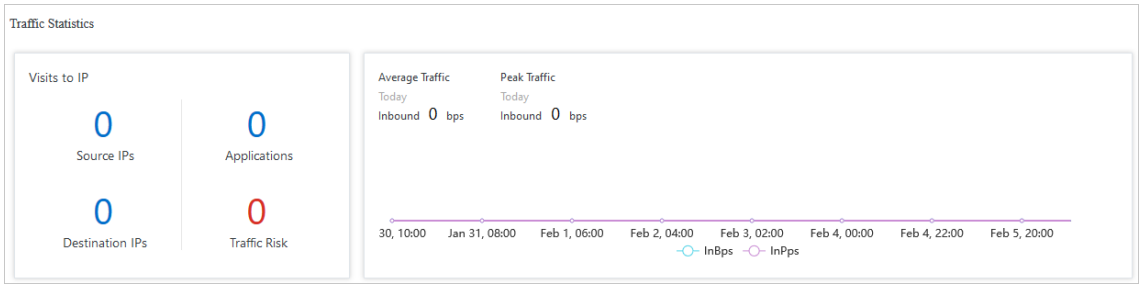
You can use traffic information to identify abnormal Internet traffic and block malicious requests.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Internet Border**.
4. Specify traffic filter conditions.

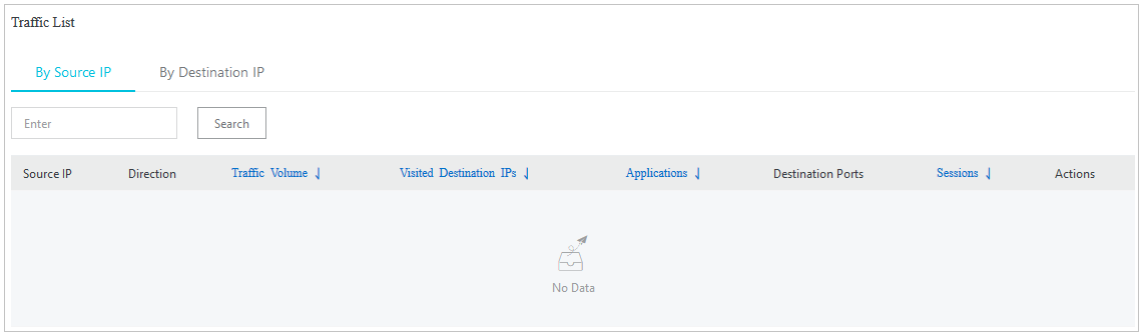
Item	Description
1	Specify the traffic direction. Valid values: *Inbound* and *Outbound*. ○ *Inbound*: The traffic flows from the Internet to the internal network. ○ *Outbound*: The traffic flows from the internal network to the Internet.
2	Specify whether you want to view the traffic from the IP address or application dimension. Valid values: *By IP* and *By Application*.
3	Specify the time range. Valid values: *Last 1 Hour*, *Last 24 Hours*, and *Last 7 Days*.

5. View details about the traffic at the Internet border.
   - **Traffic Statistics**



     - The **Visits to IP** section includes **Source IPs**, **Destination IPs**, **Applications**, and **Traffic Risk**.
     - In the traffic chart on the right, you can view **Average Traffic**, **Peak Traffic**, and traffic trends.

   - **Traffic List**



In the **Traffic List** section, you can view traffic details.

6. In the **Traffic List** section, view abnormal traffic of the specified IP address.
   - If *Inbound* is specified, you can view abnormal traffic on the **By Destination IP** tab of the **Traffic List** section.
   - If *Outbound* is specified, you can view abnormal traffic in the **Traffic List** section.

5.3. View traffic at the internal network border

This topic describes how to view the traffic at the internal network border. You can obtain up-to-date information about network security based on the traffic.

Prerequisites

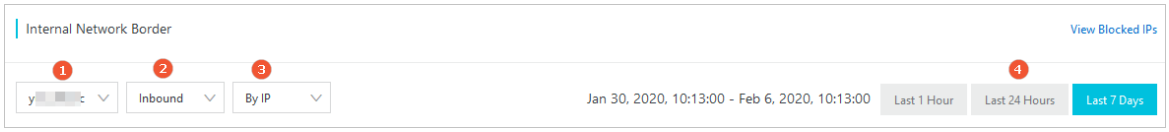
The Network Traffic Monitoring System module is purchased and deployed at the ingress (CSW) of Apsara Stack. **You can use this module to audit, analyze, and manage inbound and outbound traffic that is routed over leased lines between data centers and virtual private clouds (VPCs).**

Context

You can identify abnormal traffic from the internal network based on traffic information and block malicious requests.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Network Security > Network Traffic Monitoring**.
3. In the left-side navigation pane, click **Internal Network Border**. On the **Internal Network Border** page, specify traffic filter conditions.



Item	Description
1	Select a VPC name from the drop-down list.
2	Specify the traffic direction. Valid values: *Inbound* and *Outbound*. ○ *Inbound*: The traffic flows from the Internet to the internal network. ○ *Outbound*: The traffic flows from the internal network to the Internet.
3	Specify whether you want to view the traffic that flows through the internal network border by IP address or application. Valid values: *By IP* and *By Application*.

Item	Description
4	Specify the time range. Valid values: *Last 1 Hour*, *Last 24 Hours*, and *Last 7 Days*.

4. View details about the traffic at the internal network border.
   - **Traffic Statistics**
     - The **Visits to IP** section includes **Source IPs**, **Destination IPs**, **Applications**, and **Traffic Risk**.
     - In the traffic chart on the right, you can view the average traffic, peak traffic, and traffic trends.
   - **Traffic List**
     - In the **Traffic List** section, you can select **By Source IP** or **By Destination IP** to view traffic details by source or destination IP address.
     - If **By IP** is specified, you can view the abnormal traffic of the specified IP address in the **Traffic List** section.

5.4. Create packet capture tasks

This topic describes how to create a packet capture task. You can enable the packet capture feature to capture network data packets of IP addresses and ports, and then analyze the packets. This way, you can diagnose faults, analyze attacks, and identify security risks to network communications.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Packet Capture**.
4. On the **Packet Capture** page, click **Create Packet Capture Task**.
5. In the **Create Packet Capture Task** panel, configure parameters and click **OK**.

Parameter	Description
Task Name	The name of the packet capture task. We recommend that you enter an informative name, such as a name that indicates the purpose of the task.
Maximum Bytes	The maximum number of bytes that can be captured in a packet. If the number of bytes in a packet exceeds this value, the excessive bytes are discarded.
Duration (s)	The maximum duration of the packet capture task. Unit: seconds.

Parameter	Description
Protocol	The transmission protocol of packets. Valid values: ○ **All** ○ **TCP** ○ **UDP** ○ **ICMP**
IP Address Type	The IP protocol of packets. Valid values: **IPV4** and **IPV6**.
Direction	The direction of packets. Valid values: **Bidirectional**, **In**, and **Out**.
IP	The **IP address** of packets.
Port	The **port** of packets.

Result

You can go to the **Packet Capture** page to view the packet capture task that you created and the status of the task.

5.5. Search for logs

This topic describes how to search for and view logs.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Log Retrieval**.
4. On the **Retrieval** page, specify search conditions.

Search condition	Description
Time	Specify the time range of the logs that you want to search. Valid values: **Last Hour**, **Last 4 Hours**, **Today**, **Last 7 Days**, **Last 14 Days**, **Last 30 Days**, and **Custom**.
All Departments	Select the department to which the logs belong.
Log Type	Select the type of logs that you want to search. Valid values: **Security event log** and **Full traffic log**.
Search Template	Select a template for log search. You can save search conditions as a template.
Content	Enter the content of the logs.

5. Click the **Search** icon to view the search results.
   - **Clear**: Click **Clear** to clear the specified search conditions.
   - **Save**: Click **Save** if you want to reuse the specified search conditions. In the dialog box that

appears, specify **Name** to save the search conditions as a template.

The system displays logs of Apsara Stack Security in a column chart based on the specified search conditions. You can view the numbers of logs at different points in time within the specified time range.

In the lower part of the Log Retrieval page, you can view the details of the returned logs. You can also click the parameters in the log list to add the parameters to search conditions.

- Select the fields that you want to display in the log list: Select the fields in the lower-left corner of the Log Retrieval page.
- Export all fields of the returned logs: Click **Export All Fields** on the **Log Retrieval** page to export all fields of the returned logs. All fields of the returned logs are displayed in the lower-left column of the **Log Retrieval** page. The fields are divided into **Show fields** and **Optional fields**.
- Export the selected fields of the returned logs: Click **Export Selected Fields** on the **Log Retrieval** page to export the selected fields of the returned logs.
- View log details: Click **Details** in the Actions column to view the details of a log.
- View field details: Click **Help Information** in the upper-right corner of the Log Retrieval page to view the field details.
- Decode fields: Click **Decoding Gadget** in the upper-right corner of the Log Retrieval page to convert fields encoded in the specific format into another format.

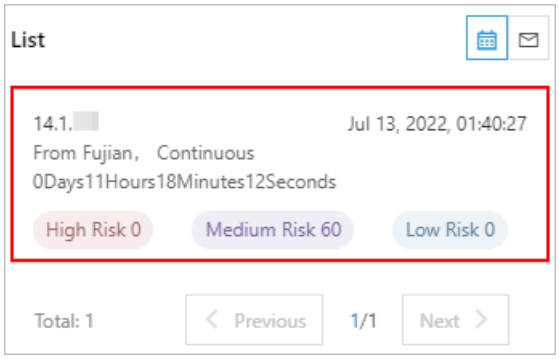
5.6. View an attacker profile

The attacker profile feature analyzes and displays the basic information, threat intelligence, attack methods, attack targets, and attack processes of the attacks that are initiated from an IP address in a centralized manner. This topic describes how to view an attacker profile.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Attacker portrait**.
4. On the **Attacker portrait** page, specify search conditions.

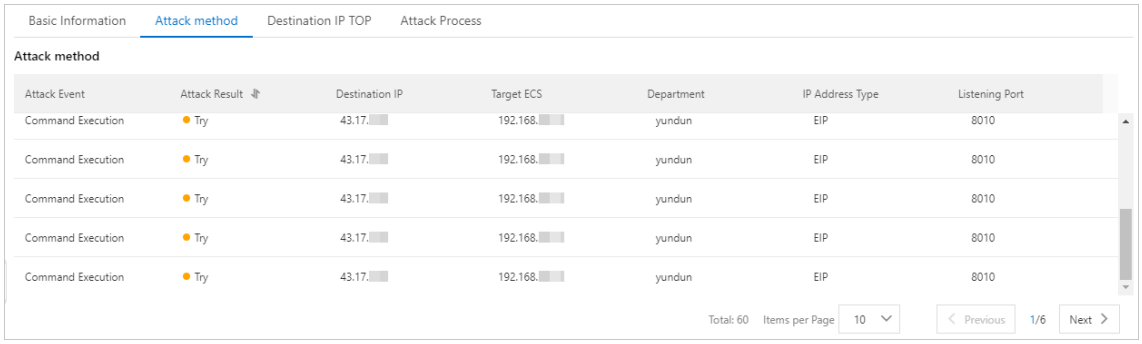
Search condition	Description
Time	Specify the time range of the attacks. Valid values: **Last Hour**, **Last 4 Hours**, **Today**, **Last 7 Days**, **Last 14 Days**, **Last 30 Days**, and **Custom**.
Attack Result	Select the type of the attack results. Valid values: **Try** and **Success**.
Threat Level	Select the severity of the attacks. Valid values: **Low Risk**, **Medium Risk**, and **High Risk**.
Attack IP Address.	Enter the IP address from which the attacks are initiated.

5. In the **List** section, view the search results.

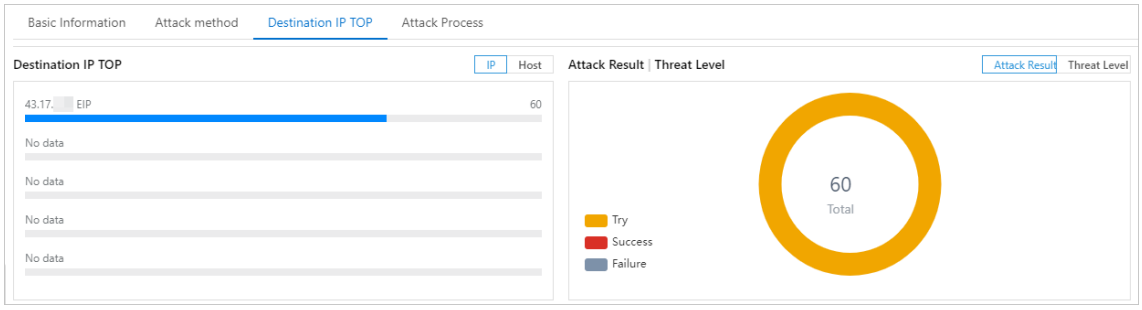


6. Click the tabs in the **List** section to view the information about the attacks that are initiated from the IP address.
   - Click the **Basic Information** tab to view the basic information about the attacks.

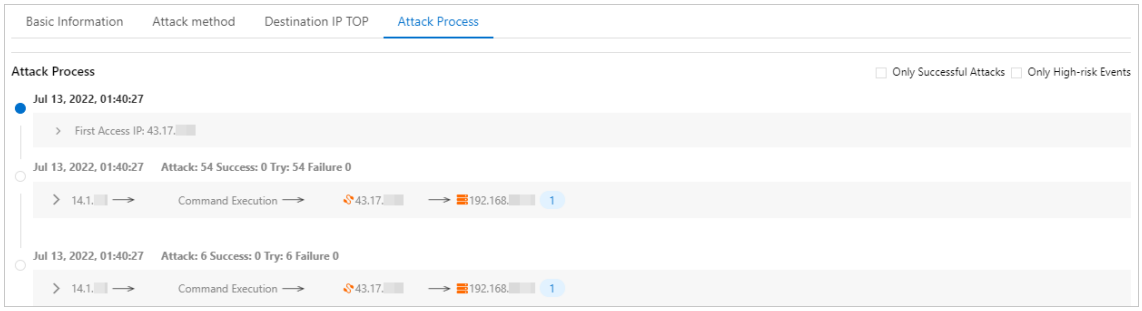
   - Click the **Attack method** tab to view the attack details.



   - Click the **Destination IP TOP** tab to view the top five hosts and IP addresses that receive the most attacks. You can also view the number of attack attempts, the number of successful attacks, and the number of attacks by severity.



   - Click the **Attack Process** tab to view the detailed process of the attacks.



5.7. Use the Threat Detection module

5.7.1. View the information on the Threat Detection page

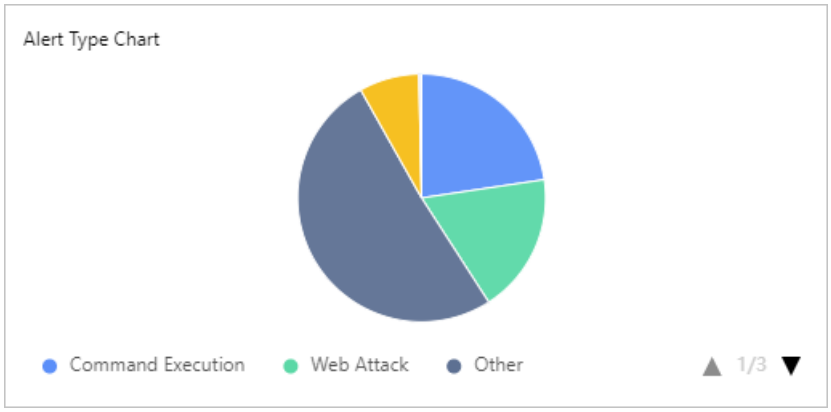
This topic describes how to view the information on the Threat Detection page.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Threat detection**.
4. On the **Threat Detection** page, click **Threat Detection**.
5. On the **Threat Detection** tab, specify search conditions.
6. Click **Query** to view the search results.

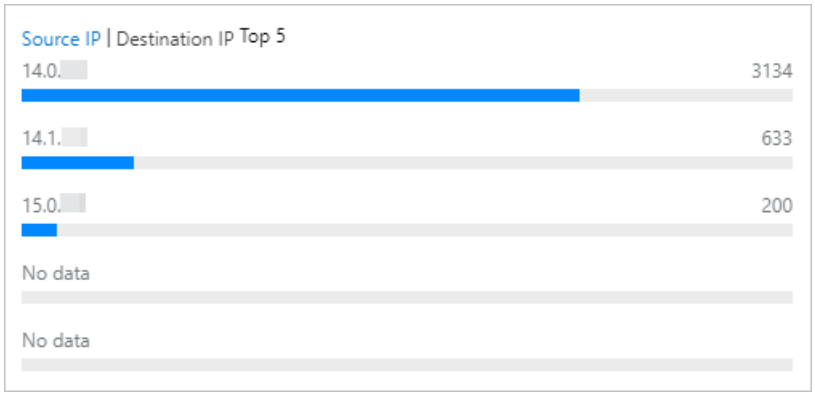
   If you no longer use the specified search conditions, click **Reset** to clear the search conditions.

   The system analyzes the attacks that meet the search conditions and displays the analysis results in charts.

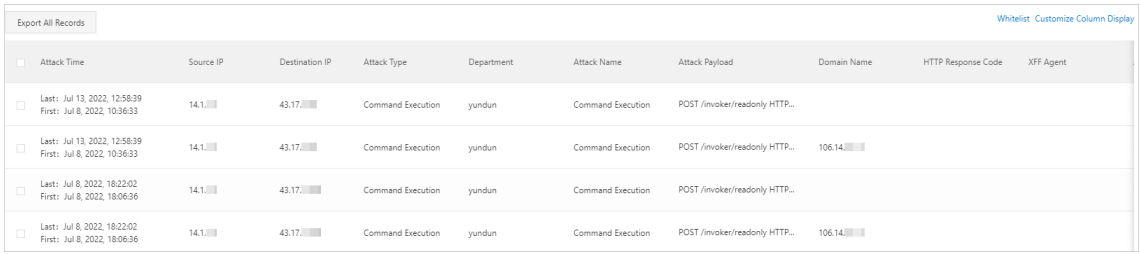
   - The pie chart in the Alert Type Chart section displays the numbers of attacks by alert type.

   - The bar chart in the Source IP | Destination IP Top 5 section displays the top five IP addresses that initiate the most attacks and the numbers of the attacks, and the top five IP addresses that receive the most attacks and the numbers of the attacks.

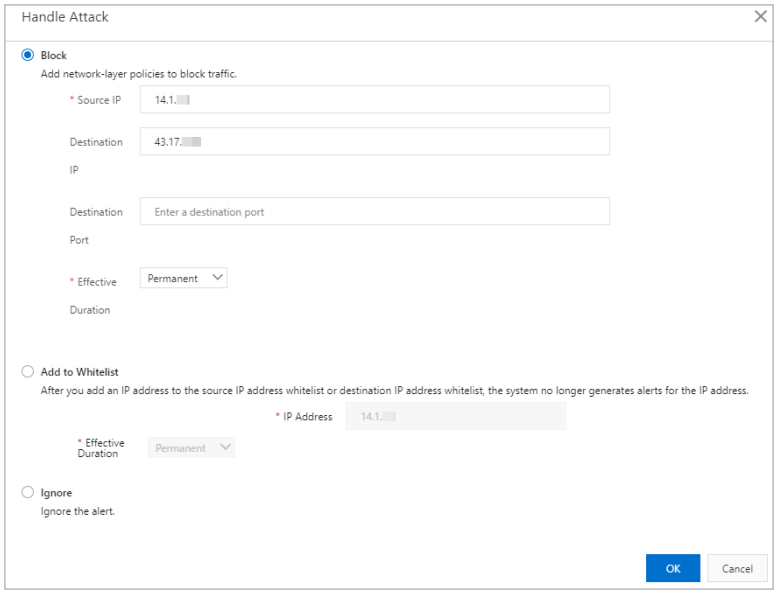


- The chart in the Alert Trend Chart section displays the trend of the number of the attacks in the specified time range.
- The attack list in the lower part of the Threat Detection page displays the detailed information about the attacks.



  - Select the columns that you want to display: Click Customize Column Display to select the columns that you want to display in the attack list. By default, the attack list displays the following columns: **Attack Time**, **Attack Name**, **Department**, **Source IP**, **Destination IP**, **Attack Payload**, **Risk Level**, **Attack Result**, and **Protection Status**.
  - View attack details: Click **Details** of an attack to view the **Basic Information**, **Rule Details**, and **Original Alert List** of the attack.
  - Add a tag to an attack: Click **Label** of an attack to add a custom tag to the attack.

- Select a handling method for an attack: Click **Handle** of an attack to select a handling method for the attack. Valid values: **Block**, **Add to Whitelist**, and **Ignore**.



  - **Block**: blocks attacking IP addresses by using network-layer access control policies.

Parameter	Description
Source IP	The IP address from which the attack is launched.
Destination IP	The IP address of the attacked asset.
Destination Port	The destination port of the attack.
Effective Duration	The validity period of the handing method. Valid values: **One Day**, **One Week**, **One Month**, **Custom**, and **Permanent**.

  - **Add to Whitelist**: adds an IP address to the whitelist. After the IP address is added to the whitelist, no alerts are generated for the attacks from the IP address or on the IP address. You can click **Whitelist** to view the added IP address. You can also remove or add an IP address in the **Whitelist Management** dialog box.
  - **Ignore**: ignores a single alert. If the same attack is launched again, a new alert is generated.

  Each state that is displayed in the Protection Status column in the attack list corresponds to the selected handling method. By default, Unhandled is displayed. After a handling method is selected, a state that corresponds to the selected handling method is displayed. If you select **Block**, **Blocked** is displayed in the Protection Status column. If you select **Add to Whitelist**, **Trusted** is displayed. If you select **Ignore**, **Ignored** is displayed.

- Export the attack list: Click **Export All Records** to export the returned data of the attacks.

5.7.2. View logs of blocked traffic

Logs of blocked traffic record the traffic that hits a blocking policy. This topic describes how to view the logs of the blocked traffic.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Threat detection**.
4. On the **Threat Detection** page, click **Blocking Log**.
5. On the **Blocking Log** tab, specify search conditions.
6. Click **Query**.
   - The bar chart in the Source IP | Destination IP Top 5 section displays the top five IP addresses that initiate the most attacks and the numbers of the attacks, and the top five IP addresses that receive the most attacks and the numbers of the attacks.
   - The line chart in the RST Packet Statistics (Global) section displays the number of reset (RST) packets at different points in time.
   - The chart in the **Protection Statistics (Count)** section displays the number of times that attacks are defended against within the specified time range.
   - The log list in the lower part of the **Blocking Log** tab displays the details of the logs for the blocked traffic.

     You can also click **Export All Records** above the log list to export the logs. In the **Actions** column of the log list, you can click **Block**, **Add to Whitelist**, and **Monitor** to configure **Protection Action** for a log. If you select multiple logs, you can configure a protection action for multiple attacks at a time.
     - **Block**: When the system detects the traffic that hits a blocking policy, the system generates an alert and blocks the traffic.
     - **Monitor**: When the system detects the traffic that hits a blocking policy, the system generates an alert but does not block the traffic.
     - **Add to Whitelist**: No alerts are generated for the traffic from the IP address that is added to the whitelist.

5.8. Use the Behavior Analysis module

5.8.1. View the information on the Encrypted Traffic Analysis tab

Encrypted traffic analysis can detect suspicious encrypted traffic by analyzing the characteristics of traffic. This topic describes how to view the information on the Encrypted Traffic Analysis tab.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Behavior Analysis**.
4. On the **Behavior Analysis** page, click **Encrypted Traffic Analysis**.
5. On the **Encrypted Traffic Analysis** tab, specify search conditions.

You can specify the **Created At**, **Department**, **Source IP**, **Destination IP**, and **Attack Tool Type** parameters.

6. Click **Query** to view the search results.

   You can view the analysis results of the encrypted traffic that meet the search conditions in charts of the following sections:

   - **Analysis of Encrypted Traffic Types**
   - **Type Analysis of Attack Tools**
   - **Source IP | Destination IP Top 5**

5.8.2. View the information on the DNS Behavior Analysis tab

DNS behavior analysis can detect suspicious DNS behavior by analyzing the characteristics of suspicious domain names. This topic describes how to view the information on the DNS Behavior Analysis tab.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Behavior Analysis**.
4. On the **Behavior Analysis** page, click **DNS Behavior Analysis**.
5. On the **DNS Behavior Analysis** tab, specify search conditions.

   You can specify the Created At, Department, Domain Name, Source IP, and Exception Type parameters based on your business requirements.

6. Click **Query**.

   The system analyzes the DNS behavior that meet the search conditions and displays the analysis results in charts.

   - The chart in the **Statistics on DGA Domain Names** section displays domain names that are generated by using domain generation algorithms (DGA). The chart in the **Statistics on DNS Tunneling-involved Domain Names** section displays domain names that are used to launch DNS tunneling attacks.
   - The chart in the **Trends of Suspicious DNS Resolutions** section displays the trend of suspicious DNS resolutions. You can view the number of DNS resolutions at different points in time within the specified time range.
   - The DNS behavior list in the lower part of the **DNS Behavior Analysis** tab displays the information about the records of suspicious DNS behavior.

     You can also perform the following operations in the DNS behavior list:

     - View the details of a record of suspicious DNS behavior: Click **Details** in the **Actions** column of a record to view the details.
     - Add a record of suspicious DNS behavior to the whitelist: Click **Add to Whitelist** in the **Actions** column of a record to add the record to the whitelist. In the **Whitelist** dialog box, you can view the records of suspicious DNS behavior that are added to the whitelist.
     - Configure a rule to detect DNS tunneling attacks: Click **DNS Tunneling Detection Rule** to configure a rule to detect DNS tunneling attacks.

5.9. Use the Policy Configuration module

5.9.1. Configure a network-layer rule

This topic describes how to create a network-layer rule and query network-layer rules in the rule list.

Create a network-layer rule

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Policy Configuration**.
4. On the **Network Layer Policy** tab, click **Create Policy**.
5. In the panel that appears, configure the parameters.

Parameter	Description
Policy Name	Specify a rule name.
Policy Description	Enter a description for the rule.
Direction	Select the direction of traffic on which the rule takes effect.
Policy Type	Select the type of the rule. Valid values: **Source IP Only**, **Destination IP Only**, and **Source IP, Destination IP/Port**.
Rules	Select one or more methods to configure the rule. Valid values: **Manual Input**, **Import File**, and **Address Book**.
Whether to Enable	Specify whether to enable the rule.
Protection Action	Select an action for the rule. Valid values: **Allow**, **Monitor**, and **Block**.
Effective Duration	Select a validity period for the rule. Valid values: **Permanent**, **One Day**, **One Week**, **One Month**, and **Custom**.

6. Click **OK**.
   The created rule is displayed in the rule list of the **Network Layer Policy** tab.

Query network-layer rules

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network**

Traffic Monitoring System in the **Network Security** section.

3. In the left-side navigation pane, click **Policy Configuration**.
4. On the **Network Layer Policy** tab, view the rule list.

   You can perform the following operations:

   - Search for a rule: Select an action or traffic direction, enter the name, description, ID, or UUID of a rule, or specify a time condition above the rule list to search for a rule.
   - Select whether to enable a rule: Turn on or off the switch in the **Whether to Enable** column of a rule to enable or disable the rule.
   - Modify a rule: Click **Edit** in the **Actions** column of a rule to modify the rule.
   - Delete a rule: Click **Delete** in the **Actions** column of a rule to delete the rule.
   - Enable all network-layer rules: Turn on **Global Network Policies** above the rule list.
   - Enable threat intelligence filtering: Turn on **Threat Intelligence Filtering** above the rule list. After you turn on Threat Intelligence Filtering, the system filters traffic that is initiated from malicious IP addresses. By default, the system blocks the traffic that matches threat intelligence.

5.9.2. Configure an application-layer rule

This topic describes how to create an application-layer rule, query application-layer rules, and query rules of web application detection.

Create an application-layer rule

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Policy Configuration**.
4. Click **Application Layer Policies**.
5. On the **HTTP Custom Policy** tab of the **Application Layer Policies** tab, click **Create Policy**.
6. In the panel that appears, configure the parameters.

Parameter	Description
Policy Name	Specify a rule name.
Direction	Select the direction of traffic on which the rule takes effect. Valid values: **Inbound** and **Outbound**.
Match condition	Specify one or more match conditions for the rule. A match condition is the core element of a rule. A rule matches traffic against the conditions and then **allows**, **monitors**, or **blocks** the traffic that meets the conditions. You must specify **Matching Field**, **Logical Operator**, **Matching Content**, and **Case Sensitive or Not** to add a match condition.

Parameter	Description
Protection Action	Select an action for the rule. Valid values: **Allow**, **Monitor**, and **Block**.
Whether to Enable	Specify whether to enable the rule.
Effective Duration	Select a validity period for the rule. Valid values: **Permanent**, **One Day**, **One Week**, **One Month**, and **Custom**.

7. Click **OK**.
   The created rule is displayed in the rule list of the **HTTP Custom Policy** tab.

Query application-layer rules

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Policy Configuration**.
4. Click **Application Layer Policy**.
5. Click the **HTTP Custom Policy** tab.
6. On the **HTTP Custom Policy** tab, specify search conditions.

   You can specify an action, state, traffic direction, and time condition to search for rules.
7. Click **Query**.
8. On the **HTTP Custom Policy** tab, view the rules in the rule list.

   You can perform the following operations:
   - Modify a rule: Click **Edit** in the **Actions** column of a rule to modify the rule.
   - Delete a rule: Click **Delete** in the **Actions** column of a rule to delete the rule.

Query rules of web application detection

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Policy Configuration**.
4. Click **Application Layer Policies**.
5. Click the **Web application detection configuration** tab.
6. On the **WEB application detection configuration** tab, specify **Startup status** and **Protection type** to search for rules.
7. Click **Search** and view the returned rules in the rule list.
   - Enable or disable a single rule of web application detection: Turn on the switch in the **Status** column of a rule, and the state of the rule becomes **In Effect**. Turn off the switch in the **Status** column of a rule, and the state of the rule becomes **Invalidated**.
   - Enable or disable all rules of web application detection: Turn on **WEB application detection**

switch above the list to enable all rules. Turn off WEB application detection switch to disable all rules.

5.9.3. Configure a spoofing rule for port scanning

A spoofing rule for port scanning lures attackers to launch attacks against ports that do not exist. This way, attacks are exposed. This topic describes how to configure a spoofing rule for port scanning.

Context

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Policy Configuration**.
4. Click **Port Scan Spoofing Policy**.
5. On the **Port Scan Spoofing Policy** tab, click **Create Policy**.
6. In the panel that appears, configure the parameters.

Parameter	Description
Organization	Select the organization of Apsara Stack Security.
Address Type	Select the type of the address that you want to protect. The address consists of an IP address and ports that are configured in a service. You can obtain the address by using the port of the security component. Valid values: **WAF**, **Public SLB**, **EIP**, and **Custom**.
Protection Address	Select the address that you want to protect.
Port Whitelist	Enter ports in the whitelist. Spoofing rules for port scanning are applied only to the ports that are not added to the whitelist.
Protection Mode	Select a protection mode. Valid values: **Monitor** and **Protect**. If you select **Monitor**, the system only generates alerts, but does not block attacks. If you select **Protect**, the system generates alerts and blocks attacks.

7. Click **OK**.

   You can perform the following operations:

   - Search for a rule: Select an action, state, traffic direction, or time condition above the rule list to search for rules.
   - Modify a rule: Click **Edit** in the **Actions** column of a rule to modify the rule.
   - Delete a rule: Click **Delete** in the **Actions** column of a rule to delete the rule.
   - Delete multiple rules at a time: Select the rules that you want to delete and click **Batch Delete**.
   - Enable or disable a rule: Turn on the switch in the **Status** column of a rule to enable the rule.

Turn off the switch in the **Status** column of a rule to disable the rule.

5.9.4. Manage address books

This topic describes how to create an address book and query address books in the address book list.

Create an address book

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Policy Configuration**.
4. Click **Address Book Management**.
5. On the **Address Book Management** tab, click **Create IP Address Book**.
6. In the **Create Address Book** panel, configure the parameters.

Parameter	Description
Address Book Name	Specify an address book name.
Address Book Type	Select the method to add addresses to the address book. Valid values: **File Import** and **Manual Input**.
IP Address	If **Address Book Type** is set to **File Import**, click Select File to import a local file. If **Address Book Type** is set to **Manual Input**, enter 32-bit IP addresses. You must specify only IPv4 addresses or only IPv6 addresses in an address book. An address book cannot contain both IPv4 addresses and IPv6 addresses.
Address Book Description	Enter a description for the address book.

7. Click **OK**.
   The created address book is displayed in the address book list of the **Address Book Management** tab.

Query address books

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Then, click **Network Traffic Monitoring System** in the **Network Security** section.
3. In the left-side navigation pane, click **Policy Configuration**.
4. Click **Address Book Management**.
5. On the **Address Book Management** tab, query address books in the address book list.

   You can perform the following operations:

   - Search for an address book: Specify an address book name, address book description, or IP address above the address book list to search for an address book.

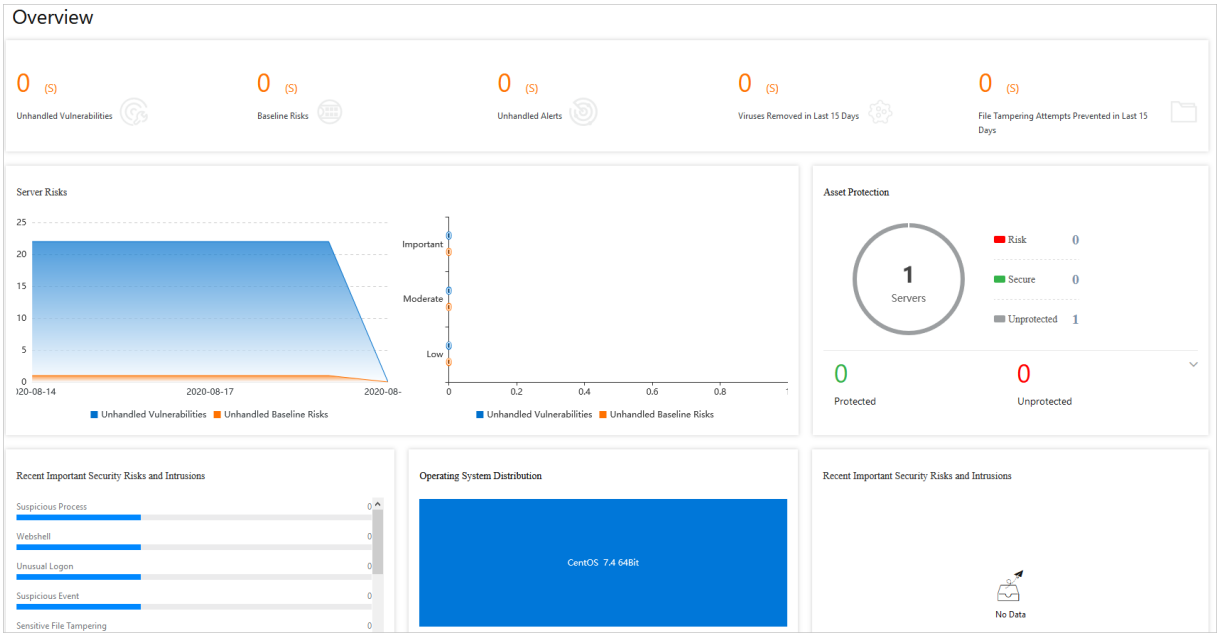
- Modify an address book: Click **Edit** in the **Actions** column of an address book to modify the address book.
- Delete an address book: Click **Delete** in the **Actions** column of an address book to delete the address book.
- Delete multiple address books at a time: Select the address books that you want to delete and click **Batch Delete**.

6.Server security

6.1. Server security overview

This topic describes how to view the details about the security of servers on the server security overview page of Apsara Stack Security Center. This helps security administrators understand the security status of the servers. The servers refer to servers on the cloud.

To view the details about the security of servers, log on to Apsara Stack Security Center and choose **Server Security > Overview**. On the page that appears, you can view detailed information on the following sections: overall statistics, Server Risks, Asset Protection, Operating System Distribution, and Recent Important Security Risks and Intrusions.



- **Overall statistics**: This section displays the numbers of security vulnerabilities and security events on servers. For security vulnerabilities, you can view **Unhandled Vulnerabilities** and **Baseline Risks**. For security events, you can view **Unhandled Alerts**, **Viruses Removed in Last 15 Days**, and **File Tampering Attempts Prevented in Last 15 Days**.
- **Server Risks**: This section displays the number of unhandled vulnerabilities, the number of baseline risks, and the distribution of risk levels.
- **Asset Protection**: This section displays the number of protected servers and the number of offline servers.
- **Recent Important Security Risks and Intrusions**: This section displays the recent important risks and events on your servers. You can click a risk or an event to view the details.
- **Operating System Distribution**: This section displays your servers by operating system.

6.2. Server fingerprints

6.2.1. Manage listening ports

This topic describes how to view information about the listening port of a server. The information helps you identify suspicious listening behavior.

Context

This topic is suitable for the following scenarios:

- Check for servers that listen on a specific port.
- Check for ports that a specific server listens.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Port** tab to view **listening ports**, **network protocols**, and server information.

   You can search for a port by using the port number, server process name, server name, or server IP address.

   In the server information list, you can view the **process**, **IP address**, and **latest scan time** of a server.

6.2.2. Manage software versions

This topic describes how to regularly view and collect the software version information about a server. This helps you check your software assets.

Context

This topic covers the following scenarios:

- Check for software assets that are installed without authorization.
- Check for outdated software assets.
- Locate affected assets if vulnerabilities are detected.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Server Security > Sever Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the page that appears, click the **Software** tab. On the tab, view all the **software assets** that are in use and the **number of the servers** that use the software assets.

   You can search for specific software by using its name, version, installation directory, server name, or IP address.
5. Click software to view the details, such as the software versions and the servers that use the software.

   You can click the icon in the upper-right corner to download a software version table to your computer for subsequent asset check.

6.2.3. Manage processes

This topic describes how to regularly collect the process information on a server and record changes. This way, you can view process information and historical process changes.

Context

This task is suitable for the following scenarios:

- Check for servers on which a specific process runs.
- Check for processes that run on a specific server.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the page that appears, click the **Process** tab. On the tab, view all running processes and the number of servers that run these processes.

   You can search for a process by using the **process name**, **running user**, **startup parameter**, or **server name or IP address**.
5. Click the name of a process to view the details of the process, such as the servers, paths, and startup parameters.

6.2.4. Manage account information

This topic describes how to regularly collect the account information on a server and record the changes to the accounts. This way, you can check your accounts and view historical changes to your accounts.

Context

You can use the information collected in this topic for the following scenarios:

- Check for servers on which a specific account is created.
- Check for accounts that are created on a server.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Account** tab.
5. View all the logged-on accounts and the numbers of servers on which the accounts are created.

   You can search for an account by using the account name, root permissions, server name, or server IP address.
6. Click an account name to view the details, such as the server information, root permissions, and user

group.

6.2.5. Manage scheduled tasks

This topic describes how to view scheduled tasks on servers.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Scheduled Tasks** tab.
5. View the paths of all tasks and the number of servers that run these tasks.

   You can search for a task by using the task path, server name, or IP address.
6. Click a task path to view the details, such as the servers, executed commands, and task cycles.

6.2.6. Set the fingerprint collection frequency

You can set the frequency at which the data of running processes, system accounts, listening ports, and software versions is collected.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. In the upper-right corner of the **Asset Fingerprints** page, click **Settings**.
5. Select the collection frequency from each drop-down list.
6. Click **OK** to complete the configuration.

6.3. Threat protection

6.3.1. Vulnerability management

6.3.1.1. Handle Linux software vulnerabilities

This topic describes how to handle Linux software vulnerabilities.

Context

Apsara Stack Security automatically scans the software that is installed on your servers to detect the vulnerabilities provided in the Common Vulnerabilities and Exposures (CVE) list. Apsara Stack Security also sends you alerts about the detected vulnerabilities. In addition, Apsara Stack Security provides commands that you can use to fix vulnerabilities and allows you to verify vulnerability fixes.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Vulnerabilities**.
4. On the **Linux Software** tab of the page that appears, view the detected Linux software vulnerabilities.

   > **Note** You can search for a specific vulnerability by using the search and filter features.

5. Find a vulnerability and click its name. In the panel that appears, you can view the details about the vulnerability and the servers that are affected by the vulnerability.

   > **Note** You can find affected servers by using the search and filter features.

   - **Detail**: This tab displays the basic information about the vulnerability, including the name, Common Vulnerability Scoring System (CVSS) score, description, and solution.
   - **Pending vulnerability**: This tab displays the servers that are affected by the vulnerability.
6. Handle the vulnerability based on its impact.

Actions on vulnerabilities

Action	Description
Generate Fix Command	Select this action to generate the commands that are used to fix the vulnerability. You can then log on to the server to run these commands.
Fix	Select this action to fix the vulnerability.
Restarted and Verified	If a vulnerability fix takes effect only after a server restart, you must restart the server after the status of the vulnerability changes to **Fixed (To Be Restarted)**. After the restart, click **Restarted and Verified**.
Ignore	Select this action to ignore the vulnerability. The system no longer generates alerts for or reports ignored vulnerabilities.
Verify	Click **Verify** to verify the vulnerability fix. If you do not manually verify a fix, the system automatically verifies the fix within 48 hours after the vulnerability is fixed.

You can handle a vulnerability for one or more affected servers at a time.

- To handle a vulnerability for one affected server, find the server and select an action in the **Actions** column of the server.
- To handle a vulnerability for multiple affected servers, select the servers and select an action in the lower-left corner.

6.3.1.2. Handle Windows system vulnerabilities

This topic describes how to handle Windows system vulnerabilities.

Context

Apsara Stack Security automatically checks whether the latest Microsoft updates are installed on your servers, and notifies you of the detected vulnerabilities. Apsara Stack Security also automatically detects and fixes major vulnerabilities on your servers.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Vulnerabilities**. On the page that appears, click the **Windows System** tab.
4. View the detected Windows system vulnerabilities.

   > **Note** You can search for a specific vulnerability by using the search and filter features.

5. Find a vulnerability and click its name. In the panel that appears, you can view details about the vulnerability and the servers that are affected by the vulnerability.

   > **Note** You can find affected servers by using the search and filter features.

   - **Detail**: This tab displays the basic information about the vulnerability, including the name, Common Vulnerability Scoring System (CVSS) score, description, and solution.
   - **Pending vulnerability**: This tab displays the servers that are affected by the vulnerability.
6. Handle the vulnerability based on its impact. describes the actions.

Actions on vulnerabilities

Action	Description
Fix	Select this action to fix the vulnerability. The system caches an official Windows patch in the cloud. Your server can automatically download the patch for updates.
Ignore	Select this action to ignore the vulnerability. The system no longer generates alerts for or reports ignored vulnerabilities.
Verify	Click **Verify** to verify the vulnerability fix.
Restarted and Verified	If a vulnerability fix takes effect only after a server restart, you must restart the server after the status of the vulnerability changes to **Fixed (To Be Restarted)**. After the restart, click **Restarted and Verified**.

You can handle a vulnerability for one or more affected servers at a time.

- To handle a vulnerability for one affected server, find the server and select an action in the **Actions** column of the server.
- To handle a vulnerability for multiple affected servers, select the servers and select an action in the lower-left corner.

6.3.1.3. Handle Web-CMS vulnerabilities

This topic describes how to handle Web-CMS vulnerabilities.

Context

The feature of Web-CMS vulnerability detection obtains information about the latest vulnerabilities and provides patches in the cloud. This helps you detect and fix vulnerabilities.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Vulnerabilities**. On the page that appears, click the **Web CMS** tab.
4. View all detected vulnerabilities.

   > **Note** You can search for a specific vulnerability by using the search and filter features.

5. Find a vulnerability and click its name. In the panel that appears, you can view details about the vulnerability and the servers that are affected by the vulnerability.

   > **Note** You can find affected servers by using the search and filter features.

6. Handle the vulnerability based on its impact. describes the actions.

Actions on vulnerabilities

Action	Description
Fix	If you select this action, the system replaces the web files that are affected by the vulnerability on your server to fix the Web-CMS vulnerability. **Note** Before you fix the vulnerability, we recommend that you back up the web files affected by the vulnerability. For more information about the paths of the web files, click Details in the Actions column.
Ignore	Select this action to ignore the vulnerability. The system no longer generates alerts for or reports ignored vulnerabilities.
Verify	After a vulnerability is fixed, you can click **Verify** to verify the vulnerability fix. If you do not manually verify the fix of a vulnerability, the system automatically verifies the fix within 48 hours after the vulnerability is fixed.
Undo Fix	For vulnerabilities that have been fixed, click **Undo Fix** to restore the web files that have been replaced.

You can handle a vulnerability for one or more affected servers at one time.

- To handle a vulnerability for one affected server, select an action in the **Actions** column of the server.
- To handle a vulnerability for multiple affected servers, select the servers and select an action in the lower-left corner.

6.3.1.4. Handle urgent vulnerabilities

This topic describes how to handle urgent vulnerabilities.

Context

Apsara Stack Security automatically detects vulnerabilities on servers, such as the unauthorized Redis access vulnerability and Struts S2-052 vulnerability, and generates alerts for detected vulnerabilities. After you fix a vulnerability, you can also check whether the fix is successful.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Vulnerabilities**.
4. On the **Vulnerabilities** page, click the **Emergency** tab.
5. View all vulnerabilities.

   You can search for a specific vulnerability by using the search and filter features.
6. Click the name of a vulnerability. In the panel that appears, view the details in the following sections: **Details**, **Suggestions**, and **Affected Assets**.

   You can find affected assets by using the search and filter features.
7. Handle the vulnerability based on its impact. describes the actions.

   Follow the instructions to fix the vulnerabilities on the **Emergency** tab.

Actions on vulnerabilities

Action	Description
Ignore	Select this action to ignore the vulnerability. The system no longer generates alerts for or reports ignored vulnerabilities.
Verify	Click **Verify** to verify the vulnerability fix. If you do not manually verify a fix, the system automatically verifies the fix within 48 hours after the vulnerability is fixed.

You can handle a vulnerability for one or more affected assets at a time.

- To handle a vulnerability for one affected asset, find the asset and select an action in the **Actions** column of the asset.
- To handle a vulnerability for multiple affected assets, select the assets and select an action in the lower-left corner.

6.3.1.5. Configure vulnerability handling policies

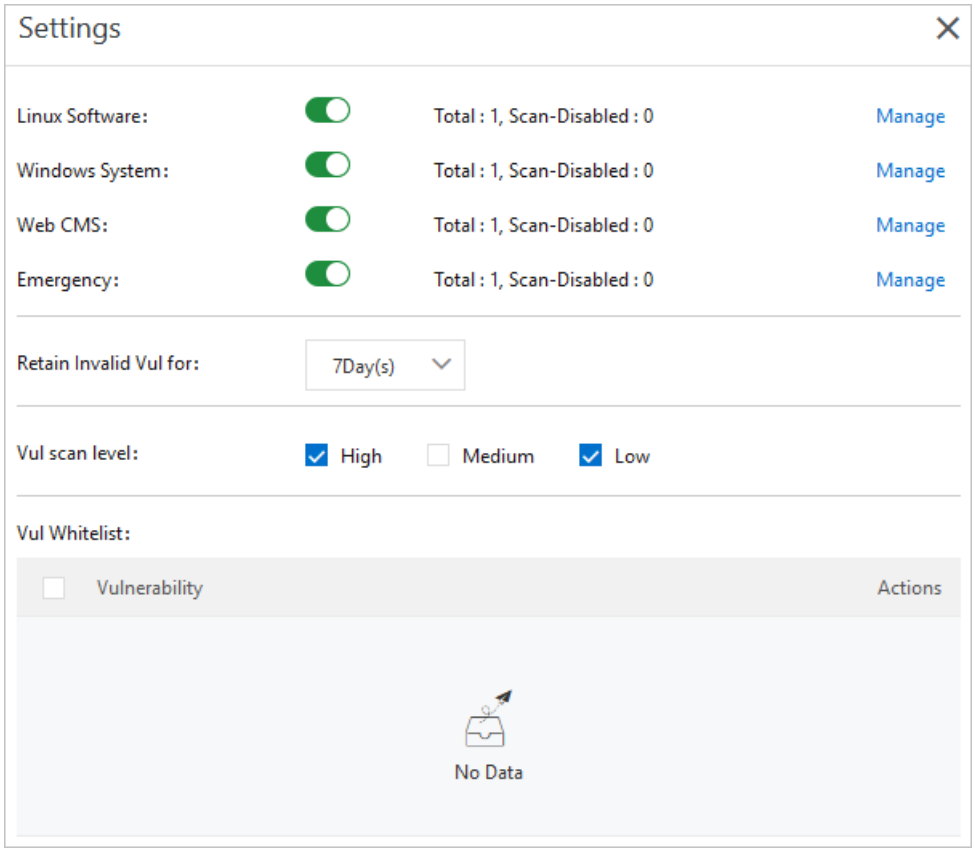
You can enable or disable automatic detection for different types of vulnerabilities and enable vulnerability detection for specific servers. You can also set a duration during which invalid vulnerabilities are retained and configure a vulnerability whitelist.

Context

A vulnerability whitelist allows you to ignore specific vulnerabilities. You can add multiple vulnerabilities in the vulnerability list to the whitelist. The system does not detect vulnerabilities that are added to the whitelist. You can configure the vulnerability whitelist on the vulnerability settings page.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Vulnerabilities**.
4. In the upper-right corner of the page that appears, click **Settings** to configure vulnerability handling policies. In the panel that appears, perform the following operations:



   - Find a vulnerability type and enable or disable detection for vulnerabilities of this type.
   - Click **Manage** next to a vulnerability type and specify the servers on which vulnerabilities of this type are detected.
   - Select a time duration during which invalid vulnerabilities are retained for Retain Invalid Vul for. Valid values: 7Day(s), 30Day(s), and 90Day(s).

> **Note** If you do not take an action on a detected vulnerability, the system determines that the alert, which indicates that a vulnerability is detected, is invalid. The system deletes the vulnerability after the specified duration.

- Select the vulnerability severities for scanning for Vul scan level. Valid values:
  - **High**: You must fix the vulnerabilities of this severity at the earliest opportunity.
  - **Medium**: You can fix the vulnerabilities of this severity later.
  - **Low**: You can ignore the vulnerabilities of this severity for now.
- Select vulnerabilities in the Vul Whitelist section and click **Remove** in the Actions column to enable the system to detect these vulnerabilities and generate alerts for these vulnerabilities.

6.3.2. Baseline check

6.3.2.1. Baseline check overview

The baseline check feature automatically checks the security configurations on servers and provides detailed check results and suggestions for baseline reinforcement.

Description

After you enable the baseline check feature, Apsara Stack Security automatically checks for risks related to the operating systems, accounts, databases, passwords, and security compliance configurations of your servers, and provides reinforcement suggestions. For more information, see Baselines.

By default, a full baseline check is automatically performed from 00:00 to 06:00 every day. You can create and manage scan policies for baseline checks. When you create or modify a policy, you can specify the baselines, interval, and time period, and select the servers to which you want to apply this policy. For more information, see Add a custom baseline check policy.

Precautions

By default, the following baselines are disabled. To check these baselines, make sure that these baselines do not affect your business and select them when you customize a scan policy.

- Baselines related to weak passwords for specific applications such as MySQL, PostgreSQL, and SQL Server

  > **Note** If these baselines are enabled, the system attempts to log on to servers with weak passwords. The logon attempts consume server resources and generate a large number of logon failure records.

- Baselines related to China classified protection of cybersecurity
- Baselines related to the Center for Internet Security (CIS) standard

Baselines

Category	Baseline

Category	Baseline
High risk exploit	• High risk exploit - CouchDB unauthorized access high exploit risk • High risk exploit - Docker unauthorized access high vulnerability risk • High risk exploit - Elasticsearch unauthorized access high exploit vulnerability risk • High risk exploit - Memcached unauthorized access high exploit vulnerability risk • High risk exploit - Apache Tomcat AJP File Read/Inclusion Vulnerability • High risk exploit - ZooKeeper unauthorized access high exploit vulnerability risk
	Security baseline check against the Alibaba Cloud standard: • Alibaba Cloud Standard-Aliyun Linux 2 Security Baseline Check • Alibaba Cloud Standard - CentOS Linux 6 Security Baseline Check • Alibaba Cloud Standard - CentOS Linux 7 Security Baseline Check • Alibaba Cloud Standard - Debian Linux 8 Security Baseline • Alibaba Cloud Standard - Redhat Linux 6 Security Baseline Check • Alibaba Cloud Standard - Redhat Linux 7 Security Baseline Check • Alibaba Cloud Standard - Ubuntu Security Baseline Check • Alibaba Cloud Standard - Windows Server 2008 R2 Security Baseline Check • Alibaba Cloud Standard - Windows 2012 R2 Security Baseline • Alibaba Cloud Standard - Windows 2016/2019 R2 Security Baseline
	Security baseline check against the CIS standard: • Alibaba Cloud Aliyun Linux 2 CIS Benchmark • CIS CentOS Linux 6 LTS Benchmark • CIS CentOS Linux 7 LTS Benchmark • CIS Debian Linux 8 Benchmark • CIS Ubuntu Linux 14 LTS Benchmark • CIS Ubuntu Linux 16/18 LTS Benchmark • CIS Microsoft Windows Server 2008 R2 Benchmark • CIS Microsoft Windows Server 2012 R2 Benchmark • CIS Microsoft Windows Server 2016/2019 R2 Benchmark

Category	Baseline
CIS and China's Protection of Cybersecurity	Baseline check on compliance of China classified protection of cybersecurity level III: • Aliyun Linux 2 Baseline for China classified protection of cybersecurity-Level III • CentOS Linux 6 Baseline for China classified protection of cybersecurity-Level III • CentOS Linux 7 Baseline for China classified protection of cybersecurity-Level III • Debian Linux 8 Baseline for China classified protection of cybersecurity-Level III • Redhat Linux 6 Baseline for China classified protection of cybersecurity-Level III • Redhat Linux 7 Baseline for China classified protection of cybersecurity-Level III • SUSE Linux 10 Baseline for China classified protection of cybersecurity-Level III • SUSE Linux 11 Baseline for China classified protection of cybersecurity-Level III • SUSE Linux 12 Baseline for China classified protection of cybersecurity-Level III • Ubuntu 14 Baseline for China classified protection of cybersecurity-Level III • Waiting for Level 3-Ubuntu 16/18 compliance regulations inspection • China's Level 3 Protection of Cybersecurity - Windows Server 2008 R2 Compliance Baseline Check • Windows 2012 R2 Baseline for China classified protection of cybersecurity-Level III • Windows 2016/2019 R2 Baseline for China classified protection of cybersecurity-Level III

Category	Baseline
Best security practices	• Alibaba Cloud Standard-Aliyun Linux 2 Security Baseline Check • Alibaba Cloud Standard - Apache Security Baseline Check • Alibaba Cloud Standard - CentOS Linux 6 Security Baseline Check • Alibaba Cloud Standard - CentOS Linux 7/8 Security Baseline Check • Alibaba Cloud Standard - Debian Linux 8 Security Baseline • Alibaba Cloud Standard - IIS 8 Security Baseline Check • Alibaba Cloud Standard - Memcached Security Baseline Check • Alibaba Cloud Standard - MongoDB 3.x Security Baseline Check • Alibaba Cloud Standard - Mysql Security Baseline Check • Alibaba Cloud Standard - Nginx Security Baseline Check • Alibaba Cloud Standard - Redhat Linux 6 Security Baseline Check • Alibaba Cloud Standard - Redhat Linux 7 Security Baseline Check • Alibaba Cloud Standard - Redis Security Baseline Check • Alibaba Cloud Standard - Ubuntu Security Baseline Check • Alibaba Cloud Standard - Windows Server 2008 R2 Security Baseline Check • Alibaba Cloud Standard - Windows 2012 R2 Security Baseline • Alibaba Cloud Standard - Windows 2016/2019 R2 Security Baseline • Alibaba Cloud Standard-Apache Tomcat Security Baseline
Weak password	• Weak Password-MongoDB Weak Password baseline(support version 2. X) • Weak password - Ftp login weak password baseline • Weak password - Linux system login weak password baseline • Weak password - MongoDB login weak password baseline • Weak password - SQL Server DB login weak password baseline • Weak password - Mysql DB login weak password baseline • Weak password - Mysql DB login weak password baseline(Windows version) • Weak password - PostgreSQL DB login weak password baseline • Weak password - Redis DB login weak password baseline • Weak password - rsync login weak password baseline • Weak password - svn login weak password baseline

6.3.2.2. Configure baseline check policies

This topic describes how to create, modify, and delete baseline check policies. This topic also describes how to specify baseline check levels.

Context

By default, the baseline check feature uses the **default policy** to check the baseline risks of assets. You can also customize baseline check policies based on your business requirements. For example, you

can customize a baseline check policy to check the compliance with classified protection requirements (MLPS level 2).

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Baseline Check**.
4. In the upper-right corner of the page that appears, click **Manage Policies**. In the **Manage Policies** panel, create, modify, or delete a baseline check policy. You can also modify the default policy.
   - In the upper-right corner of the panel, click **+Create Policy** to customize a baseline check policy. Then, click **Ok**.

Parameter	Description
Policy Name	Enter a policy name.
Schedule	Set the time interval for scheduled scan tasks to Every 1 Day, Every 3 Day, Every 7 Day, or Every 30 Day. Then, select one of the following time ranges for scheduled scan tasks: 00:00 to 06:00, 06:00 to 12:00, 12:00 to 18:00, and 18:00 to 24:00.
Check Items	Select the baseline items that need to be checked from the following categories: High risk exploit, Container security, CIS and China's Protection of Cybersecurity, Best security practices, and Weak password.
Servers	Select the server groups to which you want to apply the baseline check policy. **Note** By default, newly purchased servers are added to the **Default** group under **Asset Groups**. To apply this policy to the newly purchased servers, select **Default**.

   - Click **Edit** or **Delete** next to the created policy to modify or delete it.

     Note You cannot restore a policy after you delete it.

   - Find the **Default** policy and click **Edit** in the **Actions** column to modify the server groups to which the default policy is applied.

     Note You cannot delete the default policy or modify the baseline items of the default policy. You can only modify the server groups to which the default policy is applied.

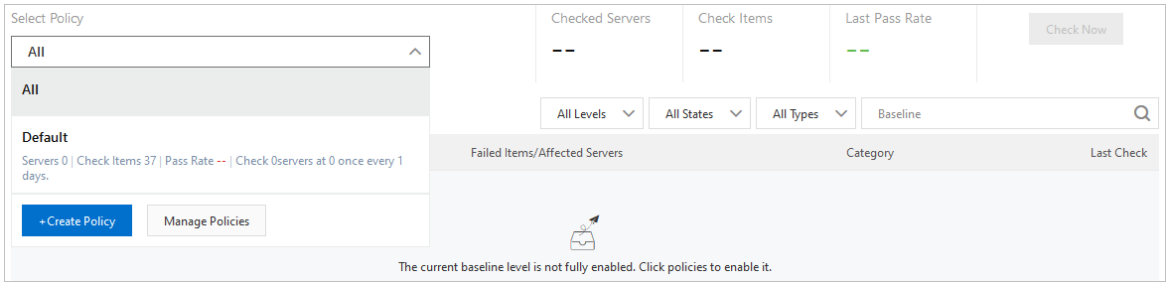
   - In the lower part of the **Manage Policies** panel, specify the baseline check levels. Valid values: High, Medium, and Low.
5. Click **Ok**.

6.3.2.3. View baseline check results and handle baseline risks

Apsara Stack Security Center provides detailed baseline check results and suggestions on how to handle baseline risks. This topic describes how to view baseline check results and handle baseline risks in Apsara Stack Security Center. The check results include information about affected assets, details of check items, and suggestions on how to handle baseline risks.

View the summary of baseline check results

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Baseline Check**.
4. In the upper part of the **Baseline Check** page, view the summary of baseline check results. You can filter data by policy.



You can select a policy from the **Select Policy** drop-down list to view the following information:

- **Checked Servers**: The number of servers on which the baseline check runs. These servers are specified in the selected baseline check policy.
- **Check Items**: The number of **check items** specified in the selected baseline check policy.
- **Last Pass Rate**: The pass rate of the check items in the last baseline check.

  If the number below **Last Pass Rate** is green, the pass rate is high. If the number is red, a large number of baseline risks have been detected on the checked servers. We recommend that you go to the details page to view and handle the baseline risks.

View all baselines

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Baseline Check**.
4. Select **All** from the **Select Policy** drop-down list.
   The **Baseline Check** page displays details about all baselines, including **Baseline**, **Checked Item**, **Failed Items/Affected Servers**, **Category**, and **Last Check**.

> **Note** You can also select a baseline check policy from the **Select Policy** drop-down list to view the baselines specified in this policy.

View details about a baseline

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Baseline Check**.
4. In the **Baseline** column, click a baseline to view its details.
5. In the details panel, handle the baseline risks.

   Find the asset that you want to handle and click **View** in the **Actions** column to open the **At-Risk Items** panel.

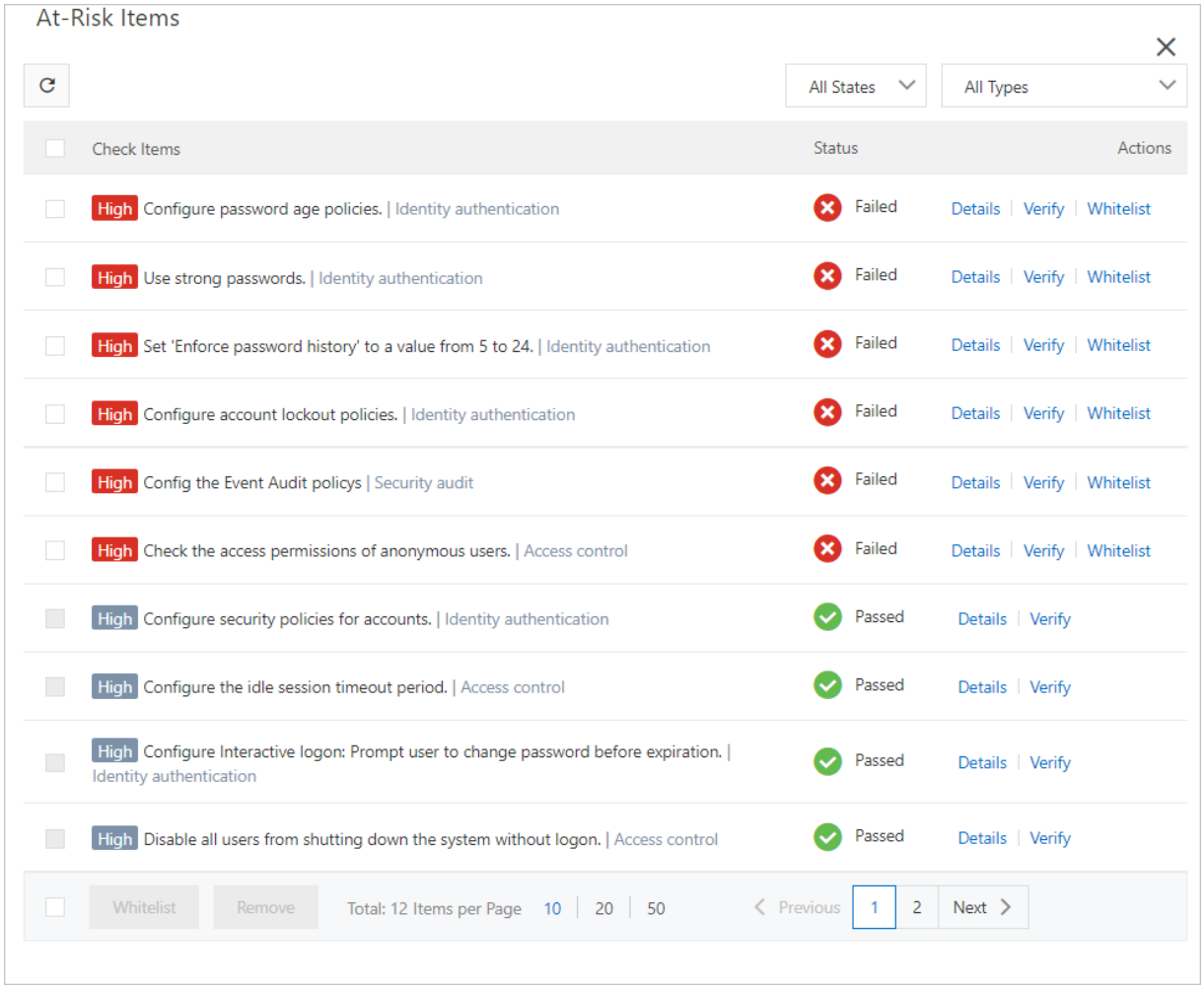
View details about a baseline risk

1. Find the baseline that you want to handle and click it. In the panel that appears, find the asset that you want to handle and click **View** in the **Actions** column to view the details about the risk items. You can view the check items of the asset and the statuses of the check items. The status can be **Passed** or **Failed**.
2. To view the details, click **Details** in the Actions column of the check items.

> **Note** We recommend that you follow the suggestions to handle risk items whose status is **Failed** at the earliest opportunity, especially high-risk items.

Handle baseline risks

In the At-Risk Items panel, handle baseline risks.



- **Add check items to the whitelist**

  If you want to disable alerts for a check item, click **Whitelist** to add the check item to the whitelist. Check items in the whitelist do not trigger alerts.

  > **Note** You can also select multiple check items and click **Whitelist** in the lower-left corner to add the check items to the whitelist at a time.

- **Fix risks**

  You can fix only the baseline risks that are detected based on the Alibaba Cloud standard at a time. You can select multiple servers on which the same baseline risk is detected and fix the risk.

  > **Notice** Risk fixing may cause service interruptions. We recommend that you back up your service data before risk fixing.

- **Remove check items from the whitelist**

  If you want to enable alerts for a check item in the whitelist, you can click **Remove** to remove the check item from the whitelist. You can remove one or more check items from the whitelist at a time. After a check item is removed from the whitelist, the check item triggers alerts again.

- **Verify the fix of a baseline risk**

If you do not manually perform the verification, Apsara Stack Security automatically verifies the fix based on the detection interval specified in the baseline check policy.

6.4. Intrusion prevention

6.4.1. Intrusion events

6.4.1.1. Intrusion event types

If Server Guard detects sensitive file tampering, suspicious processes, webshells, unusual logons, or malicious processes, it generates alerts. Based on these alerts, you can monitor the security status of your assets and handle potential threats at the earliest opportunity.

Apsara Stack Security provides statistics on enabled alerts and defense items. These statistics help you monitor the overall security of your assets. You can view the statistics on the **Intrusions** page.

Alerts

The following table describes the alerts.

Alert	Description
Threat intelligence	Identify potential threats to your assets based on the threat intelligence of Apsara Stack Security. Threat intelligence can correlate threat information to analyze and process the information. If threats are detected, threat intelligence can generate alerts. This helps improve the detection efficiency and response speed. Threat intelligence can detect the following items: • Malicious domain names • Malicious IP addresses • IP addresses of dark web services • IP addresses of command and control (C&C) servers • IP addresses of mining pools • Malicious URLs • Malicious download sources
Unusual Logon	Detect unusual logons to your servers. You can specify approved logon IP addresses, time periods, and accounts. Logons from unapproved IP addresses,time periods, or accounts trigger alerts. You can manually add approved logon locations or configure the system to automatically update approved logon locations. You can also specify assets on which alerts are triggered when unapproved logon locations are detected. Server Guard can detect the following events: • Logons to Elastic Compute Service (ECS) instances from unapproved IP addresses • Logons to ECS instances from unapproved locations • Execution of unusual commands after SSH-based logons to ECS instances • Brute-force attacks on SSH passwords of ECS instances

Alert	Description
Webshell	Use engines developed by Alibaba Cloud to scan common webshell files. Server Guard supports scheduled scan tasks, provides real-time protection, and quarantines webshell files. • Server Guard scans the entire web directory early in the morning on a daily basis. A change made to files in the web directory triggers dynamic detection. • You can specify the assets on which Server Guard scans for webshells. • You can quarantine or ignore detected trojan files. You can also restore the quarantined trojan files.
Precision defense	The **antivirus** feature provides precise protection from common ransomware, DDoS trojans, mining programs, trojans, malicious programs, webshells, and computer worms.
Suspicious Account	Detect logons to your assets from unapproved accounts.
Cloud threat detection	Detect threats in other cloud services.
Persistence	Detect suspicious scheduled tasks on servers and generate alerts when advanced persistent threats (APTs) to the servers are detected.
Unusual Network Connection	Detect disconnections or unusual network connections.
Suspicious Process	Detect whether suspicious processes exist.
Malicious Process	Scan your servers in real time. An agent is used to collect process information, and the information is uploaded to the cloud for detection. If viruses are detected, alerts are generated. You can handle detected viruses in Apsara Stack Security Center. Server Guard can detect the following malicious activities and processes: • Access to malicious IP addresses • Mining programs • Self-mutating trojans • Malicious programs • Trojans
Sensitive File Tampering	Check whether sensitive files on your servers are maliciously modified. The sensitive files include preloaded configuration files in Linux shared libraries.
Other	Detect other types of attacks, such as DDoS attacks.
Web Application Threat Detection	Detect intrusions that use web applications.
Application intrusion event	Detect intrusions that use system application components.

6.4.1.2. View and handle alert events

This topic describes how to view and handle detected alert events on the Intrusions page.

Background information

After alert events are detected, the alerts events are displayed on the **Intrusions** page in Apsara Stack Security Center. If the detected alert events are not handled, they are displayed in the **Unhandled Alerts** list on the **Intrusions** page. After the alert events are handled, the status of the alert events changes from **Unhandled Alerts** to **Handled**.

> **Note** Apsara Stack Security Center retains the records of **Unhandled Alerts** and **Handled** on the **Intrusions** page. By default, the records of **Unhandled Alerts** are displayed.

View alert events

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. On the page that appears, search for or view all alert events. You can also view the details about the alert events.

Handle alert events

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. On the **Intrusions** page, find the alert event that you want to handle and click **Handle** in the **Actions** column. In the dialog box that appears, configure Process Method and click **Process Now**.

   > **Note** If the alert event is related to multiple exceptions, the panel that shows alert event details appears after you click **Handle**. You can handle the exceptions in the panel.

   - **Ignore**: If you ignore the alert event, the status of the alert event changes to **Handled**. Server Guard no longer generates alerts for the event.
   - **Add To Whitelist**: If the alert event is a false positive, you can add the alert event to the whitelist. Then, the status of the alert event changes to **Handled**. Server Guard no longer generates alerts for the event. In the **Handled** list, you can click **Cancel whitelist** to remove the alert event from the whitelist.

     > **Note** When Server Guard generates a false alert on a normal process, this alert is considered a false positive. A common false positive is a **suspicious process that sends TCP packets**. The false positive notifies you that suspicious scans on other devices are detected on your servers.

   - **Batch unhandled**: This method allows you to batch handle multiple alert events. Before you

batch handle multiple alert events, we recommend that you view the details about the alert events.

5. (Optional)If you confirm that one or more alert events are false positives or need to be ignored, go to the **Intrusions** page. Then, select the alert events and click **Ignore Once** or **Whitelist**.

Export alert events

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-left corner above the alert event list on the **Intrusions** page, click the  icon to export the list.

   After the list is exported, the **Done** message appears in the upper-right corner of the Intrusions page.
5. In the **Done** notification of the **Alerts** page, click **Download**.
   The alert list is downloaded to your computer.

6.4.1.3. View exceptions related to an alert

Server Guard supports automatic analysis of exceptions related to an alert. You can click an alert name in the alert list to view and handle all exceptions that are related to the alert. You can also view the results of automatic attack tracing to analyze the exceptions.

Context

- Security Center automatically associates alerts with exceptions in real time to detect potential threats.
- Exceptions related to an alert are listed in chronological order. This allows you to analyze and handle the exceptions to improve the emergency response mechanism of your system.
- An automatically correlated alert is identified by the  icon.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. On the Intrusions page, click the **name of the alert** that you want to handle. The alert details panel appears.
5. In the alert details panel, view the details and related exceptions of the alert. Then, handle the exceptions.
   - View alert details

     You can view the assets that are affected by the alert, the first and latest time when the alert was triggered, and the details about the related exceptions.

- View affected assets

  You can move the pointer over the name of an **affected asset** to view the details about the asset. The details include information about all the alerts, vulnerabilities, baseline risks, and asset fingerprints on the asset.

- View and handle **related exceptions**

  In the **Related Exceptions** section, you can view the details about all the exceptions that are related to the alert. You can also view suggestions on how to handle the exceptions.

  - Click **Note** to the right of an exception to add a note for the exception.
  - Click the × icon to the right of a note to delete the note.

6.4.1.4. Use the file quarantine feature

Sever Guard can quarantine malicious files. Quarantined files are listed in the Quarantine panel of the Intrusions page. You can restore a quarantined file with a few clicks. However, 30 days after a file is quarantined, the system automatically deletes the file. This topic describes how to view and restore quarantined files.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-right corner of the **Intrusions** page, click **Quarantine**.

   In the **Quarantine** panel, you can perform the following operations:

   - View information about quarantined files. The information includes server IP addresses, directories in which the files are stored, file status, and modification time.
   - Click **Restore** in the **Actions** column to restore a quarantined file. The restored file appears in the alert list.

6.4.1.5. Configure alerts

This topic describes how to configure alerts. You can specify approved logon locations and customize web directories to scan.

Context

Server Guard supports advanced logon settings. You can configure more fine-grained logon detection rules. For example, you can specify approved logon IP addresses, logon time ranges, and logon accounts to block unauthorized requests that are sent to your assets.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.

3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-right corner of the page that appears, click **Settings**.

   Configure the parameters on different tabs.

   - **Add an approved logon location**
     a. In the **Login Location** section, click **Management** on the right.
     b. Select the logon location that you want to specify as the approved logon location and select the servers that allow logons from the specified location.
     c. Click **Ok**.

     Server Guard allows you to **edit** or **delete** approved logon locations that you have specified.

     - To change the servers that allow logons from an approved location, find the approved location and click **Edit** on the right.
     - To delete an approved logon location, find the logon location and click **Delete** on the right.

   - **Configure advanced logon settings**

     > **Note** When you configure advanced logon settings, you can specify the IP addresses, accounts, and time ranges that are allowed for logons to your assets. After the advanced logon settings are configured, Server Guard generates alerts if your assets receive unauthorized logon requests. The procedure of configuring advanced logon settings is similar to the procedure of configuring **Login Location**. You can **add**, **edit**, or **delete** advanced logon settings in a similar manner.

     - Turn on or turn off Uncommon IP Alert to the right of **Common Login IPs**. If you turn on Uncommon IP Alert and your assets receive logon requests from unapproved IP addresses, alerts are triggered.
     - Turn on or turn off Uncommon Time Alert to the right of **Common Login Time**. If you turn on Uncommon Time Alert and your assets receive logon requests during unapproved time ranges, alerts are triggered.
     - Turn on or turn off Uncommon Account Alert to the right of **Common Login Accounts**. If you turn on Uncommon Account Alert and your assets receive logon requests from unapproved accounts, alerts are triggered.

   - **Add web directories to scan**

     Server Guard automatically scans web directories of data assets in your servers and runs dynamic and static scan tasks. You can also manually add other web directories.

     a. In the **Add Scan Targets** section, click **Management** on the right.
     b. Specify a valid web directory and select the servers on which the specified web directory is scanned.

        > **Note** To ensure the scan performance and efficiency, we recommend that you do not specify a root directory.

     c. Click **Ok**.

6.4.1.6. Cloud threat detection

The cloud threat detection feature provided by Server Guard is integrated with widely-used antivirus engines. The feature detects viruses based on large amounts of threat intelligence data provided by Alibaba Cloud and the exception detection model designed by Alibaba Cloud. This model is designed based on machine learning and deep learning. This way, the cloud threat detection feature can provide full-scale and dynamic antivirus protection to safeguard your servers.

The cloud threat detection feature scans hundreds of millions of files on a daily basis and protects millions of servers on the cloud.

Detection capabilities

The cloud threat detection feature uses the Server Guard agent to collect process information and scans the retrieved data for viruses in the cloud. If a malicious process is detected, you can stop the process and quarantine the source files.

The cloud threat detection feature provides the following capabilities:

- **Deep learning engine developed by Alibaba Cloud**: The deep learning engine is built on deep learning technology and a large number of attack samples. The engine detects malicious files on the cloud and automatically identifies potential threats to supplement traditional antivirus engines.
- **Cloud sandbox developed by Alibaba Cloud**: The cloud sandbox feature allows you to simulate cloud environments and monitor attacks launched by malicious samples. The cloud sandbox feature automatically detects threats and offers dynamic analysis and detection capabilities based on big data analytics and machine learning modeling techniques.
- **Integration with major antivirus engines**: The cloud threat detection feature is integrated with major antivirus engines and updates its virus library in real time.
- **Threat intelligence detection**: The cloud threat detection feature works with the exception detection module to detect malicious processes and operations based on threat intelligence data provided by Alibaba Cloud Security.

Detectable virus types

The cloud threat detection feature is developed based on the security technologies and expertise of Alibaba Cloud. The feature provides end-to-end security services, including threat intelligence collection, data masking, threat identification, threat analysis, and malicious file quarantine and restoration. You can quarantine and restore files that contain viruses in the Security Center console.

The cloud threat detection feature can detect the following types of viruses.

Virus	Description
Mining program	A mining program consumes server resources and mines cryptocurrency without authorization.
Computer worm	A computer worm uses computer networks to replicate itself and spread to a large number of computers within a short period of time.
Ransomware	Ransomware, such as WannaCry, uses encryption algorithms to encrypt files and prevent users from accessing the files.
Trojan	A trojan is a program that allows an attacker to access information about servers and users, gain control of the servers, and consume system resources.

Virus	Description
DDoS trojan	A DDoS trojan hijacks servers and uses zombie servers to launch DDoS attacks, which interrupts your service.
Backdoor	A backdoor is a malicious program injected by an attacker. Then, the attacker can use the backdoor to control the server or launch attacks.
Computer virus	A computer virus inserts malicious code into normal programs and replicates the code to infect the whole system.
Malicious program	A malicious program may pose threats to system and data security.

Benefits

- **Self-developed and controllable**: The cloud threat detection feature is based on deep learning, machine learning, and big data analytics with a large number of attack and defense practices. The feature uses multiple detection engines to dynamically protect your assets against viruses.
- **Lightweight**: The cloud threat detection feature consumes only 1% of CPU resources and 50 MB of memory.
- **Dynamic**: The cloud threat detection feature dynamically retrieves startup logs of processes to monitor the startup of viruses.
- **Easy to manage**: You can manage all servers and view their status at any time in the Security Center console.

Threat detection limits

Apsara Stack Security Center allows you to detect and process security alerts, scan for and fix vulnerabilities, analyze attacks, and check security settings. Apsara Stack Security Center can analyze alerts and automatically trace attacks. This allows you to protect your assets. Apsara Stack Security supports a wide range of protection features. We recommend that you install the latest system patches on your assets. We also recommend that you use security services, such as Cloud Firewall and Web Application Firewall (WAF), to better protect your assets against attacks.

> **Note** Attacks and viruses are evolving, and security breaches may occur in various business environments. We recommend that you use the alerting, vulnerability detection, baseline check, and configuration assessment features provided by Apsara Stack Security to better protect your assets against attacks.

6.4.2. Website tamper-proofing

6.4.2.1. Overview

Tamper protection monitors website directories in real time, restores modified files or directories, and protects websites from trojans, hidden links, and uploads of violent and illicit content.

Background information

To make illegal profits or conduct business attacks, attackers exploit vulnerabilities in websites to insert illegal hidden links and tamper with the websites. Defaced web pages affect normal user access and may lead to serious economic losses, damaged brand reputation, or political risks.

Tamper protection allows you to add Linux and Windows processes to the whitelist and update protected files in real time.

How tamper protection works

The Security Center agent automatically collects the list of processes that attempt to modify files in the protected directories of the protected servers. It identifies unusual processes and file changes in real time and blocks unusual processes.

The alert list is displayed on the Tamper Protection page. You can view unusual file changes, the corresponding processes, and the number of attempts made by each process in the alert list. If a file is modified by a trusted process, you can add the process to the whitelist. After the process is added to the whitelist, tamper protection no longer blocks the process. In scenarios where the content of websites, such as news and education websites, is frequently modified, the whitelist saves you the effort of frequently enabling and disabling tamper protection.

Versions of operating systems and kernels supported by tamper protection

OS	Supported operating system version	Supported kernel version
Windows	Windows Server 2008 and later	All versions
CentOS	6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, and 7.6	• 2.6.32-x • 3.10.0-x
Ubuntu	14, 16, and 18	• 3.13.0-32-generic • 3.13.0-86-generic • 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-93-generic • 4.4.0-151-generic • 4.4.0-117-generic • 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-52-generic

Note

- The preceding table lists kernel versions supported by tamper protection. Servers that use an unsupported kernel version cannot use tamper protection. Make sure that your server uses a supported kernel version. If a kernel version is not supported, you must upgrade it to a supported version. Otherwise, you cannot add processes to the whitelist.
- Before you upgrade the server kernel, back up your asset data.

6.4.2.2. Configure tamper protection

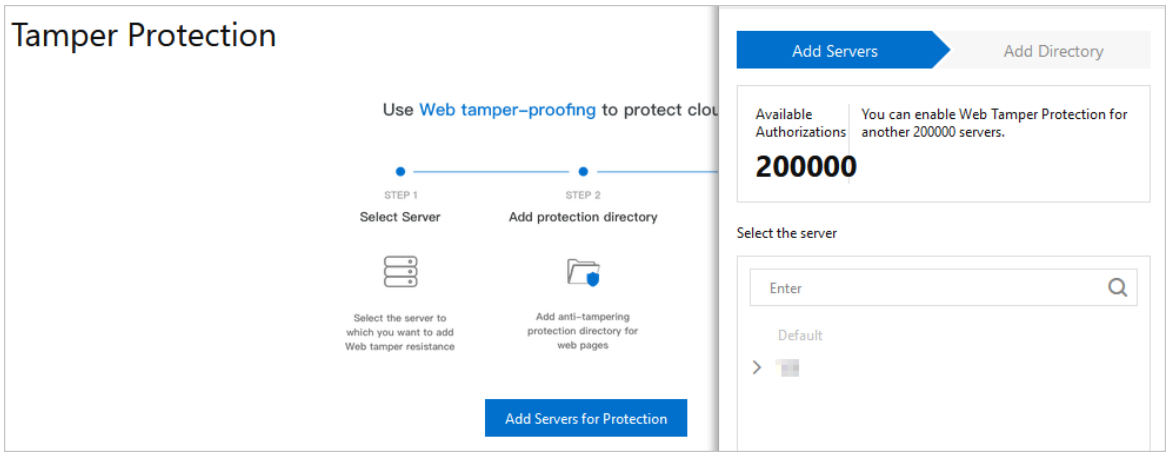
The Server Security feature allows you to configure tamper protection for web pages.

Limits

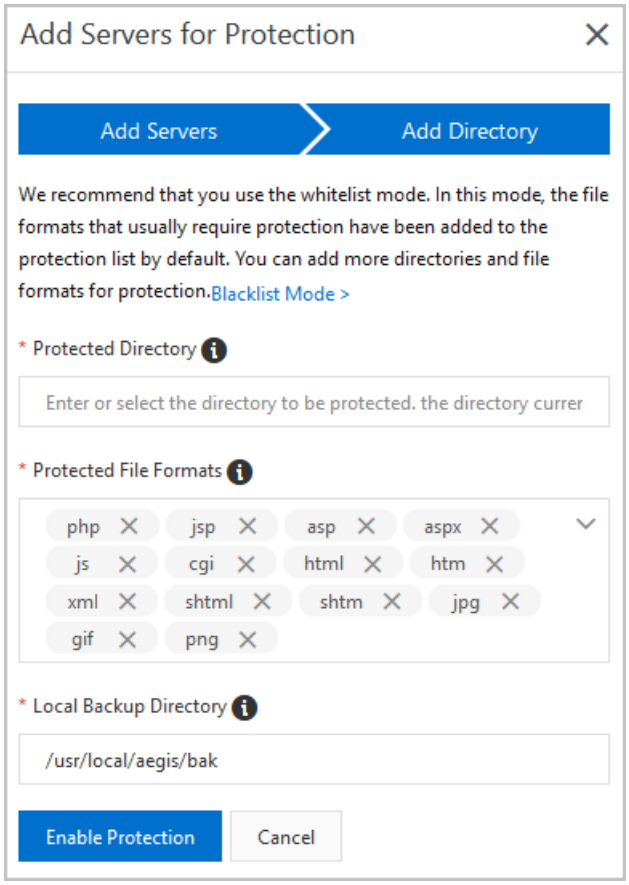
- For each server, you can add a maximum of 10 directories for protection.
- If you want to add directories that are on a Windows server, the directories must meet the following requirements: The size of each directory does not exceed 20 GB. Each directory contains no more than 2,000 folders. The number of directory levels does not exceed 20. The size of each file does not exceed 3 MB.
- If you want to add directories that are on a Linux server, the directories must meet the following requirements: The size of each directory does not exceed 20 GB. Each directory contains no more than 3,000 folders. The number of directory levels does not exceed 20. The size of each file does not exceed 3 MB.
- Before you add a directory for protection, make sure that the directory meets the preceding requirements.
- We recommend that you exclude file formats that do not require protection, such as *LOG*, *PNG*, *JPG*, *MP4*, *AVI*, and *MP3*. Multiple file formats can be separated by semicolons (;).

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **File Tamper Protection**.
4. On the **Tamper Protection** page, click **Add Servers for Protection**.
5. In the **Add Servers for Protection** panel, select a server that you want to protect.



6. Click **Next** to go to the **Add Directory** step.
7. In the **Add Directory** step, configure the parameters.



Select a protection mode. The settings of other parameters vary based on the protection mode. You can select **Whitelist Mode** or **Blacklist Mode**. In whitelist mode, tamper protection is enabled for the specified directories and file formats. In blacklist mode, tamper protection is enabled for the subdirectories, file formats, and files that are not specified. By default, Whitelist Mode is selected.

- The following table describes the parameters that you must configure if you select Whitelist Mode.

Parameter	Description
Protected Directory	Enter the path of the directory that you want to protect. **Note** Servers that run Linux or Windows operating systems use different path formats. Enter a valid directory path based on the type of your operating system.
Protected File Formats	Select file formats that you want to protect from the drop-down list, such as *js*, *html*, *xml*, and *jpg*.
Local Backup Directory	The default path in which backup files of the protected directories are stored. By default, Apsara Stack Security assigns */usr/local/aegis/bak* to Linux servers and *C:\Program Files (x86)\Alibaba\Aegis\bak* to Windows servers. You can change the default path based on your business requirements.

- The following table describes the parameters that you must configure if you select Blacklist Mode.

Parameter	Description
Protected Directory	Enter the path of the directory that you want to protect.
Excluded Sub-Directories	Enter the subdirectories that do not require tamper protection. Click **Add Sub-Directory** to add more subdirectories. Apsara Stack Security does not provide tamper protection for files in the excluded subdirectories.
Excluded File Formats	Select file formats that you do not want to protect from the drop-down list. Valid values: **log**, **txt**, and **ldb**. Apsara Stack Security does not provide tamper protection for the files in the excluded formats.
Excluded Files	Enter the path of the file for which you do not want to protect. Click **Add File** to add more files. Apsara Stack Security does not provide tamper protection for the excluded files.
Local Backup Directory	The default path in which backup files of the protected directories are stored. By default, Apsara Stack Security assigns */usr/local/aegis/bak* to Linux servers and *C:\Program Files (x86)\Alibaba\Aegis\bak* to Windows servers. You can change the default path based on your business requirements.

8. Click **Enable Protection**.
   After you enable this feature for a server, the server name is displayed on the Management tab of the **Tamper Protection** page.

   > **Note** By default, tamper protection is in the **Off** state for the server. To enable tamper protection for the server, you must **turn on** the switch in the Protection column on the **Tamper Protection** page.

9. On the **Tamper Protection** page, find the server that you add. Then, click the **Management** tab and turn on the switch in the **Protection** column to enable tamper protection for the server.

   > **Note** By default, tamper protection is in the **Off** state for the server. To enable tamper protection for the server, you must turn on the switch in the Protection column on the **Tamper Protection** page.

   After tamper protection is enabled, the status of the server changes to **Running**.

> **Note** If the status of the server is **Exception**, move the pointer over **Exception** in the Status column to view the cause and click **Retry** to enable tamper protection again.

What to do next

After you enable tamper protection for a server, you can go to the **Alerts** page and select Webpage Tampering from the alert type drop-down list to view the alerts generated upon tampering events.

> **Note**
>
> Tamper protection does not take effect immediately after you configure the protected directory, and you can still write files to the directory. In this case, you must go to the **Management** page, disable **Protection** for the server where the directory is located, and then enable **Protection** again.

Handling suggestions for abnormal protection states

State	Description	Suggestion
Initializing	Tamper protection is being initialized.	If this is the first time that you enable tamper protection for a server, the protection status becomes **Initializing**. Wait until tamper protection is enabled.
Running	Tamper protection is enabled and running as expected.	None.
Exception	An error occurred when tamper protection was enabled.	Move the pointer over **Exception** in the Status column to view the exception cause and click Retry.
Not Initialized	Tamper protection is disabled.	Turn on the switch in the **Protection** column to enable tamper protection.

6.4.2.3. View protection status

This topic describes how to view the status of tamper protection for your assets.

Context

The tamper protection feature monitors changes to the files in website directories in real time and blocks suspicious file changes. To view the status of and details about the tamper protection feature, you must log on to Apsara Stack Security Center and choose **Server Security > Intrusion Prevention > File Tamper Protection**. The following information is displayed:

- Tamper protection overview

  You can view the numbers of files that are changed on the current day and in the last 15 days, the number of protected servers, and the number of protected directories.

- Distribution of protected file types

  Protected file types include TXT, PNG, MSI, and ZIP. You can also add more types of files for tamper protection based on your business requirements.

  > Note All types of files for tamper protection can be added.

- Top five files

  This section shows the names and paths of the top five files that are ranked based on the number of changes to files in descending order in the last 15 days.

- Tamper protection alerts

  This section lists the alerts generated for blocked suspicious changes to files for your assets. You can view details about the alerts, including the severity, alert name, affected assets, paths of files with suspicious changes, and protection status.

  > Note
  > - If an alert is reported more than 100 times, we recommend that you handle the alert at your earliest opportunity.
  > - Only alerts at the **Medium** level are displayed in the console.
  > - Only alerts in the **Defended** state are displayed. These alerts are triggered when the tamper protection feature blocks suspicious processes that attempt to modify files without authorization.

6.4.3. Configure the antivirus feature

Server Guard provides the antivirus feature. This feature allows you to configure settings for virus and webshell detection.

Detect and remove viruses

The antivirus feature can automatically quarantine common Internet viruses, such as common trojans, ransomware, mining programs, and DDoS trojans. Apsara Stack Security experts check and verify all automatically quarantined viruses to avoid false positives.

If the virus blocking feature is disabled, Server Guard generates alerts when viruses are detected. You can handle the detected viruses only in Apsara Stack Security Center. We recommend that you enable the virus blocking feature to improve the security of your servers.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Virus Defence**.
4. On the **Anti-virus** tab of the page that appears, click **Scan**.
5. In the dialog box that appears, select the servers that you want to scan.
6. Click **Scan**.
7. On the **Anti-virus** page, click the **Real-time protection** tab and turn on Virus Blocking to enable the virus blocking feature.

After the virus blocking feature is enabled, Server Guard quarantines common viruses that are detected. Quarantined viruses are listed on the Alerts page. To filter these viruses, you can select the **Precision defense** type.

Detect and remove webshells

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Virus Defence**.
4. Specify servers for webshell detection.
   i. In the **Webshell Detection** section, click **Manage**.
   ii. Select the servers for which you want to enable webshell detection.
   iii. Click **OK** to complete the configuration.

6.5. Log retrieval

6.5.1. Log retrieval overview

The log retrieval function provided by Server Security allows you to manage logs scattered in various systems of Apsara Stack in a centralized manner, so that you can easily identify the causes of issues that occur on your servers.

The log retrieval function supports storage of logs for 180 days and query of logs generated within 30 days.

Benefits

The log retrieval function provides the following benefits:

- **End-to-end log retrieval platform**: Allows you to retrieve logs of various Apsara Stack services in a centralized manner and trace issues easily.
- **Cloud-based SaaS service**: Allows you to query logs on all servers in Apsara Stack without additional installment and deployment.
- Supports TB-level data retrieval. It also allows you to add a maximum of 50 inference rules (Boolean expressions) in a search condition and obtain full-text search results within several seconds.
- Supports a wide range of log sources.
- Supports log shipping, which allows you to import security logs to Log Service for further analysis.

Scenarios

You can use log retrieval to meet the following requirements:

- **Security event analysis**: When a security event is detected on a server, you can retrieve the logs to identify the cause and assess the damage and affected assets.
- **Operation audit**: You can audit the operation logs on a server to identify high-risk operations and serious issues in a meticulous way.

Supported log types

Log types

Log type	Description
Logon history	Log entries about successful system logons
Brute-force attack	Log entries about system logon failures that are generated during brute-force attacks
Process snapshot	Log entries about processes on a server at a specific time
Listening port snapshot	Log entries about listening ports on a server at a specific time
Account snapshot	Log entries about account logon information on a server at a specific time
Process initiation	Log entries about process initiation on a server
Network connection	Log entries about active connections from a server to external networks

6.5.2. Query logs

This topic describes how to search for and view server logs.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Log Retrieval**.
4. Specify search conditions.

Search condition	Description
Log source	The log source that you want to query. For more information, see Log sources.
Field	The field that is recorded for the log source. For more information, see Log sources.
Keyword	The keyword of the field.
Logical operator	The equality operator.
+	The inference rules in a search condition for a log source.
Add conditions	The search conditions for different log sources.

5. Click **Search** and view the search result.
   - **Reset**: Click **Reset** to clear the search condition configurations.
   - **Saved Searches**: Click **Saved Searches** to select and use the search condition configurations that you saved.

6.5.3. Supported log sources and fields

This topic describes the log sources and fields that are supported by the log retrieval feature.

The log retrieval feature allows you to query the following types of log sources. You can click a log source link to view the fields that can be retrieved.

Log source	Description
Logon history	Log entries about successful system logons
Logs of brute-force attacks	Log entries about failed system logons during brute-force attacks
Process snapshot logs	Log entries about processes on a server at a specific point in time
Logs of listening port snapshots	Log entries about listening ports on a server at a specific point in time
Account snapshot logs	Log entries about account-based logons on a server at a specific point in time
Process startup logs	Log entries about process startups on a server
Network connection logs	Log entries about active connections from a server to the Internet.

Logon history

The following table describes the fields that you can use to query the logon history.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
warn_ip	string	The source IP address used for the logon.
warn_port	string	The logon port.
warn_user	string	The username used for the logon.
warn_type	string	The logon type.
warn_count	string	The number of logon attempts.

Logs of brute-force attacks

The following table describes the fields that you can use to query logs of brute-force attacks.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
warn_ip	string	The source IP address of the attack.
warn_port	string	The target port of the attack.
warn_user	string	The target username of the attack.
warn_type	string	The attack type.
warn_count	string	The number of brute-force attack attempts.

Process startup logs

The following table describes the fields that you can use to query process startup logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
pid	string	The ID of the process.
groupname	string	The user group.
ppid	string	The ID of the parent process.
uid	string	The ID of the user.
username	string	The username.
filename	string	The file name.
pfilename	string	The name of the parent process file.
cmdline	string	The command line.
filepath	string	The path of the process file.
pfilepath	string	The path of the parent process file.

Logs of listening port snapshots

The following table describes the fields that you can use to query logs about listening port snapshots.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
src_port	string	The listening port.
src_ip	string	The listening IP address.
proc_path	string	The path of the process file.
pid	string	The ID of the process.
proc_name	string	The name of the process.
proto	string	The protocol.

Account snapshot logs

The following table describes the fields you can use to query account snapshot logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
perm	string	Indicates whether the user has root permissions.
home_dir	string	The home directory.
warn_time	string	The time when a password expiration notification is sent.
groups	string	The group to which the user belongs.
login_ip	string	The IP address of the last logon.
last_chg	string	The time when the password was last changed.
shell	string	The Linux shell command.
domain	string	The Windows domain.
tty	string	The logon terminal.
account_expire	string	The time when the account expires.

Field	Data type	Description
passwd_expire	string	The time when the password expires.
last_logon	string	The last logon time.
user	string	The username.
status	string	The account status. Valid values: • 0: disabled • 1: normal

Process snapshot logs

The following table describes the fields that you can use to query process snapshot logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
path	string	The path of the process file.
start_time	string	The time when the process was started.
uid	string	The ID of the user.
cmdline	string	The command line.
pname	string	The name of the parent process.
name	string	The name of the process.
pid	string	The ID of the process.
user	string	The username.
md5	string	The MD5 hash value of the process file. If the size of the process file exceeds 1 MB, the system does not calculate the MD5 hash value of the process file.

Network connection logs

The following table describes the fields that you can use to query network connection logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
src_ip	string	The source IP address.
src_port	string	The source port.
proc_path	string	The path of the process file.
dst_port	string	The destination port.
proc_name	string	The name of the process.
dst_ip	string	The destination IP address.
status	string	The status.

6.5.4. Logical operators

The log retrieval feature supports multiple search conditions. You can add multiple logical operators to one search condition for one log source, or combine multiple search conditions for several log sources by using different logical operators. This topic describes the logical operators that are supported in log retrieval. Examples are provided to help you understand these operators.

The following table describes the logical operators that are supported in log retrieval.

Logical operators

Logical operator	Description
and	Binary operator. This operator is in the format of `query 1 and query 2`, which indicates the intersection of the query results of `query 1` and `query 2`. **Note** If no logical operators are used for multiple keywords, the default operator is AND.
or	Binary operator. This operator is in the format of `query 1 or query 2`, which indicates the union of the query results of `query 1` and `query 2`.

Logical operator	Description
not	Binary operator. This operator is in the format of `query 1 not query 2`, which indicates the results that match `query 1` but do not match `query 2`. This format is equivalent to `query 1 - query 2`. **Note** If you use only `not query 1`, the log data that does not contain the query results of `query 1` is returned.

6.6. Settings

6.6.1. Install the Server Guard agent

This topic describes how to install the Server Guard agent.

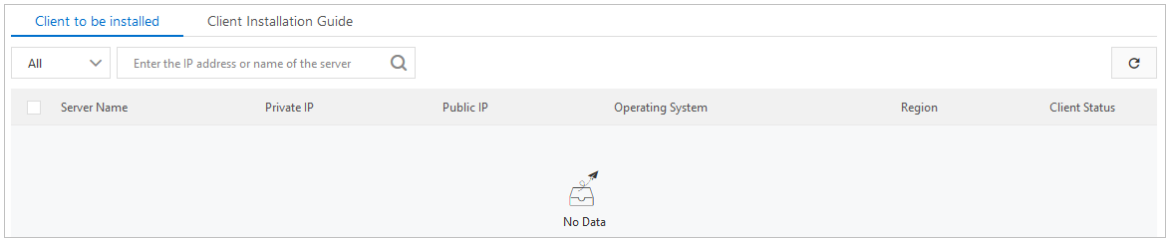
Context

To use the protection features provided by Server Guard, you must install the Server Guard agent on the operating system of your server.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Client Installation**.
4. (Optional)On the page that appears, click the **Client to be installed** tab to view the number of the servers on which the Server Guard agent is not installed. On this tab, you can also view information about these servers.

   You can specify the operating system type, server IP address, or server name to search for a server.

5. Click the **Client Installation Guide** tab.
6. Download and install the Server Guard agent based on the operating system of your server.
   - **Windows**
     a. In the left-side pane of the page, click **Click to download** to download the installation package to your computer.
     b. Upload the installation package to your server. For example, you can use an FTP client to upload the installation package to your server.

c. Run the installation package on your server as an administrator.

> **Note** If you install the agent on a server that is not in Alibaba Cloud, you are prompted to enter the installation verification key. You can find the installation verification key on the Client Installation Guide tab.

- **Linux**
  a. In the right-side pane of the page, select Alibaba Cloud Server or Non-Alibaba Server.
  b. Select the installation command for your 32-bit or 64-bit operating system and click **Copy** to copy the command.
  c. Log on to your Linux server as an administrator.
  d. Run the installation command on your Linux server to download and install the Server Guard agent.

6.6.2. Manage protection modes

This topic describes how to manage protection modes for a server to improve the performance and security of the server.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Protection Mode**.
4. On the **Protection First Mode** page, click **Manage** next to Protection Mode.

   Configure protection modes for servers.

   - **Business First Mode**: In this mode, the peak CPU utilization is less than 10%, and the peak memory usage is less than 50 MB.
   - **Protection First Mode**: In this mode, the peak CPU utilization is less than 20%, and the peak memory usage is less than 80 MB.
5. Click **OK**.

7.Physical server security

7.1. Create and grant permissions to a security administrator account

The physical server security feature is used to ensure the security of physical servers on the platform side. This feature requires you to use a dedicated security administrator account for the platform. This topic describes how to create and grant permissions to a security administrator account.

Procedure

1. Log on to the Apsara Uni-manager Management Console as a system administrator.

   For more information, see the **"Log on to the Apsara Uni-manager Management Console"** topic of *Apsara Uni-manager Management Console User Guide*.

2. Create a dedicated organization that is used to manage the security of physical servers, and obtain the primary key of the organization.

   > **Notice** Make sure that the organization is used only to manage the security of physical servers. Do not add Elastic Compute Service (ECS) instances to the organization.

   i. Create the dedicated organization.

   For more information, see **Enterprise Center > Organization Management > Create Organization** in *Apsara Uni-manager Management Console User Guide*.

   ii. Obtain the **primary key** of the newly created organization.

   For more information, see **Enterprise Center > Organization Management > Obtain the AccessKey pair of an organization** in *Apsara Uni-manager Management Console User Guide*.

3. Create a dedicated account to manage the security of physical servers.

   For more information, see **Enterprise Center > User Management > System User Management > Create User** in *Apsara Uni-manager Management Console User Guide*.

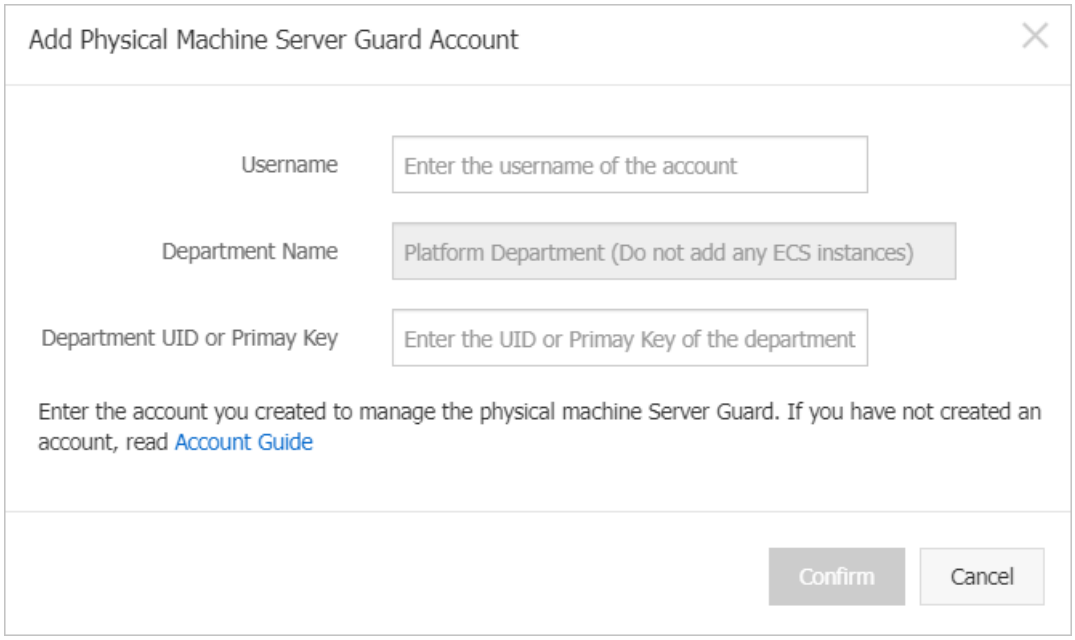
   > **Note** When you create the account, take note of the following points for the **organization** and **role**:
   >
   > - In the **Organization** section, select the organization that is created in the previous step.
   > - In the **Role** section, select **Platform Security Configuration Administrator** and **Security System Configuration Administrator**.

4. Log on to Apsara Stack Security Center by using the newly created account.

   For more information, see Log on to Apsara Stack Security Center.

5. Add the **primary key** of the newly created organization to the protection configuration of physical servers.

i. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Global Platform Security** section, click **Alibaba Cloud Security**.
ii. In the left-side navigation pane, click **Global Settings**
iii. On the **Global Settings** page, click the **Physical Machine Protection Configurations** tab.
iv. Click **Add Account**.
v. In the **Add Physical Machine Server Guard Account** dialog box, configure the **Username** and **Department UID or Primay Key** parameters.



- **Username**: Enter the account that you created in Step 3.
- **Primary Key**: Enter the primary key that you obtained in Step 2.

vi. Click **Confirm**.

Result

After the settings are complete, you can use the dedicated security administrator account that is created in this section to ensure the security of physical servers on the platform side.

7.2. Physical servers

7.2.1. Manage physical server groups

This topic describes how to manage physical server groups. To facilitate the security management of physical servers, you can add the physical servers to groups and view their security events by group.

Context

By default, physical servers do not belong to a server group. You must add your physical servers to a server group. If you delete a group, all the physical servers in the group are retained but no longer belong to a server group.

Procedure

1. Log on to Apsara Stack Security Center.

   > **Note** For more information about the Apsara Stack tenant account, see Create and grant permissions to a security administrator account.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, choose **Physical Server Security > Servers**.
4. In the left-side group pane, manage sever groups.
   - Create a group.

     Click the Add Subgroup icon next to **All Servers** or a specific group, enter a group name, and click **OK**.

     > **Note** The system supports a maximum of three levels of groups.

   - Modify a group.

     Click the Modify Group Name icon next to the target group, enter a new name, and click **OK**.

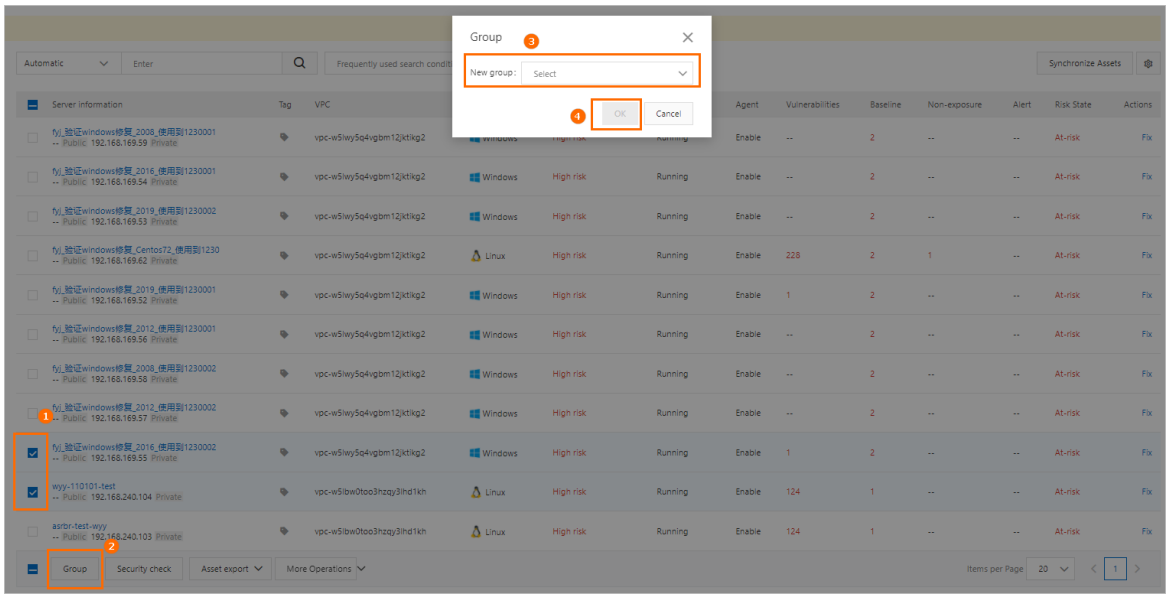
   - Delete a group.

     Click the Delete icon next to the target group. In the message that appears, click **OK**.

     > **Note** After you delete a group, all servers in the group are automatically moved to the **default** group.

   - Sort groups.

     Click **Manage Groups** to sort groups in descending order by priority.
5. Change the server group of specific physical servers.

   i. Select servers from the list on the right.

   ii. Click **Change Group**.

iii. In the Change Group dialog box that appears, select a group from the drop-down list.

iv. Click **OK**.

7.2.2. Manage physical servers

This topic describes how to manage servers. On the Servers page, you can view the status of servers protected by Server Guard.

Procedure

1. Log on to Apsara Stack Security Center.

   > **Note** For more information about the Apsara Stack tenant account, see Create and grant permissions to a security administrator account.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Servers**.
4. (Optional)Search for a server.

   To view the agent status of a server, enter the server IP address in the search bar, and click **Search**. Detailed server information, such as security information, is displayed.
5. View the agent status and detailed security information of the server.

   Click

   in the upper-right corner of the page to select the information columns you want to display. The following table lists the information categories.

Category	Information
Basic information	○ Server IP/Name ○ Tag ○ OS ○ Region
Agent status	Agent Status
Threat prevention	○ Vulnerability ○ Baseline Risk
Intrusion detection	○ Unusual Logons ○ Webshells ○ Suspicious Servers

Category	Information
Server fingerprints	○ Processes ○ Ports ○ Root Accounts/Total Accounts

6. Manage servers.

Action	Description
Change Group	Select servers and click **Change Group** to add the selected servers to a new group.
Modify Tag	Select servers and click **Modify Tag** to modify tags for the servers.
Security Inspection	Select servers and click **Security Inspection** to select the items to be checked.
Delete External Servers	Select **external** servers, and choose **More > Delete External Servers**.
Disable Protection	Select the servers whose agent status is **Online**, and choose **More > Disable Protection**. This temporarily disables protection for these servers to reduce server resource consumption.
Enable Protection	Select the servers whose agent status is **Disable Protection**, and choose **More > Enable Protection**. This enables protection for these servers.

7.3. Intrusion events

7.3.1. Intrusion event types

If Server Guard detects sensitive file tampering, suspicious processes, webshells, unusual logons, or malicious processes, it generates alerts. Based on these alerts, you can monitor the security status of your assets and handle potential threats at the earliest opportunity.

Apsara Stack Security provides statistics on enabled alerts and defense items. These statistics help you monitor the overall security of your assets. You can view the statistics on the **Intrusions** page.

Alerts

The following table describes the alerts.

Alert	Description

Alert	Description
Threat intelligence	Identify potential threats to your assets based on the threat intelligence of Apsara Stack Security. Threat intelligence can correlate threat information to analyze and process the information. If threats are detected, threat intelligence can generate alerts. This helps improve the detection efficiency and response speed. Threat intelligence can detect the following items: • Malicious domain names • Malicious IP addresses • IP addresses of dark web services • IP addresses of command and control (C&C) servers • IP addresses of mining pools • Malicious URLs • Malicious download sources
Unusual Logon	Detect unusual logons to your servers. You can specify approved logon IP addresses, time periods, and accounts. Logons from unapproved IP addresses,time periods, or accounts trigger alerts. You can manually add approved logon locations or configure the system to automatically update approved logon locations. You can also specify assets on which alerts are triggered when unapproved logon locations are detected. Server Guard can detect the following events: • Logons to Elastic Compute Service (ECS) instances from unapproved IP addresses • Logons to ECS instances from unapproved locations • Execution of unusual commands after SSH-based logons to ECS instances • Brute-force attacks on SSH passwords of ECS instances
Webshell	Use engines developed by Alibaba Cloud to scan common webshell files. Server Guard supports scheduled scan tasks, provides real-time protection, and quarantines webshell files. • Server Guard scans the entire web directory early in the morning on a daily basis. A change made to files in the web directory triggers dynamic detection. • You can specify the assets on which Server Guard scans for webshells. • You can quarantine or ignore detected trojan files. You can also restore the quarantined trojan files.
Precision defense	The **antivirus** feature provides precise protection from common ransomware, DDoS trojans, mining programs, trojans, malicious programs, webshells, and computer worms.
Suspicious Account	Detect logons to your assets from unapproved accounts.
Cloud threat detection	Detect threats in other cloud services.

Alert	Description
Persistence	Detect suspicious scheduled tasks on servers and generate alerts when advanced persistent threats (APTs) to the servers are detected.
Unusual Network Connection	Detect disconnections or unusual network connections.
Suspicious Process	Detect whether suspicious processes exist.
Malicious Process	Scan your servers in real time. An agent is used to collect process information, and the information is uploaded to the cloud for detection. If viruses are detected, alerts are generated. You can handle detected viruses in Apsara Stack Security Center. Server Guard can detect the following malicious activities and processes: • Access to malicious IP addresses • Mining programs • Self-mutating trojans • Malicious programs • Trojans
Sensitive File Tampering	Check whether sensitive files on your servers are maliciously modified. The sensitive files include preloaded configuration files in Linux shared libraries.
Other	Detect other types of attacks, such as DDoS attacks.
Web Application Threat Detection	Detect intrusions that use web applications.
Application intrusion event	Detect intrusions that use system application components.

7.3.2. View and handle alert events

This topic describes how to view and handle detected alert events on the Intrusions page.

Background information

After alert events are detected, the alerts events are displayed on the **Intrusions** page in Apsara Stack Security Center. If the detected alert events are not handled, they are displayed in the **Unhandled Alerts** list on the **Intrusions** page. After the alert events are handled, the status of the alert events changes from **Unhandled Alerts** to **Handled**.

> **Note** Apsara Stack Security Center retains the records of **Unhandled Alerts** and **Handled** on the **Intrusions** page. By default, the records of **Unhandled Alerts** are displayed.

View alert events

1. Log on to Apsara Stack Security Center.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. On the page that appears, search for or view all alert events. You can also view the details about the alert events.

Handle alert events

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. On the **Intrusions** page, find the alert event that you want to handle and click **Handle** in the **Actions** column. In the dialog box that appears, configure Process Method and click **Process Now**.

   > **Note** If the alert event is related to multiple exceptions, the panel that shows alert event details appears after you click **Handle**. You can handle the exceptions in the panel.

   - **Ignore**: If you ignore the alert event, the status of the alert event changes to **Handled**. Server Guard no longer generates alerts for the event.
   - **Add To Whitelist**: If the alert event is a false positive, you can add the alert event to the whitelist. Then, the status of the alert event changes to **Handled**. Server Guard no longer generates alerts for the event. In the **Handled** list, you can click **Cancel whitelist** to remove the alert event from the whitelist.

     > **Note** When Server Guard generates a false alert on a normal process, this alert is considered a false positive. A common false positive is a **suspicious process that sends TCP packets**. The false positive notifies you that suspicious scans on other devices are detected on your servers.

   - **Batch unhandled**: This method allows you to batch handle multiple alert events. Before you batch handle multiple alert events, we recommend that you view the details about the alert events.
5. (Optional)If you confirm that one or more alert events are false positives or need to be ignored, go to the **Intrusions** page. Then, select the alert events and click **Ignore Once** or **Whitelist**.

Export alert events

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-left corner above the alert event list on the **Intrusions** page, click the  icon to export the list.

   After the list is exported, the **Done** message appears in the upper-right corner of the Intrusions page.

5. In the **Done** notification of the **Alerts** page, click **Download**.
   The alert list is downloaded to your computer.

7.3.3. View exceptions related to an alert

Server Guard supports automatic analysis of exceptions related to an alert. You can click an alert name in the alert list to view and handle all exceptions that are related to the alert. You can also view the results of automatic attack tracing to analyze the exceptions.

Context

- Security Center automatically associates alerts with exceptions in real time to detect potential threats.
- Exceptions related to an alert are listed in chronological order. This allows you to analyze and handle the exceptions to improve the emergency response mechanism of your system.
- An automatically correlated alert is identified by the  icon.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. On the Intrusions page, click the **name of the alert** that you want to handle. The alert details panel appears.
5. In the alert details panel, view the details and related exceptions of the alert. Then, handle the exceptions.
   - View alert details

     You can view the assets that are affected by the alert, the first and latest time when the alert was triggered, and the details about the related exceptions.
   - View affected assets

     You can move the pointer over the name of an **affected asset** to view the details about the asset. The details include information about all the alerts, vulnerabilities, baseline risks, and asset fingerprints on the asset.
   - View and handle **related exceptions**

     In the **Related Exceptions** section, you can view the details about all the exceptions that are related to the alert. You can also view suggestions on how to handle the exceptions.
     - Click **Note** to the right of an exception to add a note for the exception.
     - Click the icon to the right of a note to delete the note.

7.3.4. Use the file quarantine feature

Sever Guard can quarantine malicious files. Quarantined files are listed in the Quarantine panel of the Intrusions page. You can restore a quarantined file with a few clicks. However, 30 days after a file is quarantined, the system automatically deletes the file. This topic describes how to view and restore quarantined files.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-right corner of the **Intrusions** page, click **Quarantine**.

   In the **Quarantine** panel, you can perform the following operations:

   - View information about quarantined files. The information includes server IP addresses, directories in which the files are stored, file status, and modification time.
   - Click **Restore** in the **Actions** column to restore a quarantined file. The restored file appears in the alert list.

7.3.5. Configure alerts

This topic describes how to configure alerts. You can specify approved logon locations and customize web directories to scan.

Context

Server Guard supports advanced logon settings. You can configure more fine-grained logon detection rules. For example, you can specify approved logon IP addresses, logon time ranges, and logon accounts to block unauthorized requests that are sent to your assets.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Intrusions**.
4. In the upper-right corner of the page that appears, click **Settings**.

   Configure the parameters on different tabs.

   - **Add an approved logon location**
     a. In the **Login Location** section, click **Management** on the right.
     b. Select the logon location that you want to specify as the approved logon location and select the servers that allow logons from the specified location.
     c. Click **Ok**.

   Server Guard allows you to **edit** or **delete** approved logon locations that you have specified.

   - To change the servers that allow logons from an approved location, find the approved location and click **Edit** on the right.
   - To delete an approved logon location, find the logon location and click **Delete** on the right.

- **Configure advanced logon settings**

  > **Note** When you configure advanced logon settings, you can specify the IP addresses, accounts, and time ranges that are allowed for logons to your assets. After the advanced logon settings are configured, Server Guard generates alerts if your assets receive unauthorized logon requests. The procedure of configuring advanced logon settings is similar to the procedure of configuring **Login Location**. You can **add**, **edit**, or **delete** advanced logon settings in a similar manner.

  - Turn on or turn off Uncommon IP Alert to the right of **Common Login IPs**. If you turn on Uncommon IP Alert and your assets receive logon requests from unapproved IP addresses, alerts are triggered.
  - Turn on or turn off Uncommon Time Alert to the right of **Common Login Time**. If you turn on Uncommon Time Alert and your assets receive logon requests during unapproved time ranges, alerts are triggered.
  - Turn on or turn off Uncommon Account Alert to the right of **Common Login Accounts**. If you turn on Uncommon Account Alert and your assets receive logon requests from unapproved accounts, alerts are triggered.

- **Add web directories to scan**

  Server Guard automatically scans web directories of data assets in your servers and runs dynamic and static scan tasks. You can also manually add other web directories.

  a. In the **Add Scan Targets** section, click **Management** on the right.
  b. Specify a valid web directory and select the servers on which the specified web directory is scanned.

     > **Note** To ensure the scan performance and efficiency, we recommend that you do not specify a root directory.

  c. Click **Ok**.

7.3.6. Cloud threat detection

The cloud threat detection feature provided by Server Guard is integrated with widely-used antivirus engines. The feature detects viruses based on large amounts of threat intelligence data provided by Alibaba Cloud and the exception detection model designed by Alibaba Cloud. This model is designed based on machine learning and deep learning. This way, the cloud threat detection feature can provide full-scale and dynamic antivirus protection to safeguard your servers.

The cloud threat detection feature scans hundreds of millions of files on a daily basis and protects millions of servers on the cloud.

Detection capabilities

The cloud threat detection feature uses the Server Guard agent to collect process information and scans the retrieved data for viruses in the cloud. If a malicious process is detected, you can stop the process and quarantine the source files.

The cloud threat detection feature provides the following capabilities:

- **Deep learning engine developed by Alibaba Cloud**: The deep learning engine is built on deep

learning technology and a large number of attack samples. The engine detects malicious files on the cloud and automatically identifies potential threats to supplement traditional antivirus engines.

- **Cloud sandbox developed by Alibaba Cloud**: The cloud sandbox feature allows you to simulate cloud environments and monitor attacks launched by malicious samples. The cloud sandbox feature automatically detects threats and offers dynamic analysis and detection capabilities based on big data analytics and machine learning modeling techniques.
- **Integration with major antivirus engines**: The cloud threat detection feature is integrated with major antivirus engines and updates its virus library in real time.
- **Threat intelligence detection**: The cloud threat detection feature works with the exception detection module to detect malicious processes and operations based on threat intelligence data provided by Alibaba Cloud Security.

Detectable virus types

The cloud threat detection feature is developed based on the security technologies and expertise of Alibaba Cloud. The feature provides end-to-end security services, including threat intelligence collection, data masking, threat identification, threat analysis, and malicious file quarantine and restoration. You can quarantine and restore files that contain viruses in the Security Center console.

The cloud threat detection feature can detect the following types of viruses.

Virus	Description
Mining program	A mining program consumes server resources and mines cryptocurrency without authorization.
Computer worm	A computer worm uses computer networks to replicate itself and spread to a large number of computers within a short period of time.
Ransomware	Ransomware, such as WannaCry, uses encryption algorithms to encrypt files and prevent users from accessing the files.
Trojan	A trojan is a program that allows an attacker to access information about servers and users, gain control of the servers, and consume system resources.
DDoS trojan	A DDoS trojan hijacks servers and uses zombie servers to launch DDoS attacks, which interrupts your service.
Backdoor	A backdoor is a malicious program injected by an attacker. Then, the attacker can use the backdoor to control the server or launch attacks.
Computer virus	A computer virus inserts malicious code into normal programs and replicates the code to infect the whole system.
Malicious program	A malicious program may pose threats to system and data security.

Benefits

- **Self-developed and controllable**: The cloud threat detection feature is based on deep learning, machine learning, and big data analytics with a large number of attack and defense practices. The feature uses multiple detection engines to dynamically protect your assets against viruses.
- **Lightweight**: The cloud threat detection feature consumes only 1% of CPU resources and 50 MB of

memory.

- **Dynamic**: The cloud threat detection feature dynamically retrieves startup logs of processes to monitor the startup of viruses.
- **Easy to manage**: You can manage all servers and view their status at any time in the Security Center console.

Threat detection limits

Apsara Stack Security Center allows you to detect and process security alerts, scan for and fix vulnerabilities, analyze attacks, and check security settings. Apsara Stack Security Center can analyze alerts and automatically trace attacks. This allows you to protect your assets. Apsara Stack Security supports a wide range of protection features. We recommend that you install the latest system patches on your assets. We also recommend that you use security services, such as Cloud Firewall and Web Application Firewall (WAF), to better protect your assets against attacks.

> **Note** Attacks and viruses are evolving, and security breaches may occur in various business environments. We recommend that you use the alerting, vulnerability detection, baseline check, and configuration assessment features provided by Apsara Stack Security to better protect your assets against attacks.

7.4. Server fingerprints

7.4.1. Manage listening ports

This topic describes how to view information about the listening port of a server. The information helps you identify suspicious listening behavior.

Context

This topic is suitable for the following scenarios:

- Check for servers that listen on a specific port.
- Check for ports that a specific server listens.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Port** tab to view **listening ports**, **network protocols**, and server information.

   You can search for a port by using the port number, server process name, server name, or server IP address.

   In the server information list, you can view the **process**, **IP address**, and **latest scan time** of a server.

7.4.2. Manage software versions

This topic describes how to regularly view and collect the software version information about a server. This helps you check your software assets.

Context

This topic covers the following scenarios:

- Check for software assets that are installed without authorization.
- Check for outdated software assets.
- Locate affected assets if vulnerabilities are detected.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Server Security > Sever Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the page that appears, click the **Software** tab. On the tab, view all the **software assets** that are in use and the **number of the servers** that use the software assets.

   You can search for specific software by using its name, version, installation directory, server name, or IP address.
5. Click software to view the details, such as the software versions and the servers that use the software.

   You can click the icon in the upper-right corner to download a software version table to your computer for subsequent asset check.

7.4.3. Manage processes

This topic describes how to regularly collect the process information on a server and record changes. This way, you can view process information and historical process changes.

Context

This task is suitable for the following scenarios:

- Check for servers on which a specific process runs.
- Check for processes that run on a specific server.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the page that appears, click the **Process** tab. On the tab, view all running processes and the number of servers that run these processes.

   You can search for a process by using the **process name**, **running user**, **startup parameter**, or **server name or IP address**.
5. Click the name of a process to view the details of the process, such as the servers, paths, and

startup parameters.

7.4.4. Manage account information

This topic describes how to regularly collect the account information on a server and record the changes to the accounts. This way, you can check your accounts and view historical changes to your accounts.

Context

You can use the information collected in this topic for the following scenarios:

- Check for servers on which a specific account is created.
- Check for accounts that are created on a server.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Account** tab.
5. View all the logged-on accounts and the numbers of servers on which the accounts are created.

   You can search for an account by using the account name, root permissions, server name, or server IP address.
6. Click an account name to view the details, such as the server information, root permissions, and user group.

7.4.5. Manage scheduled tasks

This topic describes how to view scheduled tasks on servers.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. On the **Asset Fingerprints** page, click the **Scheduled Tasks** tab.
5. View the paths of all tasks and the number of servers that run these tasks.

   You can search for a task by using the task path, server name, or IP address.
6. Click a task path to view the details, such as the servers, executed commands, and task cycles.

7.4.6. Set the fingerprint collection frequency

You can set the frequency at which the data of running processes, system accounts, listening ports, and software versions is collected.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Server Fingerprints**.
4. In the upper-right corner of the **Asset Fingerprints** page, click **Settings**.
5. Select the collection frequency from each drop-down list.
6. Click **OK** to complete the configuration.

7.5. Log retrieval

7.5.1. Supported log sources and fields

This topic describes the log sources and fields that are supported by the log retrieval feature.

The log retrieval feature allows you to query the following types of log sources. You can click a log source link to view the fields that can be retrieved.

Log source	Description
Logon history	Log entries about successful system logons
Logs of brute-force attacks	Log entries about failed system logons during brute-force attacks
Process snapshot logs	Log entries about processes on a server at a specific point in time
Logs of listening port snapshots	Log entries about listening ports on a server at a specific point in time
Account snapshot logs	Log entries about account-based logons on a server at a specific point in time
Process startup logs	Log entries about process startups on a server
Network connection logs	Log entries about active connections from a server to the Internet.

Logon history

The following table describes the fields that you can use to query the logon history.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
warn_ip	string	The source IP address used for the logon.

Field	Data type	Description
warn_port	string	The logon port.
warn_user	string	The username used for the logon.
warn_type	string	The logon type.
warn_count	string	The number of logon attempts.

Logs of brute-force attacks

The following table describes the fields that you can use to query logs of brute-force attacks.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
warn_ip	string	The source IP address of the attack.
warn_port	string	The target port of the attack.
warn_user	string	The target username of the attack.
warn_type	string	The attack type.
warn_count	string	The number of brute-force attack attempts.

Process startup logs

The following table describes the fields that you can use to query process startup logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
pid	string	The ID of the process.
groupname	string	The user group.
ppid	string	The ID of the parent process.
uid	string	The ID of the user.
username	string	The username.

Field	Data type	Description
filename	string	The file name.
pfilename	string	The name of the parent process file.
cmdline	string	The command line.
filepath	string	The path of the process file.
pfilepath	string	The path of the parent process file.

Logs of listening port snapshots

The following table describes the fields that you can use to query logs about listening port snapshots.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
src_port	string	The listening port.
src_ip	string	The listening IP address.
proc_path	string	The path of the process file.
pid	string	The ID of the process.
proc_name	string	The name of the process.
proto	string	The protocol.

Account snapshot logs

The following table describes the fields you can use to query account snapshot logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
perm	string	Indicates whether the user has root permissions.
home_dir	string	The home directory.
warn_time	string	The time when a password expiration notification is sent.

Field	Data type	Description
groups	string	The group to which the user belongs.
login_ip	string	The IP address of the last logon.
last_chg	string	The time when the password was last changed.
shell	string	The Linux shell command.
domain	string	The Windows domain.
tty	string	The logon terminal.
account_expire	string	The time when the account expires.
passwd_expire	string	The time when the password expires.
last_logon	string	The last logon time.
user	string	The username.
status	string	The account status. Valid values: • 0: disabled • 1: normal

Process snapshot logs

The following table describes the fields that you can use to query process snapshot logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
path	string	The path of the process file.
start_time	string	The time when the process was started.
uid	string	The ID of the user.
cmdline	string	The command line.
pname	string	The name of the parent process.
name	string	The name of the process.

Field	Data type	Description
pid	string	The ID of the process.
user	string	The username.
md5	string	The MD5 hash value of the process file. If the size of the process file exceeds 1 MB, the system does not calculate the MD5 hash value of the process file.

Network connection logs

The following table describes the fields that you can use to query network connection logs.

Field	Data type	Description
uuid	string	The ID of the client.
IP	string	The IP address of the server.
src_ip	string	The source IP address.
src_port	string	The source port.
proc_path	string	The path of the process file.
dst_port	string	The destination port.
proc_name	string	The name of the process.
dst_ip	string	The destination IP address.
status	string	The status.

7.5.2. Logical operators

The log retrieval feature supports multiple search conditions. You can add multiple logical operators to one search condition for one log source, or combine multiple search conditions for several log sources by using different logical operators. This topic describes the logical operators that are supported in log retrieval. Examples are provided to help you understand these operators.

The following table describes the logical operators that are supported in log retrieval.

Logical operators

Logical operator	Description

Logical operator	Description
and	Binary operator. This operator is in the format of `query 1 and query 2`, which indicates the intersection of the query results of `query 1` and `query 2`. **Note** If no logical operators are used for multiple keywords, the default operator is AND.
or	Binary operator. This operator is in the format of `query 1 or query 2`, which indicates the union of the query results of `query 1` and `query 2`.
not	Binary operator. This operator is in the format of `query 1 not query 2`, which indicates the results that match `query 1` but do not match `query 2`. This format is equivalent to `query 1 - query 2`. **Note** If you use only `not query 1`, the log data that does not contain the query results of `query 1` is returned.

7.5.3. Query logs

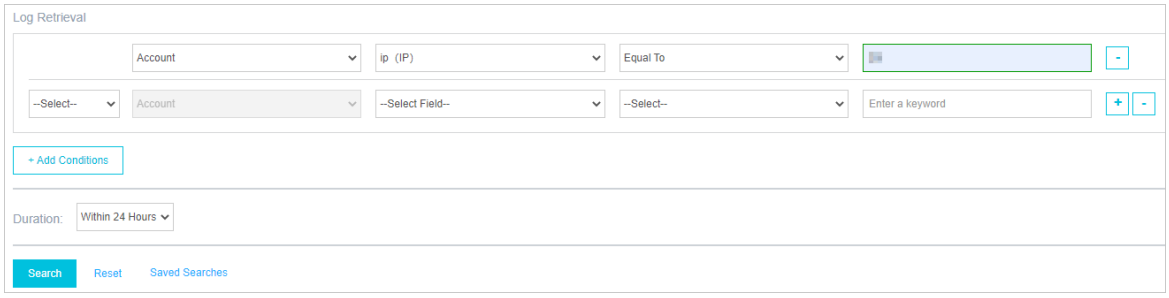
This topic describes how to search for and view physical server logs.

Procedure

1. Log on to Apsara Stack Security Center.

   Note For more information about the Apsara Stack tenant account, see Create and grant permissions to a security administrator account.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Server Security** section, click **Server Guard**.
3. In the left-side navigation pane, click **Log Retrieval**.
4. Specify search conditions.



> **Note** For more information about log sources, log fields, and logical operators, see Supported log sources and fields and Inference rules and logical operators.

5. Click **Search** and view the search result.
   - **Reset**: Click **Reset** to clear the search condition configurations.
   - **Save Search**: Click **Save Search** to save the search condition configurations which you can use to search for logs in the future.
   - **Saved Searches**: Click **Saved Searches** to select and use a search condition that you saved.

7.6. Configure security settings for physical servers

This topic describes how to configure security settings for physical servers. You can enable or disable periodic trojan scans. You can also specify the working mode of the Server Guard agent.

Procedure

1. Log on to Apsara Stack Security Center.

   > **Note** For more information about the Apsara Stack tenant account, see Create and grant permissions to a security administrator account.

2. In the left-side navigation pane, choose **Physical Server Security > Settings**.
3. Enable periodic trojan scans for physical servers.
   i. In the Trojan Scan section, click **Manage**.
   ii. In the All Servers section, select the physical servers on which you want to perform periodic trojan scans. Then, click the rightwards arrow.
   iii. Click **OK**.
4. On the **Protection First Mode** page, click **Manage** next to Protection Mode.

   Configure protection modes for servers.
   - **Business First Mode**: In this mode, the peak CPU utilization is less than 10%, and the peak memory usage is less than 50 MB.
   - **Protection First Mode**: In this mode, the peak CPU utilization is less than 20%, and the peak memory usage is less than 80 MB.

8.Application security

8.1. Quick start

This topic helps you get started with the features of Web Application Firewall (WAF).

WAF uses intelligent semantic analysis algorithms to identify web attacks. WAF also uses a learning model to enhance its analysis capabilities and meet your daily security protection requirements without relying on traditional rule libraries.

The following content describes the procedure for using WAF:

1. Customize WAF protection rules.

   WAF provides default protection policies. You can also customize policies that suit your business requirements.

   - For more information about how to configure protection policies, see Configure protection policies.
   - For more information about how to configure custom rules, see Create a custom rule.
   - For more information about how to configure HTTP flood protection rules, see Configure an HTTP flood protection rule.

2. Add websites that you want to protect.

   WAF can protect Internet websites and virtual private cloud (VPC) websites.

   - For more information about how to add an Internet website to WAF for protection, see Add an Internet website for protection.
   - For more information about how to add a VPC website to WAF for protection, see Add a VPC website for protection.

3. Configure Domain Name System (DNS) resolution.

   For more information about how to change the DNS-resolved source IP address for a website to a virtual IP address assigned by WAF, see Modify DNS resolution settings.

4. View WAF protection results.

   - For more information about how to view the protection overview, see View protection overview.
   - For more information about how to view the service access information, see View Web service access information.
   - For more information about how to view the detection logs for web attacks, see View attack detection logs.
   - For more information about how to view the detection logs for HTTP flood attacks, see View HTTP flood protection logs.

8.2. Detection overview

8.2.1. View protection overview

This topic describes how to view the Web Application Firewall (WAF) protection overview.

Context

The Detection Overview page displays information such as the statistics of previous attacks, the geographical distribution of attackers, the total number of requests, and the number of blocked requests. You can also view details about the attacks. This way, you can customize rules to protect your web services.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, click **Detection Overview**.
4. On the **Detection Overview** page, view data on the **Statistics within Last 24 Hours** and **Statistics within Last 30 Days** tabs.
   - Total Requests

     Displays the total number of requests.
   - Attack times

     Displays the total number of attacks.
   - Blocked Requests

     Displays the number of blocked requests.
   - Attacker Geographical Distribution

     Displays the distribution of attackers on a map. You can select a map of China or a map of the world.

     Displays both the numbers of total requests and blocked requests.
   - Initiate Attack IP appears most frequently (Display TOP 5)

     Displays the top five IP addresses from which the most attacks are launched in a bar chart. The x-axis indicates the numbers of requests. The y-axis indicates the IP addresses.
   - Distribution of Attack Types (Display TOP 5)

     Displays the distribution of the top five attack types and the number of attacks of each type in a bar chart.
   - Most Attacked Websites (Display TOP 5)

     Displays the top five attacked websites and the number of attacks on each website in a bar chart.

8.2.2. View access information

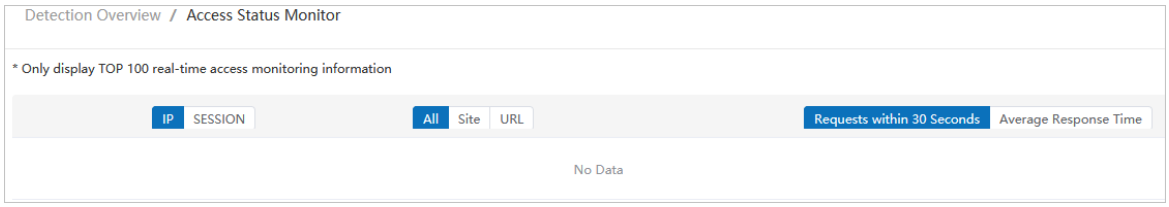
This topic describes how to view access information about web services.

Context

Web Application Firewall (WAF) monitors the access of web services. This way, security administrators can analyze the service access information to detect vulnerabilities and improve security of the services.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Statistic > Access Status Monitor**.
4. Filter access records to view details.



8.3. Protection logs

8.3.1. View attack detection logs

This topic describes how to view attack detection logs.

Context

These logs allow you to analyze attacks on your web services. You can update the protection policies and custom rules, and fix the web service vulnerabilities based on the analysis results.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Detection Logs > Attack Detection Logs**.
4. Click **Filter**, specify filter conditions, and then click **OK**.

> **Note** If you specify multiple conditions, they are evaluated by using a logical AND. The system returns the required logs only when all the conditions are met.

5. View the attack detection logs.

8.3.2. View HTTP flood protection logs

This topic describes how to view HTTP flood protection logs.

Context

These logs allow you to analyze HTTP flood attacks on your web services. In addition, you can update the HTTP flood protection rules and HTTP flood whitelist, and fix the web service vulnerabilities based on the analysis results.

Procedure

1. Log on to Apsara Stack Security Center.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Detection Logs > HTTP Flood Detection Logs**.
4. Click **Filter**, specify filter conditions, and then click **OK**.

   > **Note** If you specify multiple conditions, they are evaluated by using a logical AND. The system returns the required logs only when all the conditions are met.

5. View the HTTP flood detection logs.

   The blocked HTTP flood attacks, related rules, and attack time are displayed.

8.3.3. View bot verification logs

This topic describes how to view bot verification logs.

Context

Bot verification logs can be used to analyze bot attacks on web services. You can update bot management rules based on the analysis results to improve the security of your web services.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the top navigation bar, move the pointer over **Security** and choose **Application Security > Web Application Firewall**.
3. On the **Web Application Firewall** page, select a **region** and click **Access with Authorized Role**.
4. In the left-side navigation pane, choose **Web Application Protection > Detection Logs > Bot Verification Logs** .
5. On the **Bot Verification Logs** page, click **Verification Result Logs** or **Verification Record Logs**.

   The log list displays the log content, verification result, rule name, source IP address, and time when the bot attack occurred in each log.

Related information

- Configure the bot management feature

8.3.4. View system operation logs

This topic describes how to view system operation logs.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Detection Logs > System operation log**.
4. View the system operation logs.

The usernames, content, IP addresses, and creation time are displayed.

8.3.5. View access logs

This topic describes how to view access logs.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Detection Logs > Access Log**.
4. Click **Filter**, specify filter conditions, and then click **OK**.

   > **Note** If you specify multiple conditions, they are evaluated by using a logical AND. The system returns the required logs only when all the conditions are met.

5. View the access logs.

   The requested addresses, destination IP addresses, source IP addresses, methods, response status codes, and time are displayed.

8.4. Protection configuration

8.4.1. Configure protection policies

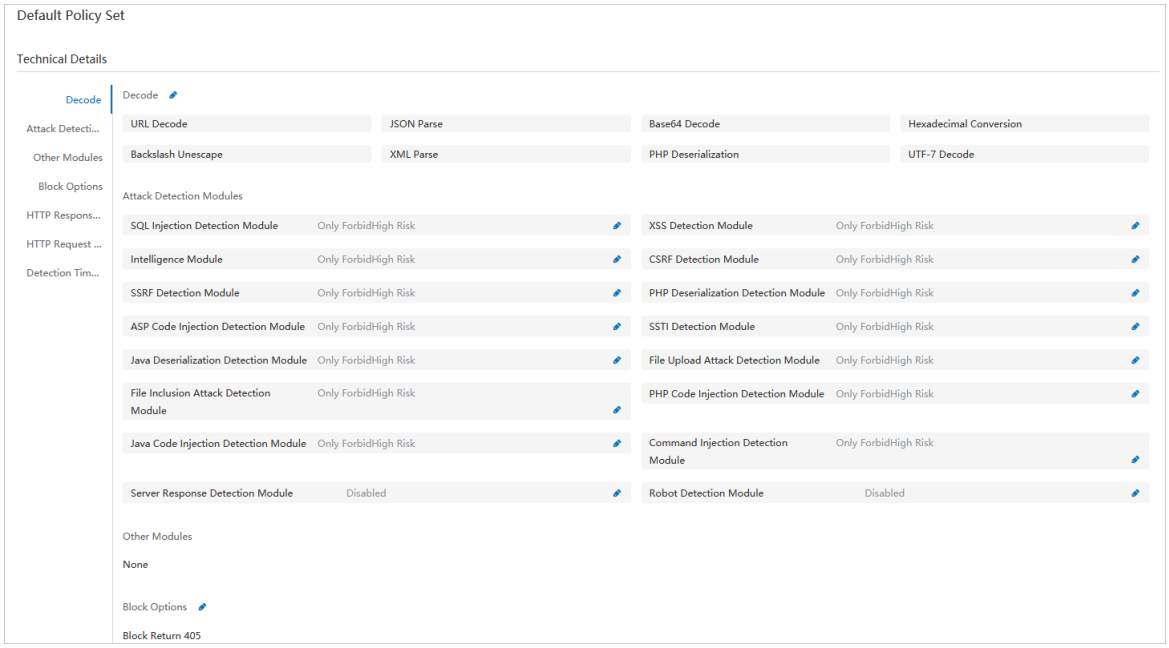
This topic describes how to configure Web Application Firewall (WAF) protection policies.

Context

WAF provides a default protection policy. You can also customize protection policies to suit your business requirements.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Protection Configuration > Website Protection Policies**.
4. Click **Add a protection policy**. In the panel that appears, configure **Policy name** and click **Confirm**.
5. In the **Actions** column of the new protection policy, click the icon to view details.



Parameter	Description
Decode	Select algorithms that you want to use to decode the requests.
Attack Detection Modules	Specify the types of attacks that you want to detect and the risk levels of attacks that you want to block.
Block Options	Specify the HTTP status code and image that you want WAF to return when it blocks an attack.
HTTP Response Detection	Configure **Enable HTTP response processing** and **Response Detection Max Body Size**.
HTTP Request Detection	Configure **Response Detection Max Body Size**.
Detection Timeout	Configure **Enable Detection Timeout** and **Timeout Threshold**.

For example, perform the following steps to configure modules in the **Attack Detection Modules** section:

i. Move the pointer over a specific module in the **Attack Detection Modules** section. In this example, move the pointer over **SQL Injection Detection Module** and click the **modify** icon.

ii. In the **SQL Injection Detection Module** panel, configure the following parameters.

Parameter	Description
Enabled	Specify whether to enable the detection module.
Blocking Threshold	Valid values: **NotForbid**, **Only ForbidHigh Risk**, **ForbidMedium or High Risk**, and **Forbid All**.
Record Threshold	Valid values: **Notrecord**, **Only recordHigh Risk**, **recordMedium or High Risk**, and **record All**.
Detect Non-Injected SQL	Specify whether to enable detection for NoSQL injection vulnerabilities.

iii. Click **OK**.

6. Manage protection policies.

   To delete a protection policy, select the protection policy. Then, in the upper-right corner, choose **More > Delete Selected Protection Policies**. In the message that appears, click **OK**.

   > **Note** You cannot delete the default protection policy.

8.4.2. Create a custom rule

This topic describes how to create a custom rule for Web Application Firewall (WAF).

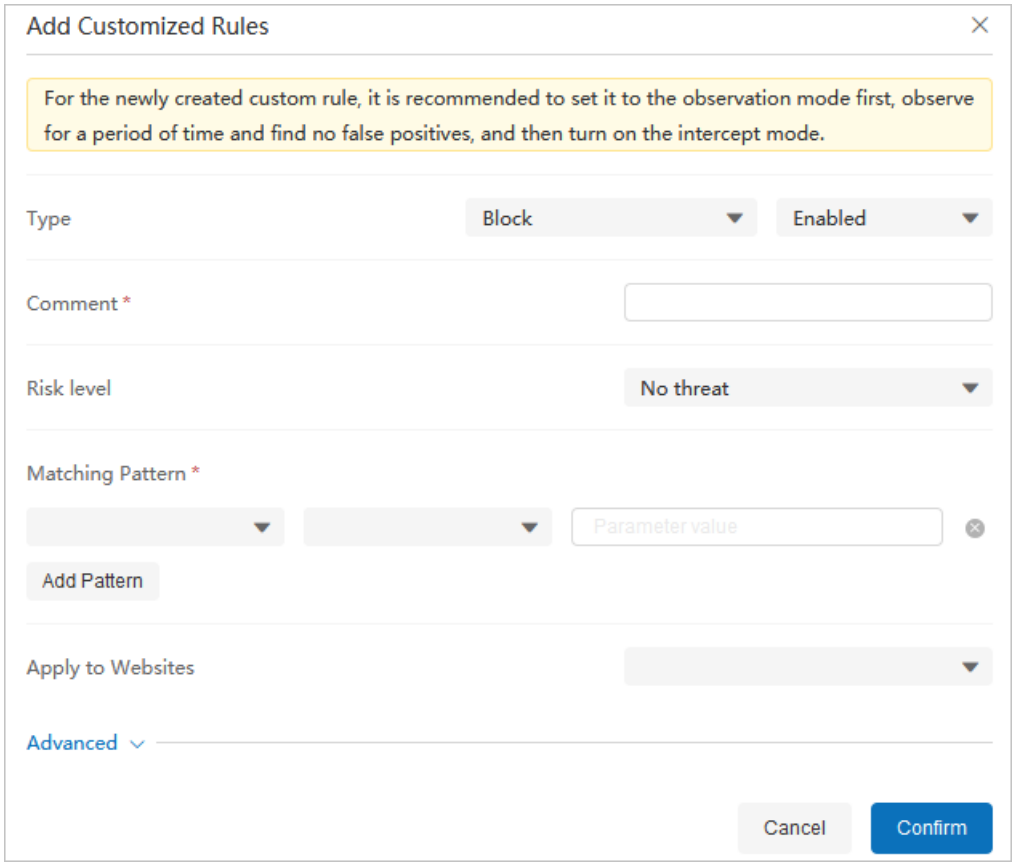
Context

You can create custom rules to meet different requirements for intrusion detection. You can create, edit, or delete custom rules as an administrator. You can use custom rules to filter out requests that meet specific conditions.

Multiple custom rules are evaluated by using a logical **OR**. If two custom rules use the same conditions but trigger different actions such as blocking traffic or allowing traffic, WAF runs the first rule.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation tree of the **WAF** page, choose **Protection Configuration > Customized Rules**.
4. In the upper-right corner, click **Add Rule**. In the **Add Customized Rules** panel, configure the parameters.



Parameters used to create a custom rule

Parameter	Description
Type	The operating mode of the rule. Valid values: **Block**, **Allow**, **Monitor**, and **Detection module control**. ○ **Block**: If an HTTP request meets the conditions of the rule, the HTTP request is blocked. ○ **Allow**: If an HTTP request meets the conditions of the rule, the HTTP request is allowed. ○ **Monitor**: If an HTTP request meets the conditions of the rule, the HTTP request is recorded and allowed. ○ **Detection module control**
Comment	The remarks about the rule. We recommend that you enter the purpose of the rule.
Risk level	The risk level. Valid values: **No threat**, **Low Risk**, **Medium Risk**, and **High Risk**.
Matching Pattern	The conditions that trigger the rule. Click **Add Pattern** to specify more than one condition. Multiple conditions are evaluated by using a logical **AND**. The custom rule takes effect only when all conditions are met.

Parameter	Description
Apply to Websites	The websites that you want the rule to protect.
Log Recording Option	Specifies whether to record a log when the rule is triggered. The default value is Enable Log Recording. After Log Recording Option is set to Enable Log Recording, all interception events are recorded in the intrusion detection logs.
Attack Type	The type of attack that you want the rule to block.
Expiration Time	The time at which the rule expires.

5. Click **Confirm**.
6. Manage custom rules.
   - Edit a rule.

     To edit a rule, click the icon in the **Actions** column.
   - Enable a rule.

     To enable a rule that is disabled, select the rule and choose **More** > **Enable Selected Rules**.
   - Disable a rule.

     To disable a rule that is enabled, select the rule and choose **More** > **Disable Selected Rules**.
   - Export a rule.

     To export a rule, select the rule and choose **More** > **Export Selected Rules**.
   - Delete a rule.

     To delete a rule that you no longer need, select the rule and choose **More** > **Delete Selected Rules**.

8.4.3. Configure an HTTP flood protection rule

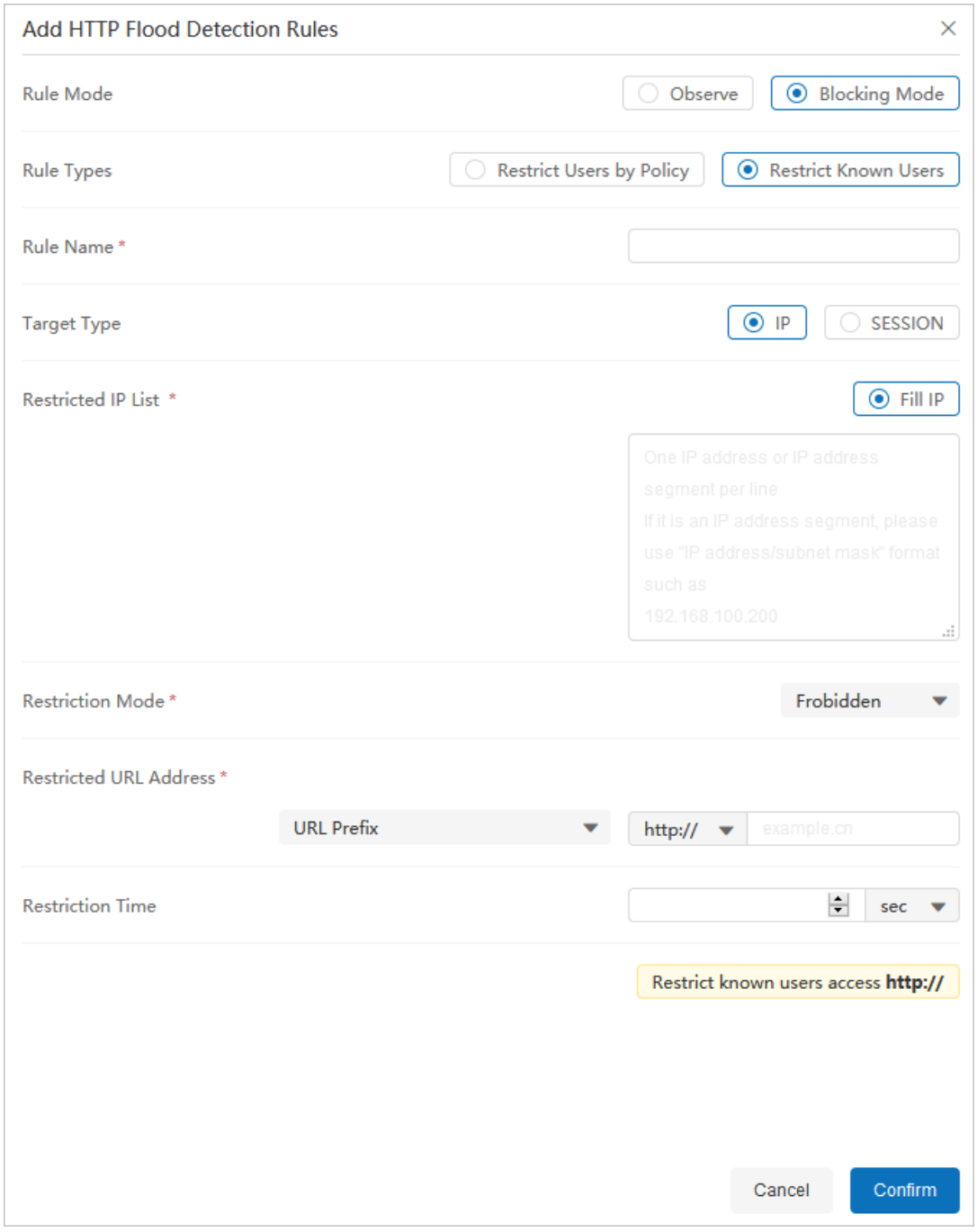
This topic describes how to configure an HTTP flood protection rule.

Context

An HTTP flood attack is a type of DDoS attack that targets the application layer. Attackers use proxy servers or zombies to overwhelm targeted web servers by sending a large number of HTTP requests.

Create an HTTP flood protection rule

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Protection Configuration** > **HTTP Flood Detection**.
4. Click **Add Rule**. The **Add HTTP Flood Detection Rules** panel appears.
5. Configure parameters and click **Confirm**.



Parameter	Description
Rule Mode	The action on requests after the HTTP flood protection rule is triggered. Valid values: **Blocking Mode** and **Observe**. ○ Blocking Mode: limits the requests that trigger the HTTP flood protection rule. ○ Observe: records the requests that trigger the HTTP flood protection rule, but does not limit the requests.

Parameter	Description
Rule Types	The type of the HTTP flood protection rule. Valid values: **Restrict Users by Policy** and **Restrict Known Users**. The difference between the two types is determined by whether requests of users are initiated from a specific IP address or in a specific session. ○ **Restrict Users by Policy**: limits requests that meet all the configuration items of the HTTP flood protection rule. Configuration items include **Restriction Trigger Threshold**, **Restricted URL Address**, **Restriction Mode**, **Restriction Time**, and **Statistical Range of Visits** in the Advanced section. ○ **Restrict Known Users**: limits requests that are initiated from specific IP addresses or in specific sessions based on the HTTP flood protection rule. To achieve this purpose, you must configure the IP address or session list and the limit mode. After you configure the list, the HTTP flood protection rule limits requests based on the list.
Rule Name	The name of the HTTP flood protection rule.
Target Type	The type of source for requests that are limited. Valid values: **IP** and **SESSION**. **Note** If you set **Target Type** to **SESSION**, you can apply the HTTP protection rule only to a website whose **User Identification** is set to **WAF User System**. For more information, see Add an Internet website for protection.
Restriction Trigger Threshold	If you set **Rule Types** to **Restrict Users by Policy**, you must configure the triggering conditions for the HTTP flood protection rule.
Restricted URL Address	If you set **Rule Types** to **Restrict Users by Policy**, you must specify the URL addresses that are protected based on the HTTP flood protection rule. ○ **URL Prefix** ○ **URL** ○ **Record all IP addresses**
Restricted IP List or **Restricted SESSION List**	If you set **Rule Types** to **Restrict Known Users**, you must enter the IP addresses or sessions from which you want to limit requests based on the setting of **Target Type**. You can enter only one IP address or session in each line.

Parameter	Description
Restricted URL Address	If you set **Rule Types** to **Restrict Known Users**, you must specify the URL addresses that are protected based on the HTTP flood protection rule. ○ **URL Prefix** ○ **URL** ○ **Restrict user access to all addresses**
Restriction Mode	The mode in which the HTTP flood protection rule limits requests. Valid values: ○ **Forbidden**: The rule blocks specific sources from accessing the specified URL address. ○ **Frequency control**: The rule limits the frequency at which specific sources access the specified URL address.
Restriction Time	The time at which the action specified in the HTTP flood protection rule takes effect.
Statistical Range of Visits	If you set **Rule Type** to **Restrict Users by Policy**, you can specify the range of data records to limit requests in the Advanced section. ○ Statistics Full Access Data: If you select this option, the frequency of requests is limited when the requests are forwarded to WAF and meet the HTTP flood protection rule, regardless of which data records the requests access. This decreases system performance. ○ Statistics TOP Access Data: If you select this option, the frequency of requests is limited when the requests meet the preceding conditions and access the top 100 data records. This option helps minimize the decrease in system performance. You can select this option when the number of accessed data records is larger than 100. Note that the top 100 data records are measured based on real-time monitoring.

Manage HTTP flood protection rules

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Protection Configuration > HTTP Flood Detection**.
4. In the rule list, manage existing HTTP flood protection rules. Modification is allowed.
   - Search for a rule.

     Click **Filter**. In the **Filter Item** panel, specify filter conditions.
   - Enable a rule.

     Select a rule that is disabled and choose **More > Enable Selected Rules**.

- Disable a rule.

  Select a rule that is enabled and choose **More > Disable Selected Rules**.

- Delete a rule.

  Select a rule and choose **More > Delete Selected Rules**.

8.4.4. Configure the HTTP flood whitelist

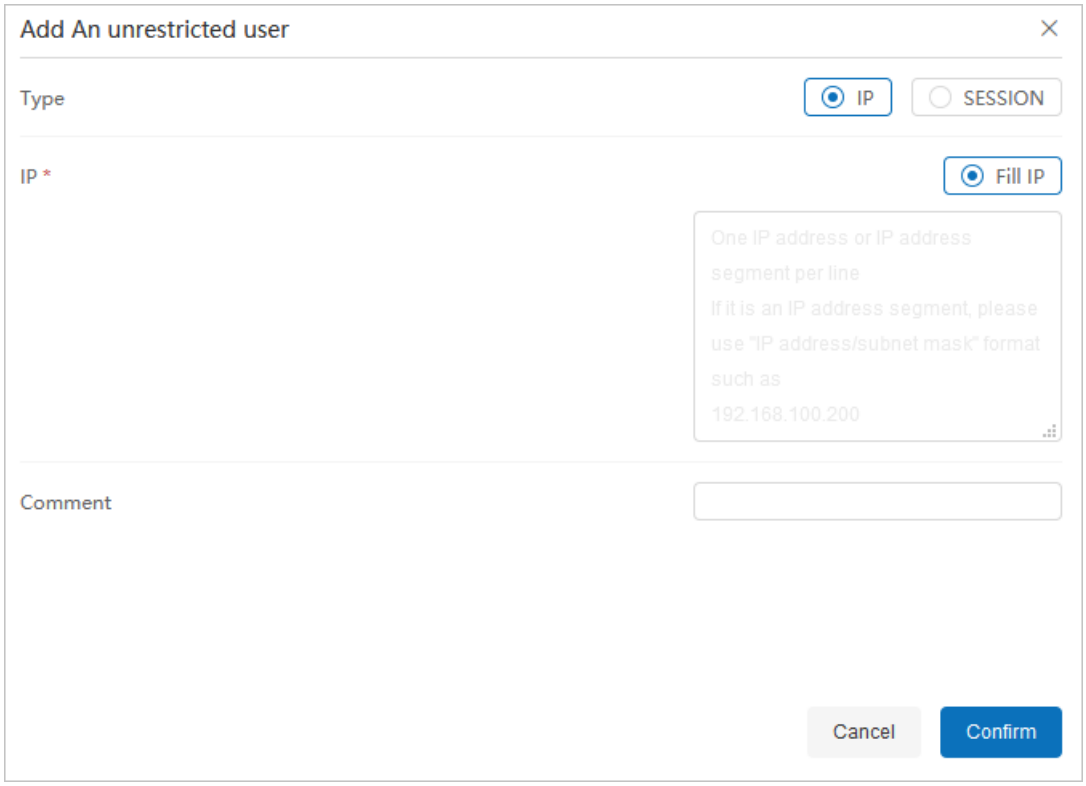
This topic describes how to configure the HTTP flood whitelist.

Context

If a request source is trusted, you can add this request source to the HTTP flood whitelist to allow all requests from this source.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation tree of the **WAF** page, choose **Protection Configuration > HTTP Flood Detection**.
4. On the **HTTP Flood Detection Whitelist** tab, click **Add Whitelist Item**, add a trusted request source, and then click **Confirm**.



Parameter	Description

Parameter	Description
Type	Select the type of the request source. Valid values: **IP** and **SESSION**.
IP or **SESSION**	Specify the IP addresses or sessions based on the setting of **Type**. You can enter only one IP address or session in each line.
Comment	Enter remarks for the request source.

5. Manage request sources in the whitelist.
   - Search for a request source in the whitelist.

     Click **Filter**. In the panel that appears, specify a filter condition or click **Add Filter Item** to specify more filter conditions.
   - Remove a request source from the whitelist.

     Select the request source and choose **More > Delete Selected Items**.

8.4.5. Configure the bot management feature

This topic describes how to configure the bot management feature to block bot traffic.

Context

The feature identifies bot traffic and web code to detect and block malicious network behaviors such as crawlers, spam user registrations, brute-force attacks, and promotion abuses.

Create a bot management rule

1. Log on to Apsara Stack Security Center.
2. In the top navigation bar, move the pointer over **Security** and choose **Application Security > Web Application Firewall**.
3. On the **Web Application Firewall** page, select a **region** and click **Access with Authorized Role**.
4. In the left-side navigation pane, choose **Web Application Protection > Protection Configuration > Bot Management**.
5. On the **Bot Management** page, click **Add BOT Protection Strategy**.
6. In the **Add Bot Management** panel, configure the parameters and click **Confirm**.

Parameter	Description
BOT Strategy Status	The status of the bot management rule. Valid values: ○ Enable: enables the rule. ○ Disable: disables the rule.
Name	The name of the bot management rule.

Parameter	Description
Configure Site	The website to which you want to apply the bot management rule. You can select websites from **Internet Websites** or **VPC Websites**. You can select multiple websites. **Notice** If you want to apply the bot management rule to multiple addresses, click **Add Effective Address** to add the addresses.
Policy Effective Address	The address to which you want to apply the bot management rule. The following operators are supported: **Prefix Match**, **Regular Expression Match**, and **Exact Match**.
Port Settings	The port to which you want to apply the bot management rule. **Notice** Ports of the selected websites are automatically added. If you want to apply the bot management rule to other ports, click **Add a group of ports** to add the ports.
Ignore Search Engines	The search engine whose traffic you want the bot management rule to bypass.
Man-machine Verification	Specifies whether to enable or disable the CAPTCHA verification feature.
Matching Features	The condition that is used to trigger the CAPTCHA verification feature.
Mode	The CAPTCHA verification mode. Valid values: ◦ Browser ◦ Verification Code
Validity Period	The validity period during which you are not required to perform the verification again after the CAPTCHA verification is passed.

Parameter	Description
Logging	Specifies whether to record CAPTCHA verification logs. Valid values: ○ Record Verification Logs ○ Not Record Verification Logs **Notice** If you select **Record Verification Logs**, you can choose **Detection Logs > Bot Verification Logs** to view the details of the recorded logs.

Enable, disable, or delete a bot management rule

1. Log on to Apsara Stack Security Center.
2. In the top navigation bar, move the pointer over **Security** and choose **Application Security > Web Application Firewall**.
3. On the **Web Application Firewall** page, select a **region** and click **Access with Authorized Role**.
4. In the left-side navigation pane, choose **Web Application Protection > Protection Configuration > Bot Management**.
5. On the **Bot Management** page, select the rule that you want to enable, disable, or delete.

   You can also click **Edit** in the **Actions** column to modify the bot management rule.

8.4.6. Manage SSL certificates

This topic describes how to upload or delete SSL certificates.

Context

After you upload an SSL certificate on the **Certificate Management** page, you can select this certificate when you add an HTTPS website for protection on the **Protection Site Management** page.

Note When you add an HTTPS website for protection on the **Protection Site Management** page, you must select the SSL certificate that corresponds to the domain of the HTTPS website.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Protection Configuration > Certificate Management**.
4. Upload a new certificate.
   i. Click **Upload SSL Certificate**.

ii. In the **Name** field, enter a **name for the new certificate**.

We recommend that you enter the domain name for easier management.

> **Note** If your Certificate Authority (CA) certificate and private key are in the same file, select **Include private key in certificate file**.

iii. In the **File** section, upload the CA certificate file and private key file.

iv. Configure **Certificate Password**.

v. Click **Confirm**.

5. (Optional)Delete the uploaded SSL certificate.

You can delete expired SSL certificates.

i. In the SSL certificate list, select the certificate that you want to delete.

ii. Choose **More > Delete selected SSL certificate**.

iii. In the message that appears, click **OK**.

8.4.7. Add Internet websites for protection

This topic describes how to add Internet websites to Web Application Firewall (WAF).

Context

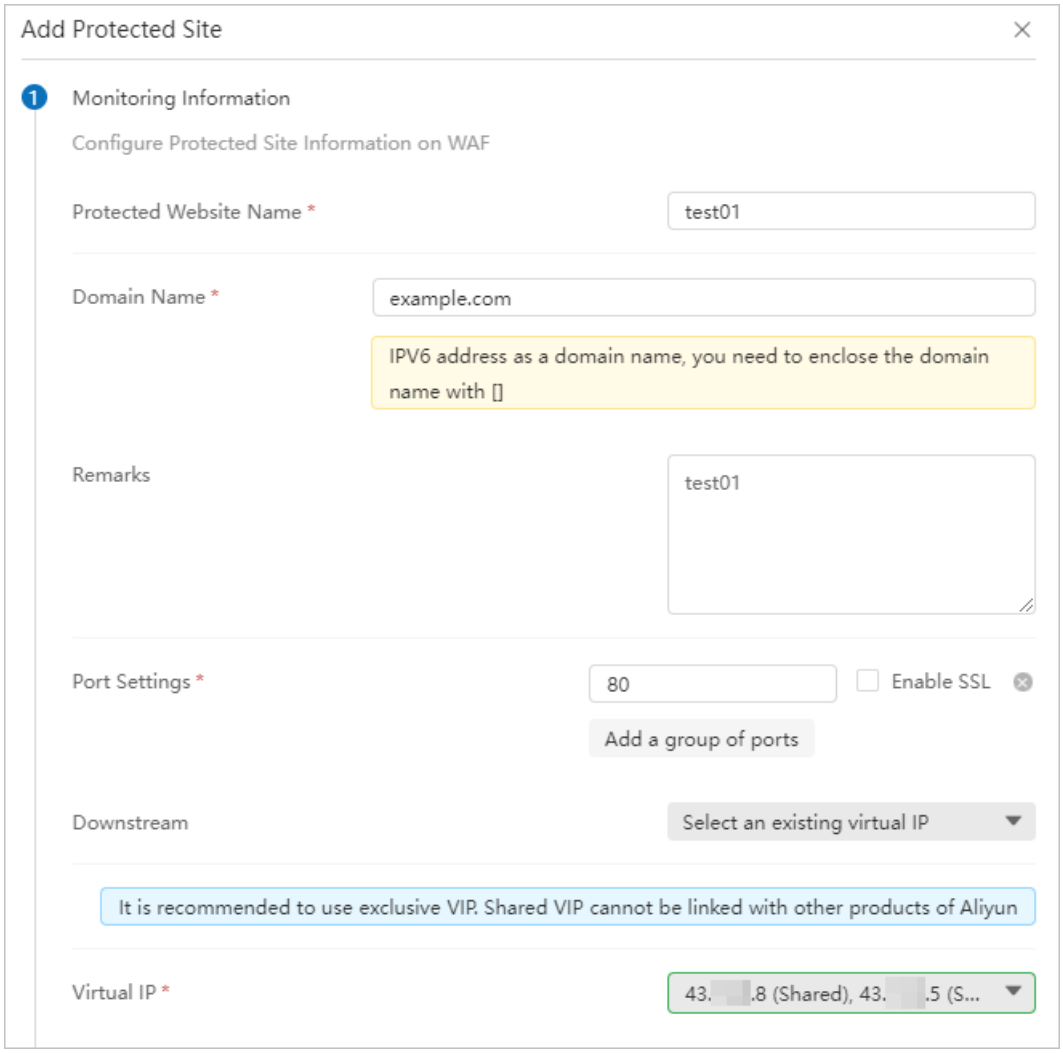
WAF can protect the following types of websites:

- Internet websites.
- Virtual Private Cloud (VPC) websites. For more information about how to add VPC websites to WAF, see Add a VPC website for protection.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane,, choose **Protection Configuration > Protection Site Management**.
4. On the **Internet Websites** tab, click **Add a site**.
5. In the Monitoring Information step, configure parameters and click **Next**.

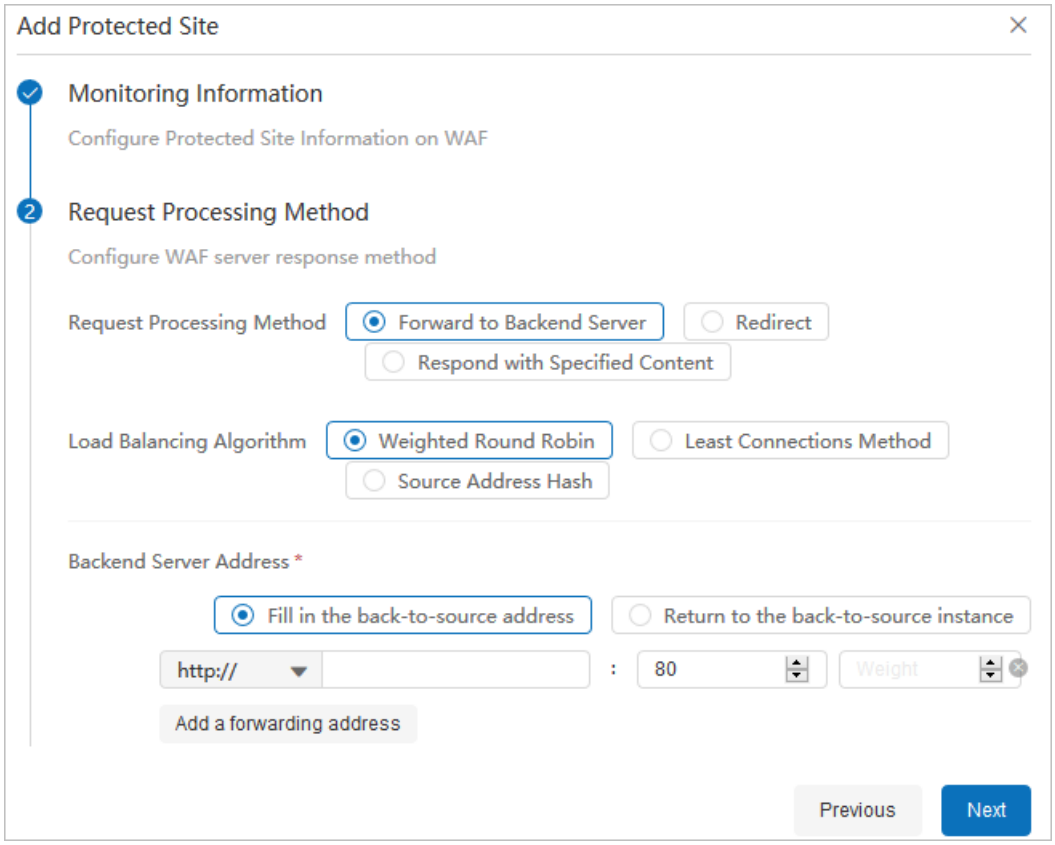
Specify the Internet website that you want WAF to protect. WAF can protect both HTTP and HTTPS websites.



Parameter	Description
Protected Website Name	The name of the website that you want WAF to protect.
Domain Name	The domain name of the website. ○ You can use an asterisk (*) as a wildcard. ○ If you specify multiple domain names, separate them with commas (,).
Port Settings	The port that WAF listens on. ○ If the website supports HTTPS requests, select **Enable SSL** and upload an HTTPS certificate. ○ If the website can be accessed over multiple ports, click **Add a group of ports** to add the required ports.

Parameter	Description
Cert Setting	The HTTPS certificate of the website. Valid values: *Upload a New Certificate* and *Choose an Existing Certificate*. ○ *Upload a New Certificate*: If the HTTPS certificate of the website has not been uploaded to WAF, select this option. By default, the HTTPS certificate and private key are separately uploaded. If you select **Include private key in certificate file**, upload only one file that contains both the HTTPS certificate and private key. ○ *Choose an Existing Certificate*: If the HTTPS certificate of the website has been uploaded to WAF, select this option. Then, select the required HTTPS certificate from the drop-down list. **Note** This parameter is required only if you select **Enable SSL** next to the **listening port** field.
Name	The name of the HTTPS certificate. **Note** This parameter is required only if you select **Enable SSL** next to the **listening port** field and select Upload a New Certificate.
File	The HTTPS certificate and private key. By default, the HTTPS certificate and private key are separately uploaded. If you select **Include private key in certificate file** next to **Name**, upload only one file that contains both the HTTPS certificate and private key. **Note** This parameter is required only if you select **Enable SSL** next to the **listening port** field and select Upload a New Certificate.
Virtual IP	The IP address type and virtual IP address. **Note** You can select an IPv6 address as the virtual IP address for WAF. By default, WAF provides 10 virtual IP addresses. You can add more virtual IP addresses based on your business requirements. **Note** A virtual IP address is available only for the department to which the creator of the virtual IP address belongs.

6. In the Request Processing Method step, configure parameters and click **Next**.



Response mode	Parameter	Description
Forward to Backend Server	**Load Balancing Algorithm**	The algorithm for load balancing. Valid values: **Weighted Round Robin**, **Source Address Hash**, and **Least Connections Method**.
	Backend Server Address	The address of the origin server to which WAF forwards inbound traffic. Valid values: **Fill in the back-to-source address** and **Return to the back-to-source instance**. ◦ **Fill in the back-to-source address**: Enter the address of the origin server. If you enter multiple addresses, load balancing is performed based on the specified **load balancing algorithm**. ◦ **Return to the back-to-source instance**: Enter the address of a specific ECS or SLB instance. If you enter multiple addresses, load balancing is performed based on the specified **load balancing algorithm**.
	X-Forwarded-For	The pass-through mode of the actual source IP address. The X-Forwarded-For (XFF) header is used to identify the actual source IP address of an HTTP client. The header is used for traffic forwarding services, such as HTTP proxy and load balancing.

Response mode	Parameter	Description
Redirect	**Response Status Code**	The HTTP status code that WAF returns when it redirects inbound traffic to a specified address. Valid values: **301**, **302**, **307**, and **308**. ○ **301**: The requested page is permanently moved to another URL. ○ **302**: The requested page is temporarily moved to another URL. The requester must continue to use the original URL for future requests. ○ **307**: The requested page is temporarily moved to another URL. The requester must continue to use the original URL for future requests.
	Redirect address	The destination URL for redirection.
Respond with Specified Content	**Response Status Code**	The HTTP status code that WAF returns when it returns specified content. Valid value: **200**, **400**, **401**, **402**, **404**, **405**, **500**, **503**, and **504**.
	Response	The content to return. For example, you can upload an image for the **Response** parameter. If a user visits the website, WAF returns the uploaded image.

7. In the Protection Policy step, configure parameters and click Next. Then, go to the **Finish** step.

> **Note** You can configure a protection policy only if you set **Request Processing Method** to **Forward to Backend Server**.

Parameter	Description
Protection Policy	Select a WAF protection policy. For more information, see Configure protection policies.
User Identification	Specify whether to enable the user identification feature. > **Note** If you enabled HTTP flood protection for the protected website and set **Target Type** to **SESSION** when you configured the HTTP flood protection rule, you must set **User Identification** to **WAF User System**.

8.4.8. Add VPC websites for protection

This topic describes how to add virtual private cloud (VPC) websites to Web Application Firewall (WAF) for protection.

Context

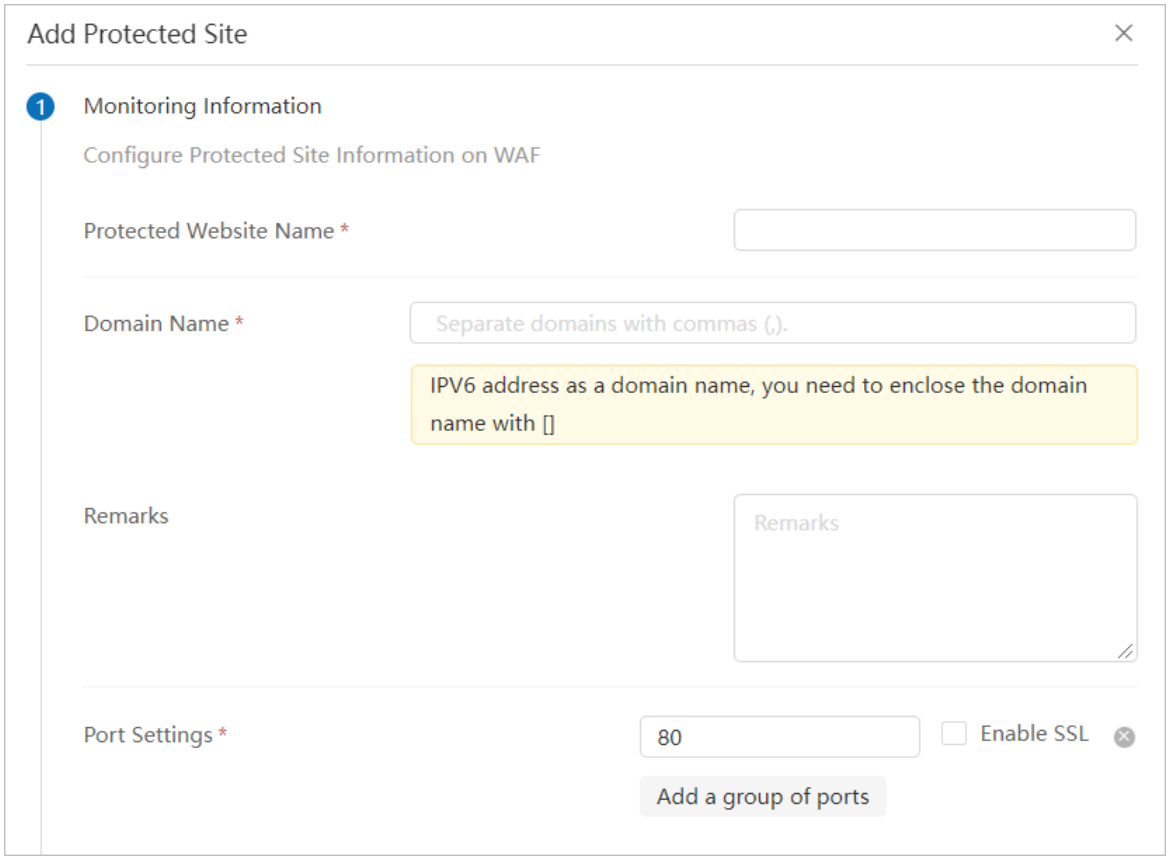
WAF can protect the following types of websites:

- Internet websites. For more information about how to add an Internet website for protection, see Add an Internet website for protection.
- VPC websites.

Procedure

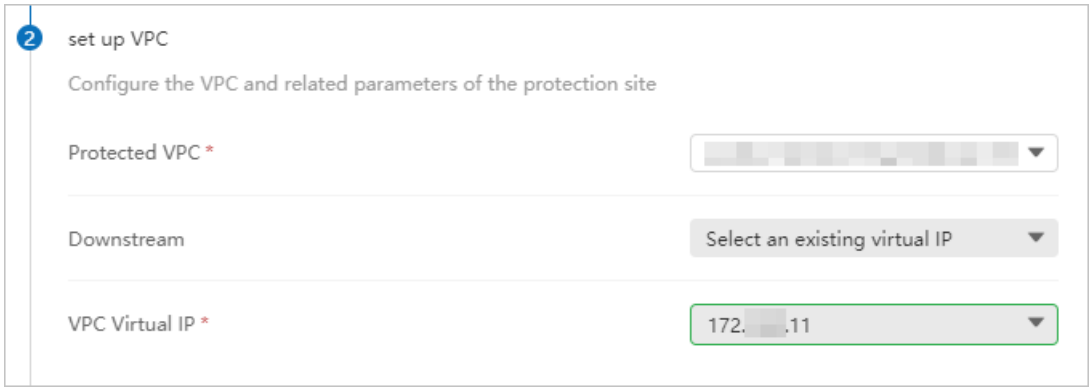
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Application Security > Web Application Firewall**.
3. In the left-side navigation pane, choose **Protection Configuration > Protection Site Management**.
4. Click the **VPC Websites** tab. Then, click **Add a site**. The **Add Protected Site** panel appears.
5. In the Monitoring Information step, configure parameters and click **Next**.

   Specify the VPC website that you want WAF to protect. WAF can protect both HTTP and HTTPS websites.



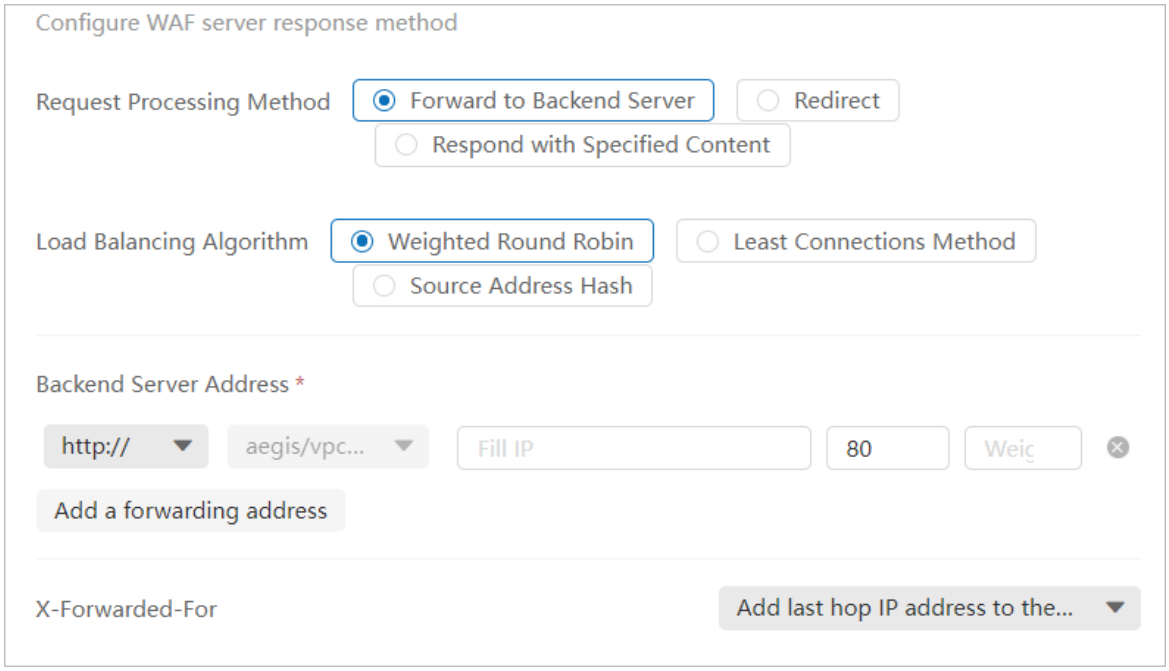
Parameter	Description
Protected Website Name	The name of the website that you want WAF to protect.
Domain Name	The domain name of the website. ○ You can use an asterisk (*) as a wildcard. ○ If you specify multiple domain names, separate them with commas (,).
Port Settings	The port that WAF listens on. ○ If the website supports HTTPS requests, select **Enable SSL** and upload an HTTPS certificate. ○ If the website can be accessed over multiple ports, click **Add a group of ports** to add the required ports.
Cert Setting	The HTTPS certificate of the website. Valid values: **Upload a New Certificate** and **Choose an Existing Certificate**. **Note** Specify this parameter only if you select **Enable SSL** next to **Port Settings**. ○ **Upload a New Certificate**: If the HTTPS certificate used by the website is not uploaded to WAF, select this option. By default, the HTTPS certificate and private key are separately uploaded. If you select **Include private key in certificate file**, upload only a file that contains both the HTTPS certificate and private key. ○ **Choose an Existing Certificate**: If the HTTPS certificate used by the website is uploaded to WAF, select this option. Then, select the HTTPS certificate from the drop-down list.
Name	The name of the HTTPS certificate. **Note** Specify this parameter only if you select **Enable SSL** next to **Port Settings** and set Cert Setting to Upload a New Certificate.
File	The HTTPS certificate and private key to upload. By default, the HTTPS certificate and private key are separately uploaded. If you select **Include private key in certificate file** next to **Name**, upload only a file that contains both the HTTPS certificate and private key. **Note** Specify this parameter only if you select **Enable SSL** next to **Port Settings** and set Cert Setting to Upload a New Certificate.

6. In the set up VPC step, configure parameters and click **Next**.



Parameter	Description
Protected VPC	The VPC to which the website belongs.
Virtual Switch	The vSwitch associated with the specified VPC.
Create Virtual IP Method	The method to create a virtual IP address. Valid values: **Select an existing virtual IP** and **Create virtual IP**.
VPC Virtual IP	○ If you set **Create Virtual IP Method** to **Select an existing virtual IP**, select an existing virtual IP address from the **VPC Virtual IP** drop-down list. ○ If you set **Create Virtual IP Method** to **Create virtual IP**, click **Click to Create Vip** next to **VPC Virtual IP** to generate a virtual IP address.

7. In the Request Processing Method step, configure parameters and click **Next**.



Request processing method	Parameter	Description
Forward to Backend Server	**Load Balancing Algorithm**	The algorithm for load balancing. Valid values: **Weighted Round Robin**, **Source Address Hash**, and **Least Connections Method**.
	Backend Server Address	The address of the origin server to which WAF forwards inbound traffic. Valid values: **Fill in the back-to-source address** and **Return to the back-to-source instance**. ○ **Fill in the back-to-source address**: Enter the address of the origin server. If you enter multiple addresses, load balancing is performed based on the specified **load balancing algorithm**. ○ **Return to the back-to-source instance**: Enter the address of a specific Elastic Compute Service (ECS) or Server Load Balancer (SLB) instance. If you enter multiple addresses, load balancing is performed based on the specified **load balancing algorithm**.
	X-Forwarded-For	The pass-through mode of the actual source IP address. The X-Forwarded-For (XFF) header is used to identify the actual source IP address of an HTTP client. The header is used for traffic forwarding services, such as HTTP proxy and load balancing.
Redirect	**Response Status Code**	The HTTP status code that WAF returns when it redirects inbound traffic to a specified address. Valid values: **301**, **302**, **307**, and **308**. ○ **301**: The requested page is permanently moved to another URL. ○ **302**: The requested page is temporarily moved to another URL. The requester must continue to use the original URL for future requests. ○ **307**: The requested page is temporarily moved to another URL. The requester must continue to use the original URL for future requests.
	Redirect address	The destination URL for redirection.
Respond with	**Response Status Code**	The HTTP status code that WAF returns when it returns specified content. Valid value: **200**, **400**, **401**, **402**, **404**, **405**, **500**, **503**, and **504**.

Request processing method	Parameter	Description
Respond with Specified Content	Response	The content to return. For example, you can upload an image for the **Response with Specified Content** parameter. If a user visits the website, WAF returns the uploaded image.

8. In the Protection Policy step, configure parameters and click Next. Then, go to the **Finish** step.

Parameter	Description
Protection Policy	Select a WAF protection policy. For more information, see Configure protection policies.
User Identification	Specify whether to enable the user identification feature.

8.4.9. Verify the configurations of a website on your on-premises server

This topic describes how to verify the configurations of a website on your on-premises server.

Context

Before you use Web Application Firewall (WAF) to scrub traffic destined for a website, we recommend that you verify the configurations of the website on your on-premises server. After you add the virtual IP address and the domain of a website to the hosts file on your on-premises server, the request to access the domain from a local browser passes through WAF first.

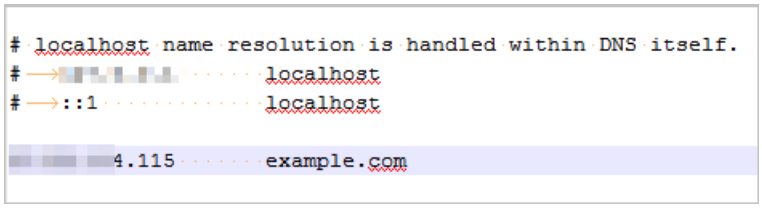
Procedure

1. Log on to Apsara Stack Security Center.
2. Add the virtual IP address and domain name to the *hosts* file on your on-premises server.

   If your computer runs Windows 7, the hosts file is stored in the following path: *C:\Windows\System32\drivers\etc\hosts*.

   i. Open the hosts file by using a text editor, such as Notepad.

ii. Add the following content to the end of the file: `<The virtual IP address that is assigned by WAF><Protected domain name>` .



> **Note** The IP address preceding the domain name is the virtual IP address that is assigned by WAF.

3. Ping the protected domain name from your on-premises server.

   The returned IP address must be the virtual IP address that is assigned by WAF in the hosts file. If the returned IP address is still the IP address of the origin server, refresh the local Domain Name System (DNS) cache.

4. Enter the domain name in the address bar of your browser and press Enter.

   If the access configurations on WAF are correct, you can visit the website.

5. Verify the protection capability of WAF.

   Simulate a web attack request and check whether WAF blocks the request.

   For example, add `/?alert(xss)` after the URL. If you try to visit `www.example.com/?alert(xss)` , WAF is expected to block the request.

8.4.10. Modify DNS resolution settings

This topic describes how to modify the Domain Name System (DNS) resolution settings to connect your website to Web Application Firewall (WAF).

Context

Before you can modify the DNS resolution settings, you must verify the settings on your computer and make sure that the settings are correct. Then, the traffic destined for your website can be redirected to WAF after you modify the settings.

The domain name of a protected website may not be resolved by a DNS provider. For example, a website may use a Server Load Balancer (SLB) instance to connect to the Internet. In this case, you can perform the following operation to protect the website by using WAF: Specify the virtual IP address that WAF assigns to your website as the back-to-origin IP address of the SLB instance.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **Protection Configuration > Protection Site Management**.
4. Find the website whose DNS resolution settings you want to modify and click the icon in the **Actions** column.

5. On the **Basic Information** tab, record the virtual IP address assigned to the website.
6. Log on to the console of the DNS provider and find the DNS resolution settings for the domain name of the website. Then, change the IP address in the A record to the virtual IP address assigned to the website.

> **Note** We recommend that you set the TTL to 600 seconds in DNS resolution settings. The larger the TTL is, the longer it takes to synchronize and update DNS records.

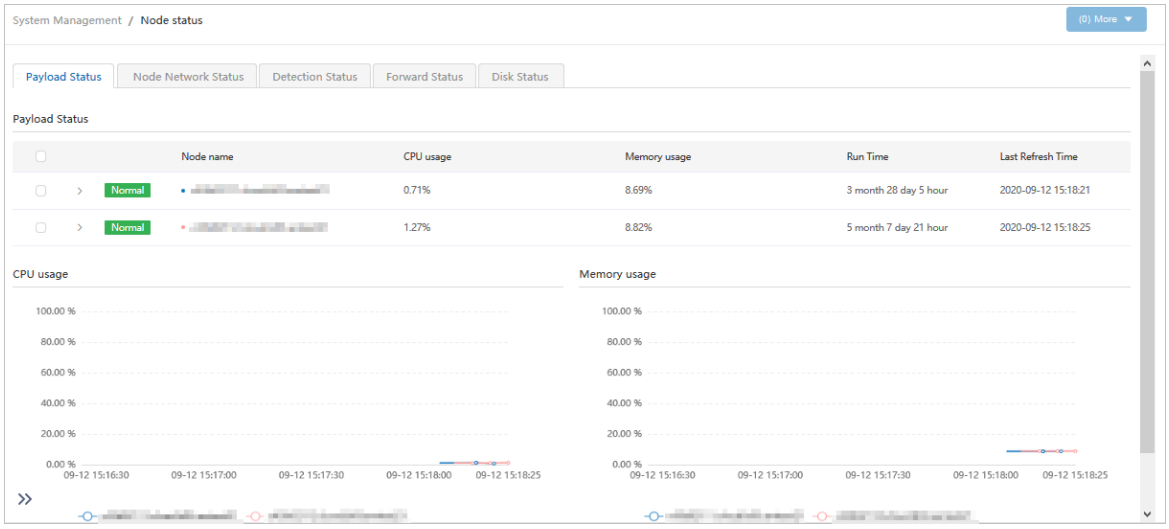
8.5. System management

8.5.1. View the load status of nodes

This topic describes how to view the load status of Web Application Firewall (WAF) nodes. The status information includes CPU utilization and memory usage. You can identify faults based on the status and check whether scale-out or scale-up is required.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation tree of the **WAF** page, choose **System Info > Node status**.
4. On the **Payload Status** tab, view the load status of WAF nodes.



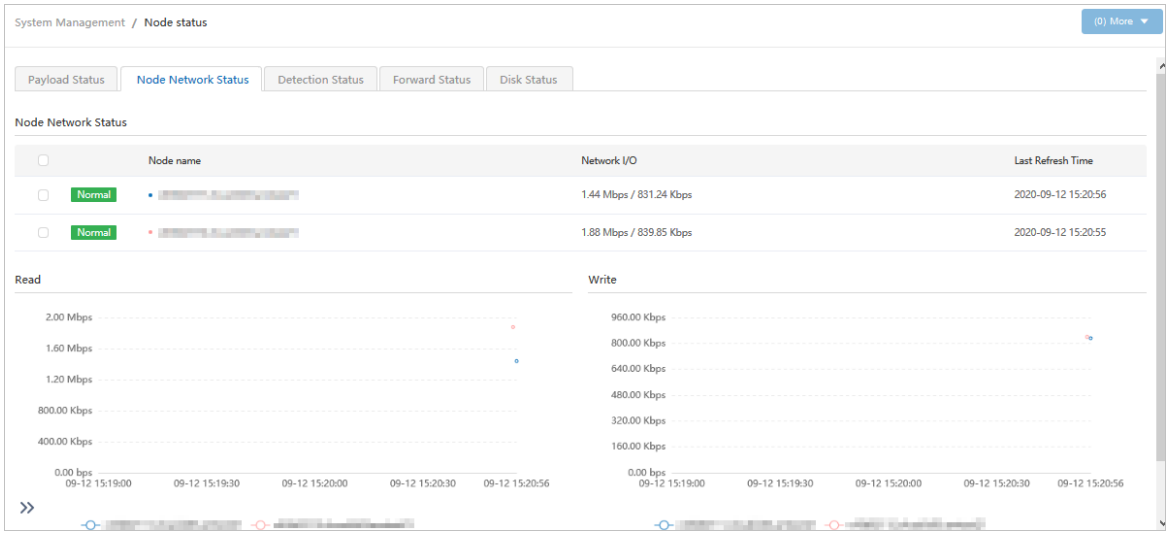
In the Payload Status section, you can view the CPU utilization and memory usage of WAF nodes. In the CPU usage and Memory usage sections, you can view the changes in CPU utilization and memory usage over a specific period of time.

8.5.2. View the network status of nodes

This topic describes how to view the network status of Web Application Firewall (WAF) nodes. The status information includes network I/O, traffic detection status, and traffic forwarding status.

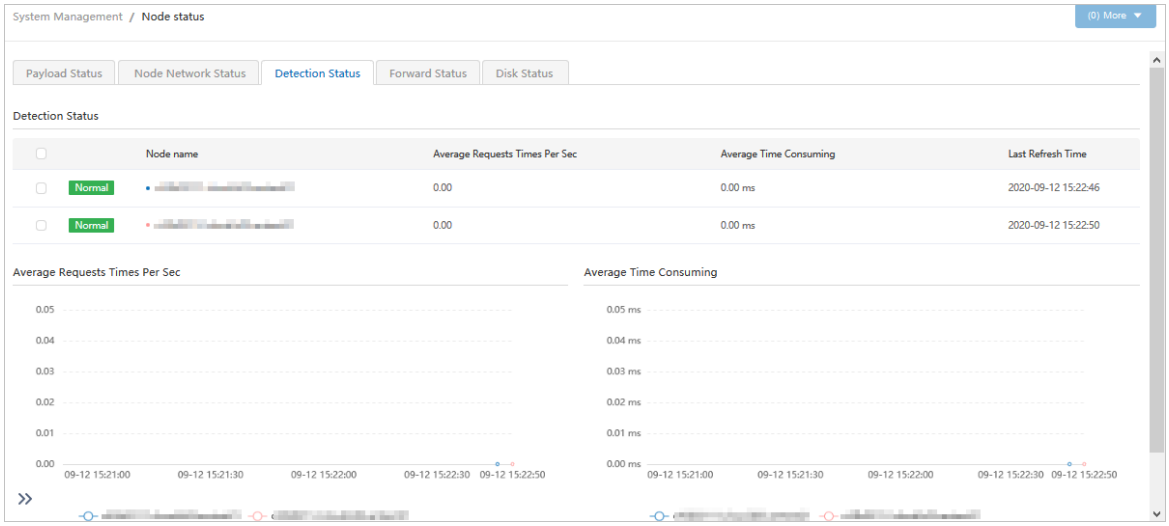
Node network status

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **System Info > Node status**.
4. On the **Node status** page, click the **Node Network Status** tab.
5. View the network I/O of WAF nodes.



Traffic detection status

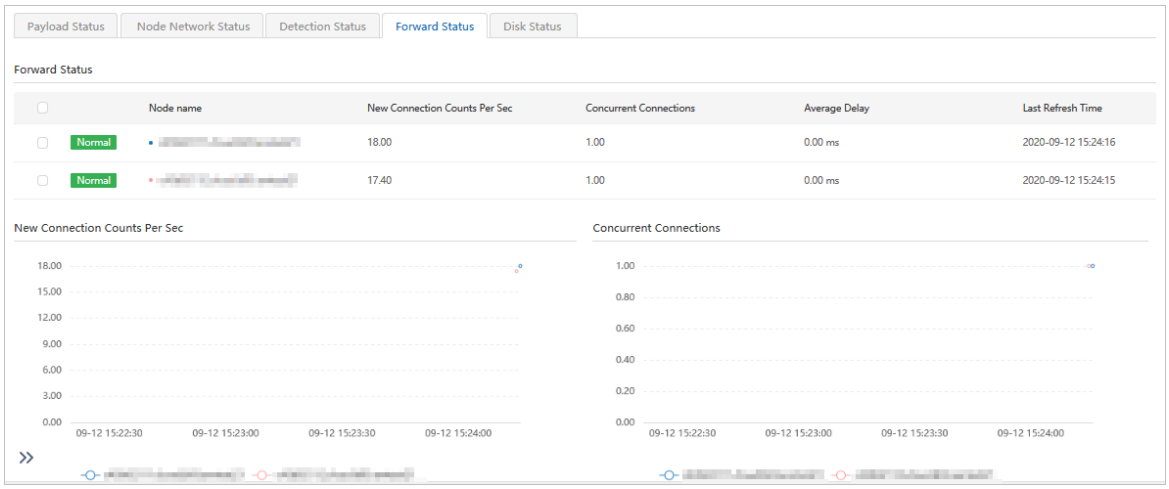
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **System Info > Node status**.
4. On the **Node Status** page, click the **Detection Status** tab.
5. View the traffic detection status of WAF nodes.



Traffic forwarding status

1. Log on to Apsara Stack Security Center.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **System Info > Node status**.
4. On the **Node status** page, click the **Forward Status** tab.
5. View the traffic forwarding status of WAF nodes.

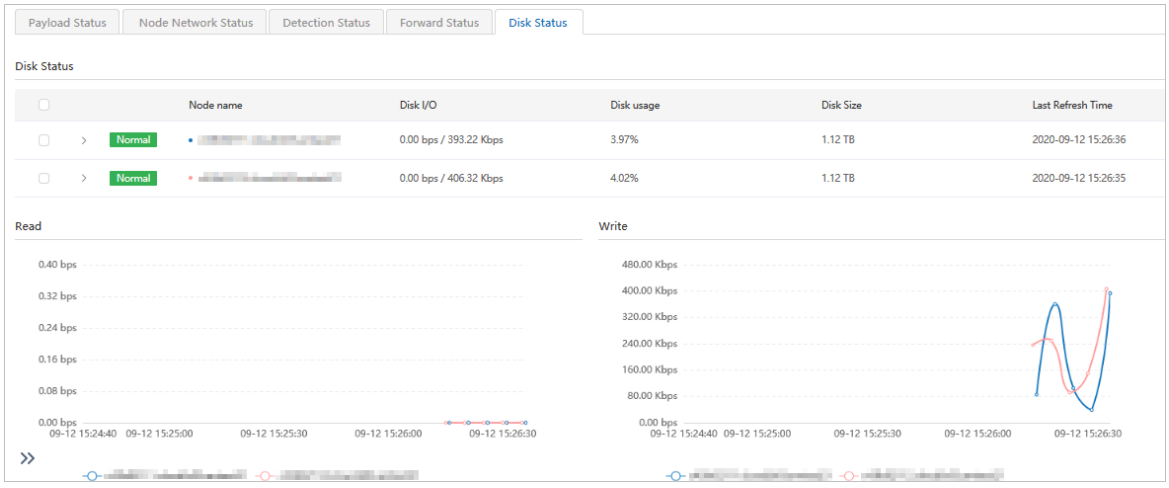


8.5.3. View the disk status of nodes

This topic describes how to view the disk status of Web Application Firewall (WAF) nodes. You can identify faults based on the status and check whether scale-out or scale-up is required.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **System Info > Node status**.
4. Click the **Disk Status** tab to view the disk status of WAF nodes.



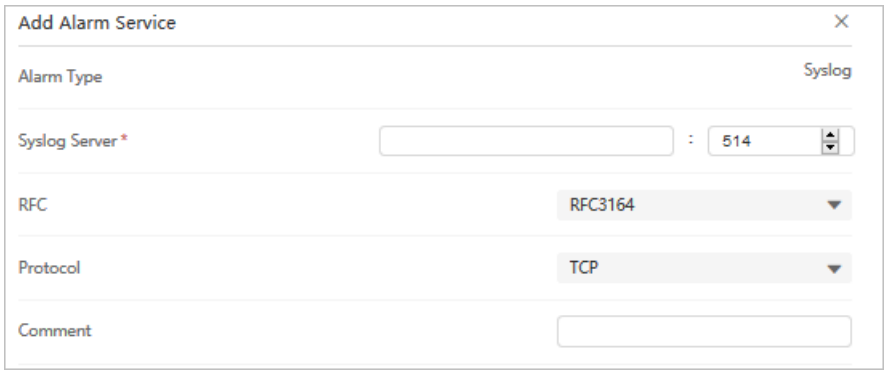
In the Disk Status section, you can view the disk I/O and disk usage of WAF nodes. In the **Read** and **Write** sections, you can view the changes in disk reads and writes over a specific period of time.

8.5.4. Configure alerts

This topic describes how to add a syslog server to Web Application Firewall (WAF). After the syslog server is added, WAF alert logs can be pushed to the syslog server over the syslog protocol.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **System Settings > Syslog Configuration** .
4. On the **Alarm Service Configuration** tab, click **Add alarm service**.
5. In the **Add Alarm Service** panel, configure parameters.



Parameter	Description
Syslog Server	The IP address and port number of the syslog server.
RFC	The Request for Comments (RFC) document that defines the syslog protocol. Valid values: **RFC3164** and **RFC5424**.
Protocol	The transmission protocol. Valid values: **TCP** and **UDP**.
Comment	The description of the syslog server. This information facilitates subsequent identification and management.
General	The type of alert. Valid values: System Management and System Monitor and Alarm.
Security	The module whose alert logs are sent to the syslog server.

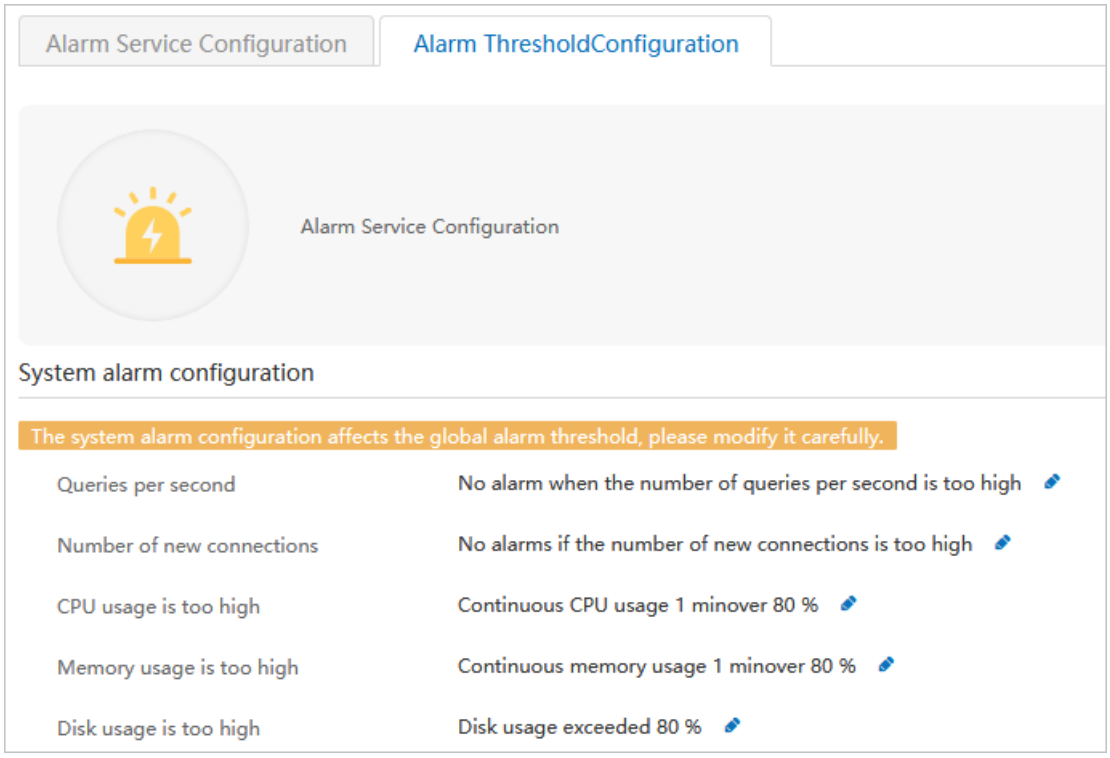
6. Click **Confirm**. The newly added syslog server appears in the list of the Alarm Service Configuration tab.
7. Find the newly added syslog server and click the icon in the **Operation** column to test whether alerts are sent.
   - If a message appears, indicating that the alert test is successful, the syslog server is added.
   - If an error message appears, WAF cannot connect to the syslog server.

8.5.5. Configure alert thresholds

This topic describes how to configure alert thresholds.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Application Security** section, click **Web Application Firewall**.
3. In the left-side navigation pane, choose **System Settings > Syslog Configuration** .
4. Click the **Alarm ThresholdConfiguration** tab and click the icon next to the threshold that you want to modify.
5. In the panel that appears, specify the threshold.



Threshold	Description
Queries per second	If queries per second exceed this threshold, alerts are sent. If this threshold is set to 0, no alerts are sent.
Number of new connections	If a large number of new connections exist, no alerts are sent.
CPU usage is too high	If CPU utilization exceeds this threshold in a specific period of time, alerts are sent.
Memory usage is too high	If memory usage exceeds this threshold in specific a period of time, alerts are sent.

Threshold	Description
Disk usage is too high	If disk usage exceeds this threshold, alerts are sent.

6. Click **OK**.

9.Security Operations Center (SOC)

9.1. Use the Operations Center module

The Operations Center module provides data security-related details of Apsara Stack. Security administrators can use this module to obtain the information about network attacks and defenses. This helps improve network security performance.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, click **Operations Center**.
4. On the **Operations Center** page, view the following operations data.

Section	Description	Supported operation

Section	Description	Supported operation
Data display setting section (Section 1)	In the section, you can specify the data that is displayed on the Operations Center page.	○ Select display items: Click Select View to select the types of data that you want to display from the drop-down list. By default, the following items are selected: **Alert data**, **Distribution of Alert Handling Methods**, **ECS Instance Protection**, **Risk Level**, **Distribution of Alerting Data Sources**, **Distribution of Alert Types**, **Top 10 Attacking IP Addresses**, **Top 10 Attacked IP Addresses**, **Top 5 Attacked Websites**, and **List display area**. You can select data types based on your business requirements. ○ Select data sources: Select data sources from the drop-down list next to Select View. ○ Save a view: Click the  icon to save the current view. ○ Manually update data: Click the  icon to manually update the data of the current view. ○ Enable automatic data update: Turn on  . The system updates the data of the current view every 5 minutes. ○ Export data: Click the  icon to export the data of the current view.

Section	Description	Supported operation
Query condition section (Section 2)	In the section, you can configure query conditions to query data. You can configure the following query conditions: **time range**, **alert asset or attacker IP address**, **handling status**, **global data**, **data source**, **alert type**, **severity**, **attack source**, and **tag**.	Configure query conditions and click **Search**. If you want to reconfigure the query conditions, click **Reset**.
Query result section (Section 3)	The section displays the query results that are returned based on the configured query conditions.	None.
Details section (Section 4)	The section displays the details of the query results that are returned based on the configured query conditions.	○ Configure the data display mode: ■ Click **Details**. The system displays the details of all attacked IP addresses in chronological order. ■ Click **Aggregate**. The system aggregates alerts with the same attacked IP address, attacker IP address, and severity level every 10 minutes and displays the details of the aggregated alerts. ○ View data details: Click **Details** in the Actions column of an alert to go to the **Details** panel. In the panel, you can view the details of the alert. ○ Add tags: Click **Batch Add Tags** to add tags to the alerts. This helps you troubleshoot issues. ○ Update data in the list: Click the  icon to manually update the data. ○ Configure display items: Click the  icon to select the items that you want to display in the list. By default, all items are selected.

9.2. Use the Threat Monitoring module

This topic describes how to view the overall security information about the Apsara Stack network environment.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, click **Threat Monitoring**.
4. In the upper-right corner of the **Threat Monitoring** page, select a time range from the **Time Statistics** drop-down list.

   Valid values: Last 24 Hours, **Last 7 Days**, and **Last 30 Days**.
5. View the overall security information within the specified time range.

   The Threat Monitoring page displays the following information:

   - **Newly Detected Attacks**, **Newly Detected Suspicious Processes**, **New Vulnerabilities**, and **Protected Organization**
   - **TOP5 attacked by the organization**, **TOP5 Pending Exception Behavior Organization**, **TOP5 Pending Vulnerability Organization**, and **ECS Protection State**
   - **Security Trend**, which supports a switchover between Tenant and Platform
   - **Latest abnormal behavior**, **Abnormal behavior type distribution**, and **New Assets**
   - **Latest Cyber Attack**, **Network attack type distribution**, and **Protected Assets**

9.3. Use the Risk Analysis module

9.3.1. View threat events

This topic describes how to view threat events. Security administrators can obtain threat details based on these events and ensure network security.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Security Operations Center**.
3. In the left-side navigation pane, choose **Risk Analysis > Threat Events**.
4. On the **Threat Events** page, view the details of threat events.

Section	Description	Supported operation
Search condition section (marked 1 in the preceding figure)	Specify search conditions for threat events. You can specify the **query time**, **threat level**, **threat type**, **attack stage**, **tag**, **threat name**, or **source or destination IP address** to search for threat events.	Select options from drop-down lists or enter keywords, and click the icon. If you do not specify search conditions, all threat events are automatically displayed.

Section	Description	Supported operation
Result section (marked 2 in the preceding figure)	The result section displays information about threat events that meet the specified search conditions.	◦ To view the details of a threat event, click the **name of the threat event** or click **Details** in the Actions column of the threat event. On the Threat Events page, view the information on the **Threat Details** and **Evidence Details** tabs. ◦ To add a tag to a threat event, click **Tag** in the Actions column of the threat event. This helps you identify the threat event in subsequent operations.

View the information on the **Threat Details** tab: On the **Threat Details** tab, view **Start Time**, **Last Detected At**, **Analysis Rules**, **Network protocol**, **Threat Intelligence**, **Source Details**, **Target Details**, and **Key Information**.

View the information on the **Evidence Details** tab: On the **Evidence** tab, view the raw logs of the threat event.

9.3.2. View vulnerability analysis results

This topic describes how to view vulnerability analysis results on the platform side and the tenant side. Security administrators can use the results to locate issues.

View platform-side vulnerability analysis results

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Security Operations Center**.
3. In the left-side navigation pane, choose **Risk Analysis > Vulnerability Analysis**.
4. On the **Vulnerability Analysis** page, click **Platform**.
5. On the **Platform Baseline** tab, specify the search conditions for platform baseline risks and click the icon.

> **Note** If you do not specify search conditions, all platform baseline risks are automatically displayed.

Search condition	Description
Risk Level	The level of the platform baseline risk.
Handling Status	The handling status of the platform baseline risk.
Start time and end time	The time range to query the platform baseline risk.
Risk Name	The keyword to match, such as the name of the platform baseline risk.

All the query results are displayed in the list of platform baseline risks. You can perform the following operations based on your business requirements:

- Click the icon to refresh the list of platform baseline risks.
- Click the icon to export the list of platform baseline risks.

View tenant-side vulnerability analysis results

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Risk Analysis > Vulnerability Analysis**.
4. On the **Vulnerability Analysis** page, click **Tenant**.
5. On the **Tenant** tab, click the **Vulnerabilities** or **Server Configurations** tab.
   - The **Vulnerabilities** tab provides information about vulnerabilities.
   - The **Server Configurations** tab provides information about server baseline risks.
6. Specify search conditions for vulnerabilities or server baseline risks and click the icon.

> **Note** If you do not specify search conditions, all vulnerabilities or server baseline risks are automatically displayed.

Search condition	Description
Organization	The organization to which the assets affected by the vulnerability or server baseline risk belong.
Level	The level of the vulnerability or server baseline risk.
Handling Status	The handling status of the vulnerability or server baseline risk.
Start time and end time	The time range to query the vulnerability or server baseline risk.
Vulnerability or risk name, asset keyword, or CVE ID keyword	The name of the vulnerability or server baseline risk, or the keywords of affected assets or Common Vulnerabilities and Exposures (CVE) IDs.

All the query results are displayed in the list of vulnerabilities or server baseline risks. You can perform the following operations based on your business requirements:

- Click the icon to refresh the list of vulnerabilities or server baseline risks.
- Click the icon to export the list of vulnerabilities or server baseline risks.

9.3.3. View traffic analysis results

This topic describes how to view the global traffic, including the average traffic, peak traffic, overall traffic trends, traffic of tenants, and traffic of platforms.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Security Operations Center**.
3. In the left-side navigation pane, choose **Risk Analysis > Traffic Analysis**.
4. On the **Traffic Analysis** page, view the global traffic information.

   You can view the following information on this page:

   - View the average traffic and peak traffic
     a. In the upper-left corner of the **Traffic Analysis** page, select a time range and traffic direction.

        Valid values of time ranges: **Last 6 Hours**, **Last 24 Hours**, and **Last 7 Days**.

        Valid values of traffic directions: **Inbound** and **Outbound**.

     b. In the upper-left corner of the Traffic Analysis page, view the average and peak traffic of the specified traffic direction within the specified time range.
   - View traffic trends
     a. In the upper-left corner of the **Traffic Analysis** page, select a traffic type.
     b. View the overall traffic trends of each traffic type within the specified time range.
   - View the traffic of tenants on the **Tenant Traffic** tab
   - View the traffic of platforms on the **Platform Traffic** tab

9.3.4. View threat intelligence

This topic describes how to view the overall situation and statistics of threats to your assets within the last 30 days.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Security Operations Center**.
3. In the left-side navigation pane, choose **Risk Analysis > Threat Intelligence**.
4. On the **Overview** page, view the statistics and threats that are detected on Apsara Stack services by the threat intelligence module.

   You can perform the following operations:

   - Search for an IP address to check whether the IP address is malicious.

     Enter the IP address that you want to check in the search box in the upper-right corner and click the icon. The information about the IP address is displayed on the details page of the IP address.
   - View the **Total malicious metric intelligence** section.

In the **Total malicious metric intelligence** section, view the information about the detected threats on Apsara Stack services. The information includes the number of malicious IP addresses, malicious domain names, and malicious URLs.

- View information in the **Malicious metric Intelligence Trends** section.
- View information in the **Threat Intelligence call summary** section.

  In the **Threat Intelligence call summary** section, view **Threat Intelligence Metrics**, **Threat IOC Query Type**, **Label Distribution in threat intelligence**, and **Threat Intelligence Query Statistics**.

9.4. Asset Management

9.4.1. View tenant assets

This topic describes how to view the assets of tenants. The assets include Elastic Compute Service (ECS) instances, ApsaraDB RDS instances, Object Storage Service (OSS) buckets, Server Load Balancer (SLB) instances, and elastic IP addresses (EIPs).

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Security Operations Center**.
3. In the left-side navigation pane, choose **Assets > Tenant Assets**.
4. On the **Tenant Assets** tab, you can view statistics in the **Assets**, **New Tenants in the Last 24 Hours**, and **Internet Assets** sections.
5. Select the required service and specify search conditions to view a specific asset. Service example: **Elastic Compute Service (ECS)**.

   You can also enter an IP address or instance name in the search box to search for an asset.

   > **Note** If you do not specify search conditions, all assets are automatically displayed

Search condition	Description
Organization	The organization to which the asset belongs.
VPC	The virtual private cloud (VPC) to which the asset belongs.
Status	The status of the asset.
New	Specifies whether the asset to query is newly added.
Automatic Snapshot Risk Level	The risk level of automatic snapshots for the asset.
Server name or IP address	The name or IP address of the server on which the asset is deployed.

6. View asset information in the asset list.

To export the asset information, click the  icon.

9.4.2. View platform assets

This topic describes how to view the protection information about physical machines on which platform assets are deployed. Security administrators can locate issues and obtain handling suggestions based on the information.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Assets > Platform Assets**.
4. On the **Server Security** tab of the **Platform Assets** page, search for a specific asset.

   The asset is displayed in the platform asset list.

   > **Note** By default, all assets are displayed.

5. Click the name of the asset. On the page that appears, view the information on the **Servers** and **Suspicious Process** tabs.

   If a large number of alerts are displayed, you can specify the **Data Source**, **Reminder**, **Warning**, **Urgency**, **Handling Status**, **Alert Type**, or **Start time and End time** parameter to filter a specific alert.

   When you handle an alert, click the **alert name** to go to the **Details** page. You can view **Affected Asset**, **Occurred At**, and **End At**. You can also view the details of the alert and the handling suggestion in the **Related Exceptions** section.

9.5. Use the Logs module

9.5.1. View the information on the Log Overview page

This topic describes how to view the logs that are displayed in the widgets on the Log Overview page.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane,, choose **Logs > Log Overview**.
4. On the **Log Overview** page, view the widgets of the logs.

   The **Log Overview** page displays the widgets of the logs that you add. You can modify or delete the widgets. You can also add other widgets.

   - Modify a widget (marked 1 in the preceding figure)

- Modify a widget (marked 1 in the preceding figure)
  a. Click **Modify** in the upper-right corner of the widget.
  b. In the **Modify** dialog box, reconfigure the **Chart Type**, **Category**, and **Value** parameters. When you configure the **Category** and **Value** parameters, take note of the following points:
     - **Category**: If you set **Chart Type** to **Bar Chart**, **Line Chart**, **Pie Chart**, or **Sheet**, you must specify this parameter.
     - **Value**: If you set **Chart Type** to **Pie Chart** or **Individual Value Plot**, you must specify this parameter.
  c. Click **Refresh** to preview the widget in the right side of the Modify dialog box.
  d. Above the widget, enter a new name to rename the widget.
  e. Click **OK**. The widget is updated on the **Log Overview** page.
- Delete a widget (marked 2 in the preceding figure)
  a. Click **Delete** in the upper-right corner of the widget.
  b. In the message that appears, click **OK**. The widget is deleted from the **Log Overview** page.
- Create a widget (marked 3 in the preceding figure)
  a. To create a widget, click **Please go to the log audit page to add a chart** in the **Add custom visualization chart** section in the lower part of the **Log Overview** page.
  b. On the **Perform Logs** page, create a custom widget. For more information, see View global logs.

9.5.2. Query raw logs

Security Operations Center (SOC) allows you to query raw logs. Raw logs contain information that is required for debugging. Security administrators can use these raw logs to troubleshoot system failures. This topic describes how to query raw logs.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane,, choose **Logs > Log Query**.
4. On the **Log Query** page, specify the **time**, **organization**, **system type**, **log source**, **log type**, and **query syntax**. Then, click **Search**.

   The numbers of the queried logs within the specified time range are displayed in a bar chart. The log details are displayed in a list. The following list describes the supported query syntax:

   - **Full-text match**

     Example 1: 12.12.12.12. Example 2: www.bai*.c?m.

   - **Field-based query**

     Example 1:

     ```
     src_ip: 12.12.12.12 AND hostname:abc?o*al OR filesize:>100
     ```

     Example 2:

```
12.12.12.12 AND appName:yundun-soc
```

- **SQL-like query**

  Example 1:

```
select * from mytable where src_ip = '12.12.12.12' order by gmt_create desc
```

  Example 2:

```
select src_ip, count(*) as cnt, max(filesize) as filesize from mytable group by src_ip limit 10
```

  Example 3:

```
select count(*) as cnt from mytable where hostname like '%abc%'
```

> **Notice**
>
> - When you perform field-based queries, specify the logical operators AND, OR, and NOT in upper-case letters.
> - When you enter an SQL statement to query logs, specify the database table name as **mytable**.
> - When you enter an SQL statement to query logs, user-defined functions (UDFs) and nested queries are not supported.
> - When you enter an SQL statement to query logs, the DISTINCT operations are not supported.
> - When you enter an SQL statement to query logs, you can use the count(*) as cnt function to rename the queried log fields cnt. You cannot use src_ip as ip to rename the queried IP addresses ip.
> - When you enter an SQL statement to query logs, only fields of the string type can be aggregated.
> - If a query times out when you use a wildcard character to query logs, you can narrow down the query scope and try again.

5. In the log list, select the fields that you want to query and view the logs about the fields.

   You can also expand a display field to view the top 5 values of the field.

9.5.3. View platform logs

Platform logs record information about Apsara Stack Security. Security administrators can use these logs to troubleshoot issues that occur on Apsara Stack Security. This topic describes how to view platform logs.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane,, choose **Logs > Platform Logs**.

4. On the **Platform Logs** page, specify the data source, time range, and query content to query logs based on your business requirements. You can also click **Advanced Search** and enter domain-specific language (DSL) statements to query logs in exact match mode.

   The system displays platform logs in a bar chart based on the query conditions that you specify. You can view the numbers of logs at different points in time within the specified time range.

5. On the **Logs** tab of the **Platform Logs** page, view the details of the returned logs.

   - To configure the fields that you want to display in the log list, click the  icon.
   - To view the details of a log, click **Details** in the data column of the log.
   - To export the log list, click the  icon.

6. Click the **Visualization** tab, configure the parameters, and view the displayed widget of logs.

   To display the widget on the **Log Overview** page, specify a name for the widget on the Visualization tab and click **Add to Log Visualization**. This way, you can track logs in a convenient manner.

Parameter	Description
Chart Type	The type of widget that you want to display on the **Log Overview** page. Valid values: **Bar Chart**, **Line Chart**, **Pie Chart**, **Individual Value Plot**, and **Sheet**.
Category	This parameter is required only if you select **Bar Chart**, **Line Chart**, **Pie Chart**, or **Sheet** for **Chart Type**. The type of item that you want to display in the horizontal axis or the column header of the widget.
Value Category	The type of item that you want to display in the vertical axis or the row header of the widget.
Value Type	The type of value that you want to display in the widget. Valid values: **count**, **max**, **min**, **avg**, **sum**, **unique_count**, and **median**. If you want to display multiple value types in the widget, click **Add Value Field**. Then, you can configure the **Value Category** and **Value Type** parameters.

9.5.4. View tenant logs

Tenant logs record information about tenants. Security administrators can use these logs to troubleshoot issues that occur on the tenant side. This topic describes how to view tenant logs.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane,, choose **Logs > Tenant Logs**.
4. On the **Tenant Logs** page, specify the **data source**, **time range**, and query content to query

logs based on your business requirements. You can also click **Advanced Search** and enter domain-specific language (DSL) statements to query logs in exact match mode.

The system displays **tenant logs** in a bar chart based on the query conditions that you specify. You can view the numbers of logs at different points in time within the specified time range.

5. On the **Logs** tab of the **Tenant Logs** page, view the details of the queried logs.
   - To configure the fields that you want to display in the log list, click the icon.
   - To view the details of a log, click **Details** in the data column of the log.
   - To export the log list, click the icon.
6. Click the **Visualization** tab, configure the parameters, and view the displayed widget of logs.

   To display the widget on the **Log Overview** page, specify a name for the widget on the Visualization tab and click **Add to Log Visualization**. This way, you can track logs in a convenient manner.

Parameter	Description
Chart Type	The type of widget that you want to display on the **Overview** page. Valid values: **Bar Chart**, **Line Chart**, **Pie Chart**, **Individual Value Plot**, and **Sheet**.
Category	This parameter is required only if you select **Bar Chart**, **Line Chart**, **Pie Chart**, or **Sheet** for **Chart Type**. The type of item that you want to display in the horizontal axis or the column header of the widget.
Value Category	The type of item that you want to display in the vertical axis or the row header of the widget.
Value Type	The type of value that you want to display in the widget. Valid values: **count**, **max**, **min**, **avg**, **sum**, **unique_count**, and **median**. If you want to display multiple value types in the widget, click **Add Value Field**. Then, you can configure the **Value Category** and **Value Type** parameters.

9.5.5. Log configurations

9.5.5.1. Manage log sources

This topic describes how to manage the log sources that are connected to Security Operations Center (SOC).

Manage log sources

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform**

Security section, click **Security Operations Center**.

3. In the left-side navigation pane,, choose **Logs > Log Settings**.
4. On the **Log Sources** tab of the **Log Settings** page, click **New log source**.
5. In the **New log source** panel, configure the following parameters.

Parameter	Description
Log Source	Specify the log source. The value is fixed as Third-party Network Element.
Name	Specify the name of the log source. The name can be 0 to 64 characters in length.
Access System Type	Select the type of the source system in the log source that is connected to SOC. Valid values: **Host**, **Storage**, **Application**, **Network**, **Data**, **Security**, and **Others**.
Reliability Level	Enter the reliability level of the log data that is obtained from the log source. This value is used as the weight value of log analysis and affects the analysis result. Valid values: 0 to 100.
Data Protocol	Select the protocol over which the log data is shipped to SOC. Valid values: ○ **Syslog** ○ **SLS**
IP Address	Enter the IP address of the log source.
Host Name	Enter the hostname of the host on which the log source is deployed.
Protocol	Select the protocol. Valid values: ○ **UDP** ○ **TCP**
Log Parsing	Select a log parsing template. You can click **Create Log Parsing Template** to create a log parsing template. You can also select an existing log parsing template. For more information, see Configure a log parsing template.
Storage Period	Specify the log storage period. Valid values: 0 to 180. Unit: days.
Permission Scope	Specify the level of the log source. Valid values: ○ **Platform** ○ **Tenant** If you want to visualize threats that are generated for the specified log source level on the Operations Center page, select Display Alerts in Operations Center.

Parameter	Description
Description	Enter the description for the log source. The description can be 0 to 128 characters in length.

6. Click **OK**.
   After the log source is created, the log source is displayed in the log source list. You can modify the information about the log source or delete the log source based on your business requirements. If the log source list contains a large number of log sources, you can search for a log source by **system type**, **data source**, **data protocol**, or **status of log source**.

9.5.5.2. Configure a log parsing template

Security Operations Center (SOC) provides the log parsing feature. Security administrators can configure log parsing templates based on their business requirements to manage logs in an efficient manner.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. On the **Log Settings** page, click **Log Parsing**.
4. On the **Log Parsing** tab, click **Create Log Parsing Template**.
5. In the **Create Log Parsing Template** panel, specify **Template Name** and **Application Scope**. Click **Next**.
6. Click **Create Rule** to create a rule that is associated with the log parsing template.
   i. Specify information about the rule.

      Specify **Rule Name** and **Log Type**. Then, click **Next**.

      Valid values of Log Type: **System Log**, **Operation Log**, **Network Log**, **Threat Log**, **Application Log**, and **Others**.

   ii. Configure a log parsing method.

      Specify **Log Sample** and **Log Identifier**, and select a value for **Parsing Method**. Then, click **Parse**. After the parsing is complete, click **Next**.

      You can also click **Add** to configure multiple parsing methods.

   iii. Specify field mappings to format logs.

      Specify field mappings to format logs and click **Confirm**.

   If you want to create multiple rules, repeat the preceding steps.

7. After the rule is created, click **Confirmation**.
   The log parsing template that you create is displayed in the log parsing list. You can modify or delete the template based on your business requirements.

9.5.5.3. Configure log forwarding

Security Operations Center (SOC) provides the log forwarding feature. Security administrators can forward logs based on their business requirements and view logs in a timely manner.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Logs > Log Settings**.
4. On the **Log Settings** page, click **Log Forwarding**.
5. On the **Log Forwarding** tab, configure the following parameters.

Parameter	Description
Enable Log Forwarding	Turn on or off the switch to enable or disable the log forwarding feature.
IP:Port	Specify the IP address and port number of the server or third-party platform to which logs are forwarded. To add multiple IP addresses and port numbers, click **Add**.
Data Protocol	Select the protocol of log data. The value is fixed as **Syslog**.
Select Log Source	Select the log sources from the **Log Source** list and add the selected log sources to the **Selected Log Sources** list. The logs of the selected log sources are forwarded.

6. Click **Save**.

9.6. Use the Reports module

This topic describes how to create a report task. After you create a report task, the system sends reports to the specified email addresses at specified intervals.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane,, click **Reports**.
4. On the **Reports** page, click **Create Report**.
5. In the **Create Report** dialog box, configure the parameters.

Parameter	Description
Report Name	The name of the report task. We recommend that you enter information such as the report purpose for easier identification and management.
Task type	The type of the task. Valid values: **Daily Report**, **Weekly Report**, and **Monthly Report**.
Organization	The organizations to which the report task is related.
Email Box	The email address of the report recipient. If you enter more than one email address, separate the email addresses with commas (,).

6. Click **OK**.

Result

In the report task list, you can download, edit, and delete the newly created report tasks.

9.7. Use the Rules module

9.7.1. Create an analysis rule

You can use analysis rules to perform comprehensive association analysis on a large number of logs. You can also trace attack paths of multi-phase attacks based on the detected high risks. This way, security administrators can obtain helpful risk information in an efficient and quick manner and the efficiency of security operations is improved. This topic describes how to create a custom analysis rule.

Procedure

Security Operations Center (SOC) provides built-in rules based on common business requirements. You can only view the details of the built-in rules but cannot modify the rules. If the built-in rules cannot meet your business requirements, you can perform the following steps to create a rule:

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Rules > Analysis Rules**.
4. On the **Analysis Rules** page, click **Create Rule**.
5. On the **Create Rule** page, configure the following parameters.

Parameter	Description
Threat Name	Specify a name for a threat.

Parameter	Description
Threat level	Select a level for the threat. Valid values: ○ **Info** ○ **Suspicious** ○ **Moderate** ○ **Serious** ○ **Critical**
Threat type	Select one or more types for the threat. Valid values: ○ **Network Scanning** ○ **Vulnerability Exploitation** ○ **Malware** ○ **Network Attack** ○ **Suspicious Network Connection** ○ **Privilege Escalation** ○ **Suspicious Process**
ATT&CK ID	Enter the one or more IDs of the attacks that are involved in the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) stages.
Time Series	Specify the time condition for the rule that you want to create. Valid values: ○ **Periodicity**: indicates that the rule is used to detect the threats that occur within the same period of time. ○ **Chronological Order**: indicates that the rule is used to detect the threats that occur in sequence.
Associated Object	Specify the object on which the rule is used to detect threats. The value is fixed as **Same Asset**.

Parameter	Description
Trigger Condition	Specify the trigger condition. You can configure the following parameters to specify the trigger condition: ○ **Condition Type**. Valid values: **Necessary Condition** and **Sufficient Condition**. ○ **Log Scope**, which includes the **Log Source**, **Log Type**, and **Log Level** parameters. ○ **Source IP** and **Destination IP**. ○ **Keyword**. If you specify multiple keywords, separate them with semicolons (;). ○ **Duration**. Valid values: 0 to 1440. Unit: minutes. ○ **Number of Logs**. ○ **Attack Phase**. Valid values: **Payload Delivery**, **Vulnerability Exploitation**, **Backdoor Installation**, **Command and Control**, **Scanning**, and **Action on Objectives**.
Execution Period	Specify the interval at which the rule is executed. Default value: 5 minutes.
Description	Enter the description of the threat. The description can be 0 to 256 characters in length.
Handling Suggestion	Enter the handling suggestion. The suggestion can be 0 to 256 characters in length.

6. Click **OK**.
   The created rule is displayed in the rule list.

   You can click **Edit** or **Delete** in the Actions column of a custom rule to modify or delete the rule based on your business requirements.

9.7.2. Create a blocking rule

This topic describes how to manually block requests for a specific IP address with a few clicks.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Rules > Blocking Rules**.
4. On the **Blocking Rules** page, click **Add**.
5. In the **Add** dialog box, configure the following parameters.

Parameter	Description

Parameter	Description
Protocol	Specify the type of the IP address that you want to block. Valid values: **IPv4** and **IPv6**.
Source IP Address	Enter the source IP address that you want to block.
Destination IP Address	Enter the destination IP address that you want to block.
Destination Port	Enter the destination port that is used with the specified destination IP address.
Blocking Duration	Select a time range during which you want to block requests. Valid values: **1 Day**, **7 Days**, and **30 Days**.
Type	Select the blocking mode. Valid values: **Whitelist** and **Blacklist**.
Description	Enter the reason for blocking.

6. Click **OK**.
   The created blocking rule is displayed in the rule list. You can **query** or **delete** the rule based on your business requirements.

9.8. Use the Operations module

9.8.1. Security Audit

9.8.1.1. Overview

A security audit refers to the systemic and independent inspection and verification of activities and behavior in the computer network environment. Delegated by property owners and authorized by management authorities, professional auditors give their assessments according to relevant laws and regulations. When the administrator needs to backtrack system operations, the administrator can perform a security audit.

Security audits are long-term security management activities 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 important, 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.

9.8.1.2. View the summary information about security audit

This topic describes how to view the summary information about security audit.

Context

The **Overview** tab provides reports on the raw log trend, audit event trend, audit risk distribution, and security event distribution. The reports are displayed in run charts or pie charts to help security administrators analyze the trend of risks in your cloud services.

On the **Overview** tab, security administrators can check the number of logs and the storage usage in a specific time range.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click the **Overview** tab.
5. On the **Overview** tab, view the audit summary for the last seven days.
   - Trends of Raw Log

     This chart displays the trend of logs that are generated by **Platform Database**, **Server**, **Network Device**, **User Actions**, **Administrator Actions**, and **ECS** in the last seven days. Security administrators can analyze the trend to check whether the number of logs is at a normal level.
   - Audit Events

     This chart displays the trend of audit events that are generated by **Platform Database**, **Server**, **Network Device**, **User Actions**, **Administrator Actions**, and **ECS** in the last seven days. Security administrators can analyze the trend to check whether the number of audit events is at a normal level.
   - Audit Risk Distribution

     This chart displays the percentage distribution of audit events at different risk levels in the last seven days. Risk levels are important, moderate, and low. Security administrators can analyze the trend to check whether the audit events are at acceptable risk levels.
   - Security Issue Distribution

     This chart displays the percentage distribution of different event types in the last seven days. Security administrators can analyze this chart to check for the most frequent audit events and identify high-risk events to improve security protection.
   - Log Size

     This chart displays the volume of online logs and offline logs. If these logs consume a large number of storage resources, we recommend that you back up required audit logs and delete unnecessary logs.
   - Audit Log Size

     This chart displays the size of logs for each audit type.
6. View the audit summary in a specific time range.
   i. Specify **End Time** as the end of the time range to query.
   ii. In **Audit Type**, select the audit types to query.
   iii. Click **View** to view the audit summary in the last seven days before the specified end time.

9.8.1.3. Query audit events

This topic describes how to query audit events.

Context

On the **Audit Query** tab, you can view the details of audit events, including the log creation time, audit type, audit object, action type, risk level, and log content.

The system matches the logs that are collected by a security audit module against audit rules. If the log content matches the regular expression in an audit rule, an audit event is reported.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click the **Audit Query** tab.
5. On the **Audit Query** tab, configure query conditions to view audit events within the specified time range.
   - Basic query
     a. Configure **Audit Type**, **Audit Target**, **Action Type**, **Risk Level**, and **Notify**
     b. Specify a time range to query.
     c. In the **Full-Text Search** search box, enter a keyword.
     d. Click **Search**.
   - Advanced query

     In addition to the basic query conditions, you can configure advanced query conditions.
     a. Configure basic query conditions.
     b. Click **Advanced Search**.
     c. In the **Filter Condition** section, configure **Filter Name**, **User**, **Target**, **Action**, **Result**, and **Cause**.
     d. Click **Save**.
6. Click **Export** to export the audit events.

   Download the exported file for analysis. For more information, see Manage export tasks.

9.8.1.4. View raw logs

This topic describes how to view raw audit logs.

Context

On the **Raw Log** tab, you can view the raw logs that are generated by a running audit object. Raw logs contain information that is required for debugging. Security administrators can use these raw logs to troubleshoot system failures.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click the **Raw Log** tab.
5. On the **Raw Log** tab, configure query conditions to view the log summary chart and raw logs within a specific time range.
   i. Specify **Audit Type** and **Audit Target**.
   ii. Enter a keyword.
   iii. Specify a time range to query.
   iv. Click **Search**.
6. Click **Export** to export the audit events.

   Download the exported file for analysis. For more information, see Manage export tasks.

9.8.1.5. View the number of logs

This topic describes how to view and manage log sources.

Context

You can view the number of logs and specify whether to show logs by log type or log source.

- The Log Types tab provides the number of all logs for a specific audit object of a specific device instance.
- The Log Sources tab provides the number of logs for all audit objects of a specific device instance.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click the **Log Types** tab to view the number of logs by audit object.

   You can view the number of logs that are recorded on the current day and the number of logs that are recorded during the last 30 days for each audit object.

   If you do not want to display the logs for an audit object, perform the following steps:

   i. Find the audit object and click **Hide** in the **Actions** column.
   ii. In the Note message, click **Confirm**.

   > **Note** The process that is used to display the logs for an audit object is similar to the process that is used to hide the logs.

5. Click the **Log Sources** tab and view the number of logs for each device instance.

You can view the number of logs that are recorded on the current day and the number of logs that are recorded during the last 30 days for each device instance.

If you do not want to display the logs for an audit object from a specific device instance, perform the following steps:

i. Find the device instance and click **Hide** in the **Actions** column.

ii. In the message that appears, click **OK**.

> **Note** The process that is used to display the logs for an audit object is similar to the process that is used to hide the logs.

9.8.1.6. Policy settings

9.8.1.6.1. Manage audit rules

This topic describes how to create, modify, or delete an audit rule.

Context

If a log matches an audit rule, an audit event is reported. You can specify regular expressions in an audit rule to match logs. A regular expression defines a matching pattern for character strings and can be used to check whether a string contains a specific substring. The following table provides examples about the pattern.

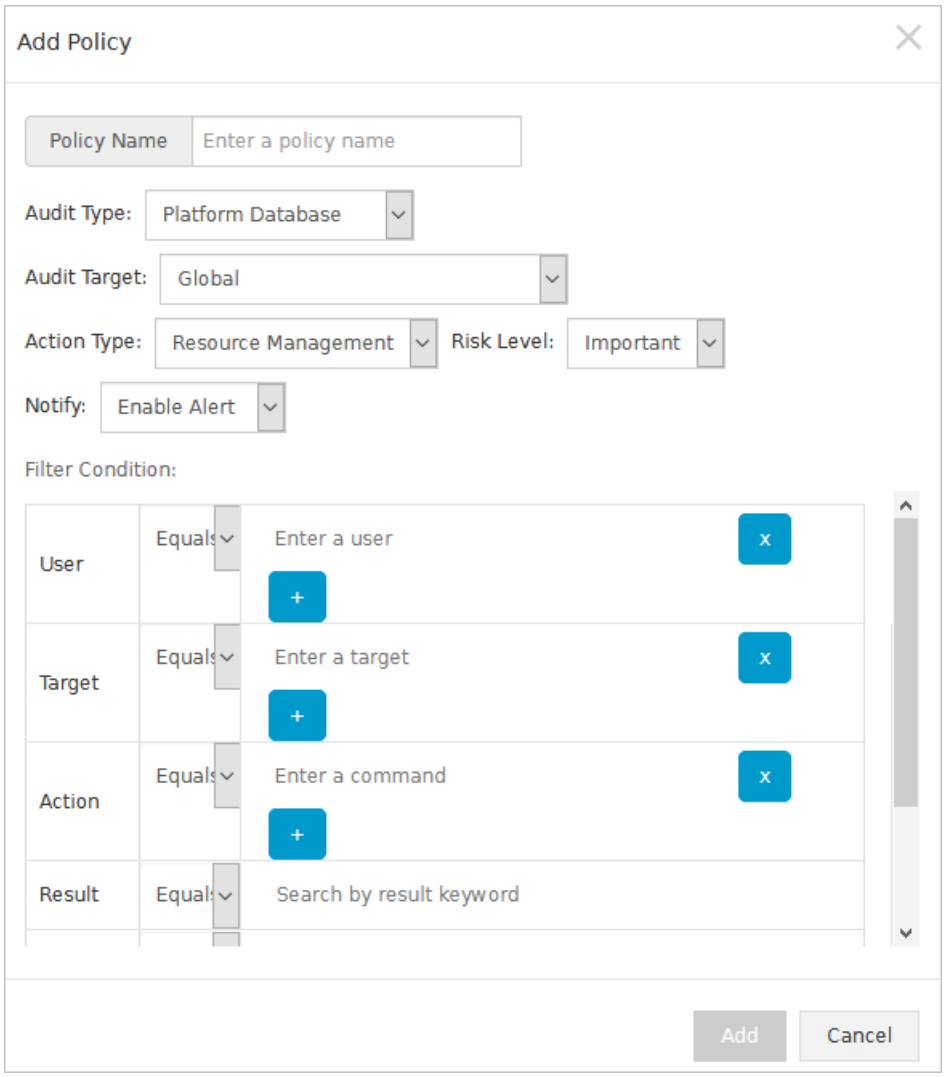
Regular expression	Description
`^\d{5,12}$`	Matches the consecutive numbers from the fifth number to the twelfth number.
`load_file\(`	Matches the "load_file(" string.

The security audit module defines the default audit rule based on the string that is generated in the log. This applies when an audit event is reported. A security administrator can also customize audit rules based on the string that is generated in the log. This applies when the system encounters an attack.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click the **Policies** tab.
5. On the **Policies** tab, click the **Audit Rules** tab.
6. Create an audit rule.
   i. Click **New** in the upper-right corner.

ii. In the **Add Policy** dialog box, configure the parameters.



iii. Click **Add**.

The system sends an alert email to the specified alert recipient after you create an audit rule. This applies if one string in an audit log of the specified audit type, audit object, or risk level matches the regular expression of the audit rule.

7. Manage audit rules.

   You can create, query, disable, enable, and delete audit rules.

   - Query audit rules

     Specify **Audit Type** and **Audit Target**. Enter a keyword in the search box and click **Search**.

   - Disable an audit rule

     Find the audit rule that you want to disable and click **Disable** in the **Actions** column.

   - Enable an audit rule

     Find the audit rule that has been disabled and click **Enable** in the **Actions** column.

   - Delete an audit rule

     Find the audit rule that you want to delete and click **Delete** in the **Actions** column.

> **Note** You can delete only custom rules.

9.8.1.6.2. Configure alert recipients

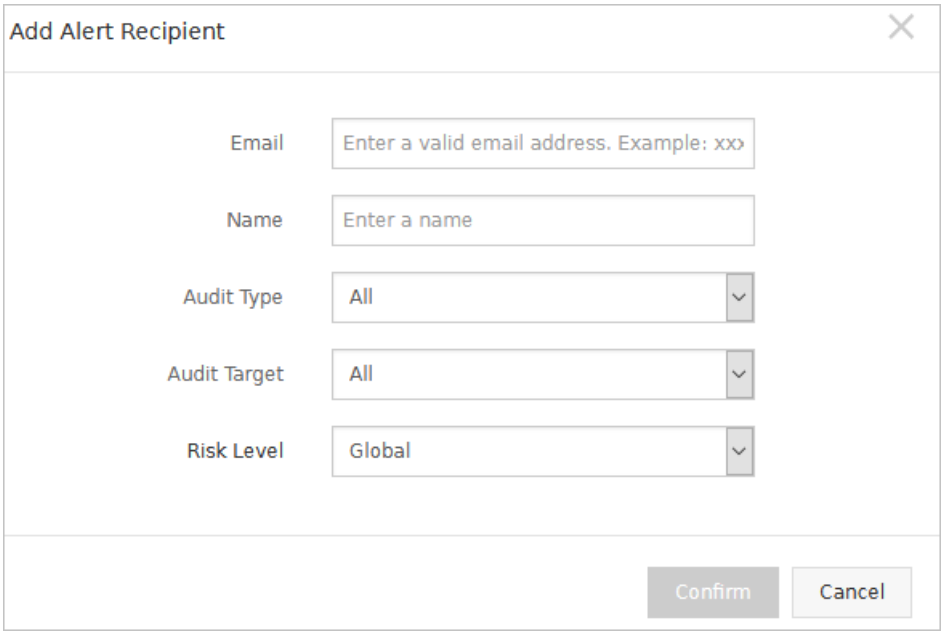
This topic describes how to configure the recipients of alerts on audit events.

Context

After you specify an alert recipient, the system sends a report to the email address of the alert recipient when an audit event occurs.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click the **Policies** tab.
5. On the **Policies** tab, click the **Alert Settings** tab.
6. Create an alert recipient.
   i. Click **New**.
   ii. In the **Add Alert Recipient** dialog box, configure the parameters.



   iii. Click **Confirm**.
7. Manage alert recipients.
   - Search for alert recipients

     Specify **Audit Type**, **Audit Target**, and **Risk Level**, enter the keyword of the email address, and then click **Search**.

- Delete alert recipients

  Find the email address that you want to delete and click **Delete** in the Actions column.

9.8.1.6.3. Query the archives of audit events and raw logs

This topic describes how to query and download the archives of audit events and raw logs.

Context

You can download the archives of events and logs to analyze audit events. This ensures the security of the Apsara Stack environment.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click the **Policies** tab.
5. On the **Policies** tab, click the **Archiving** tab.
6. Query the archives of events and logs.
   i. Specify **Audit Type** and **Archiving Type**.
   ii. Specify a time range to query.
   iii. Click **Search**.

   Find the file where the archive information is stored and click **Download** in the **Actions** column to save the archive file to your computer.

9.8.1.6.4. Download exported audit events or logs

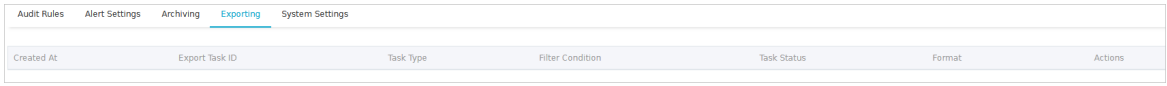
This topic describes how to download exported audit events or logs.

Context

You can export audit events or logs on the **Audit Query** or **Raw Log** tab of the Security Audit page. After you export audit events or logs, you can manage the export tasks on the Exporting tab.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click the **Policies** tab.
5. On the **Policies** tab, click the **Exporting** tab.
6. View the created export tasks.



7. Click **Download** to download audit events or logs to your on-premises server.

   To delete an export task, click **Delete**.

9.8.1.6.5. Modify system settings

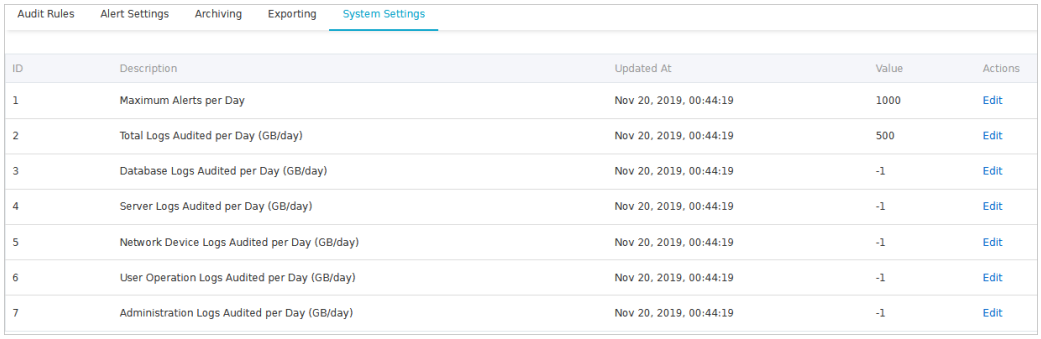
This topic describes how to configure system parameters for security audit.

Context

You can configure system parameters to specify the maximum number of system alerts per day and the maximum number of audits per day for raw logs.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Security Audit**.
4. On the **Security Audit** page, click **Policies**.
5. On the **Policies** tab, click the **System Settings** tab.
6. Find the system parameter that you want to modify and click **Edit** in the **Actions** column.



7. Enter a required value in the Value column and click **Confirm** in the Actions column.

9.8.2. Configure the log storage policy

Security Operations Center (SOC) allows you to create a custom log storage policy based on your business requirements. This topic describes how to configure the log storage policy.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > Storage Management**.
4. On the **Storage Management** page, click **Modify**.

SOC provisions default values for the log storage policy. If the default values do not meet your business requirements, you can specify other values for the log storage policy.

5.

Section	Parameter	Description
Log Storage (Advanced)	Maximum Log Size	The upper limit of the storage that can be used to store logs.
	Maximum Storage Period	The maximum number of days during which logs can be stored.
Security Monitoring Data Storage (Advanced)	Internal RDS Storage	The maximum number of days for which monitoring data can be stored.

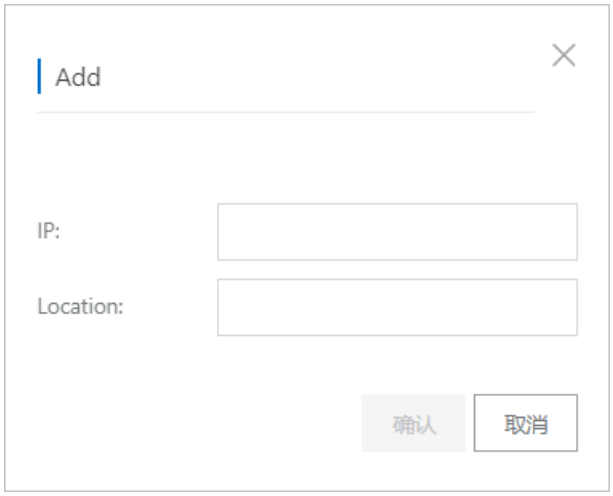
9.8.3. Add custom IP addresses and locations

This topic describes how to add custom IP addresses and locations. You can customize internal IP addresses based on your network plan. After you configure the internal IP addresses, IP addresses from the public address library do not match the addresses outside China.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Security Operations Center**.
3. In the left-side navigation pane, choose **Operations > IP Address Library**.
4. Click **Add**.

   If you want to add multiple IP addresses and locations at a time, click **Batch Upload (.txt)**. This can be used to import multiple IP addresses and locations as a template.
5. In the **Add** dialog box, configure the parameters.



6. Click **OK**.
   The added IP address is displayed in the IP address list. You can perform the following operations

based on your business requirements:

- Modify the IP address and location

  Click **Modify** to the right of the IP address. In the **Modify** dialog box, modify the IP address and location.

- Delete the IP address and location

  Click **Delete** to the right of the IP address. In the **Delete** message, click **OK**.

10.Optional security products

10.1. Anti-DDoS settings

10.1.1. Overview

In DDoS attacks, attackers exploit the client/server architecture to combine multiple computers into a platform that can launch attacks on one or more targets. This significantly increases the threat of attacks.

The following section describes common DDoS attacks:

- **Network-layer attacks**: A typical example is UDP reflection attacks, such as NTP flood. When this type of attacks are launched, the network of the victim is congested by heavy traffic. As a result, the victim cannot respond to user requests.
- **Transport-layer attacks**: Typical examples include SYN flood and connection flood. When this type of attacks are launched, a large number of connection resources of the target server are consumed. As a result, the server rejects service requests.
- **Session-layer attacks**: A typical example is SSL flood. These attacks consume the SSL session resources of a server to cause denial of service.
- **Application-layer attacks**: Typical examples include DNS flood, HTTP flood, and NTP flood. When this type of attacks are launched, a large number of connection resources of the target server are consumed. As a result, the server rejects service requests.

Apsara Stack Security can redirect, scrub, and re-inject attack traffic to protect your server against DDoS attacks and ensure normal business operations.

> **Note** Apsara Stack Security cannot scrub the traffic between internal networks.

10.1.2. View and configure DDoS mitigation policies

This topic describes how to view and configure DDoS mitigation policies. Anti-DDoS provides default DDoS mitigation policies and DDoS traffic scrubbing policies.

Context

After an alert threshold of DDoS traffic for an IP address is set, an alert is triggered when traffic to the IP address reaches the threshold. The alert threshold for an IP address must be specified based on the traffic volume. An excessively large traffic volume may indicate DDoS attacks. We recommend that you set an alert threshold to a value that is slightly higher than the peak traffic volume.

Apsara Stack Security supports a global alert threshold, alert threshold for a specific CIDR block, and alert threshold for an IP address.

- Global alert threshold: You cannot specify a global alert threshold. The threshold is automatically specified when Apsara Stack Security is initialized.
- Alert threshold for a CIDR block: You can specify an alert threshold for a CIDR block based on the traffic volume of the CIDR block. CIDR block-specific alert thresholds allow you to manage the traffic

to each CIDR block.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Network Security > Traffic Scrubbing**.
3. In the left-side navigation pane, click **DDoS Defense Policy**. On the **Anti-DDoS Policy** page, view and customize DDoS mitigation policies.

Operation	Description
View the default policy	Move the pointer over the icon next to Built-in Default Policy to view the default DDoS mitigation policy.
Customize a policy	Click View to view CIDR block-specific policies. Click +Add to customize a DDoS mitigation policy for a CIDR block.

To customize a policy for a CIDR block, perform the following steps:

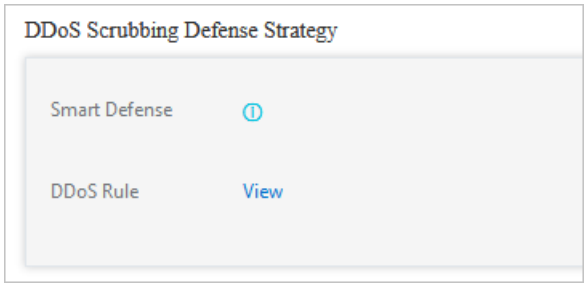
i. Click **+Add** to the right of **Custom Mode**.

ii. In the **Modify** dialog box, configure the parameters.

Parameter	Description
CIDR Block	The CIDR block for which you want to use the alert threshold.
Bandwidth Threshold (pps)	The alert threshold for bandwidth usage in a data center. When the sum of inbound and outbound traffic reaches the threshold specified by this parameter, DDoS detection is triggered. Set this parameter to a value that is slightly higher than the peak traffic volume. We recommend that you set the value to 100 or higher. Unit: Mbit/s.
Packet Threshold (pps)	The alert threshold for the packet rate in a data center. When the sum of inbound and outbound packet rates reaches the threshold specified by this parameter, DDoS detection is triggered. Set this parameter to a value that is slightly higher than the peak packet rate. We recommend that you set the value to 20000 or higher. Unit: packets per second (pps).

iii. Click **OK**.

4. In the **Policy for DDoS Attack Traffic Scrubbing** section, click **View** to view DDoS traffic scrubbing policies.



10.1.3. View DDoS traffic scrubbing events

This topic describes how to view DDoS traffic scrubbing events.

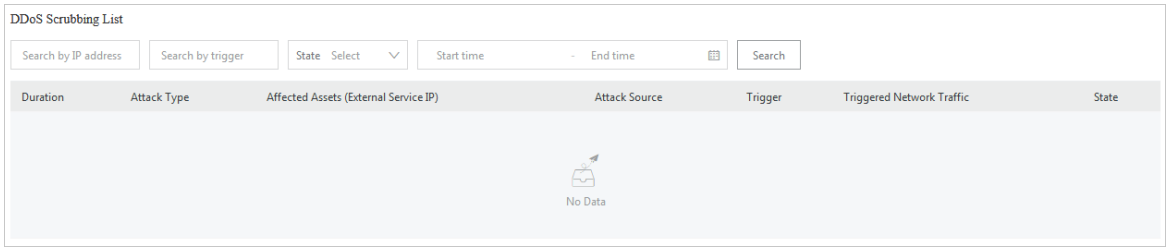
Context

Apsara Stack Security reports security events to Apsara Stack Security Center during and after traffic scrubbing.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Network Security > Traffic Scrubbing**.
3. In the left-side navigation pane, click **Network Protection**. On the **Anti-DDoS** page, view anti-DDoS statistics.
4. (Optional)In the **DDoS Attack Traffic Scrubbing** section, specify search conditions and click **Search**.

> **Note** If you want to view all traffic scrubbing events, skip this step.



Search condition	Description
Search by IP address	The IP address that was under a DDoS attack.
Search by trigger	The metric whose value exceeds the specified alert threshold in the DDoS attack traffic.

Search condition	Description
Status	The status of DDoS attack traffic scrubbing. Valid values: ○ **Local Scrubbing** ○ **Switching to Anti-DDoS Pro** ○ **Switching to Anti-DDoS Service** ○ **Local Scrubbing Completed** ○ **Cloud Scrubbing Completed** ○ **Under Blackhole Filtering**
Start time and end time	The start time and end time of DDoS attack traffic scrubbing.

5. In the DDoS Scrubbing List section, view details about DDoS traffic scrubbing events.

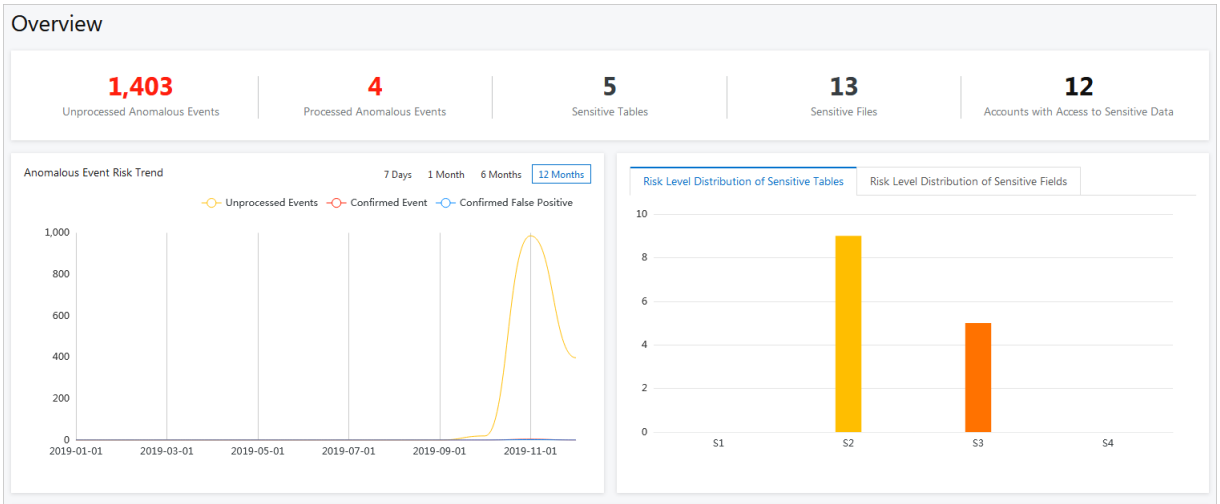
10.2. Sensitive Data Discovery and Protection

10.2.1. SDDP overview

This topic provides an overview about Sensitive Data Discovery and Protection (SDDP). The Overview page of SDDP displays the overall security status of data protected by SDDP. The information on this page allows security administrators to have an overview of sensitive data and take countermeasures in time.

SDDP can detect sensitive data in your data assets based on specific detection rules and track the use of sensitive data. SDDP also provides an overview of sensitive data to help you obtain the security status of your data assets in real time.

If you want to view the overall security status of the sensitive data, log on to Apsara Stack Security Center. In the top navigation bar, choose **Security > Data Security > Sensitive Data Discovery and Protection**. In the left-side navigation pane, click Overview.



- **Overview**: displays the overall information about sensitive data. The information includes

Unprocessed Anomalous Events, **Processed Anomalous Events**, **Sensitive Tables**, **Sensitive Files**, and **Accounts with Access to Sensitive Data**.

- **Abnormal Event Risk Trend**: displays the trends of different events in a line chart. You can click **7 Days**, **1 Month**, **6 Months**, or **12 Months** to view the trends of different events, such as **Unprocessed Events**, **Confirmed Event**, and **Confirmed False Positive**.
- **Risk Level Distribution of Sensitive Tables**: displays the distribution of sensitive tables at each sensitivity level, including S3 (high sensitivity), S2 (moderate sensitivity), S1 (low sensitivity), and N/A (unknown sensitivity).
- **Risk Level Distribution of Sensitive Fields**: displays the distribution of sensitive fields at each sensitivity level, including S3 (high sensitivity), S2 (moderate sensitivity), S1 (low sensitivity), and N/A (unknown sensitivity).
- **Data Flow Status**:
  - Displays the dynamic statistics on core data flows in DataHub and Data Integration.
  - Provides a data flowchart. The flowchart dynamically shows data flows and abnormal output. You can click an anomalous event in the flowchart to go to the **Abnormal Data Flow** page.

    You can monitor the data links among different entities, such as data storage services, data transmission services, data stream processing services, external databases, and external files. The data storage services include MaxCompute, AnalyticDB for MySQL, Object Storage Service (OSS), and Tablestore. The data transmission services include DataHub and Data Integration. The data stream processing services include Blink.

10.2.2. Data asset authorization

10.2.2.1. Authorize SDDP to access data assets

Sensitive Data Discovery and Protection (SDDP) must be authorized to access your data assets before it can detect sensitive data in the data assets. Supported data assets include Object Storage Service (OSS) buckets, ApsaraDB RDS instances, PolarDB-X databases, Tablestore instances, self-managed databases hosted on Elastic Compute Service (ECS) instances, MaxCompute projects, AnalyticDB for MySQL clusters, ApsaraDB for OceanBase clusters, and AnalyticDB for PostgreSQL instances. This topic describes how to authorize SDDP to access your data assets.

Context

SDDP can access and scan specific data assets to detect and mask sensitive data only after you grant the required permissions to SDDP.

> **Notice** 已开启授权的OSS Bucket（OSS文件桶）会消耗您的OSS存储容量，已开启授权的数据库或项目会消耗您的数据库和项目数。只有在OSS存储容量、数据库和项目数量充足时，您才可以成功进行相应授权操作。您可以在**云上托管**页面查看剩余的OSS存储容量、数据库和项目数。

For more information about how to authorize SDDP to access supported data assets, see the following sections:

- Authorize SDDP to access OSS buckets
- Authorize SDDP to access ApsaraDB RDS instances
- Authorize SDDP to access PolarDB-X databases
- Authorize SDDP to access Tablestore instances

- Authorize SDDP to access self-managed databases hosted on ECS instances
- Authorize SDDP to access MaxCompute projects
- Authorize SDDP to access AnalyticDB for MySQL clusters or AnalyticDB for PostgreSQL instances
- Authorize SDDP to access ApsaraDB for OceanBase clusters

Authorize SDDP to access OSS buckets

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **OSS** tab, grant the required permissions on instances or buckets.
   - If you want to grant permissions on a single instance or bucket, turn on the switches in the **Identify permissions**, **Desensitization permissions**, **OCR Authority**, and **Audit permissions** columns of the instance or bucket. Then, configure the **Sensitive data sampling** and **Audit log archiving** parameters.

Parameter	Description
Identify permissions	The permissions to detect sensitive data in selected data assets.
Desensitization permissions	The permissions to mask sensitive data in selected data assets.
OCR Authority	The permissions to detect sensitive data in text on images.
Audit permissions	The permissions to audit data in selected data assets.
Sensitive data sampling	The number of sensitive data samples to reserve after SDDP detects sensitive data. If you turn on the switch in **Identify permissions**, you must also specify this parameter. If SDDP detects sensitive data in a data asset, SDDP collects samples of the detected data. You can use the sensitive data samples for further analysis. Valid values: **0**, **5**, and **10**.
Audit log archiving	The duration to retain the audit logs of selected data assets. If you turn on the switch in **Audit permissions**, you must also specify this parameter. Valid values: **30 days**, **90 days**, and **180 days**. **Note** You do not need to activate Log Service to archive the audit logs generated by SDDP.

   - If you want to grant permissions on multiple instances or buckets at the same time, perform the following steps:
     a. Select the required instances or buckets and click **Batch operation**.

b. In the **Batch processing for selected assets** dialog box, turn on the switches of detection, audit, masking, and OCR permissions, and configure the parameters that remain.

c. Click **Ok**.

After SDDP is authorized, SDDP scans the OSS buckets to detect sensitive data. If SDDP scans an OSS bucket for the first time, SDDP automatically performs a full scan.

In the list of OSS buckets on which SDDP has access permissions, you can modify or revoke permissions on the OSS buckets. If you revoke permissions on an OSS bucket, SDDP no longer scans the OSS bucket.

> **Note** SDDP scans only the accessible OSS buckets and analyzes the risks of sensitive data detected in these OSS buckets.

Authorize SDDP to access ApsaraDB RDS instances

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **Cloud hosting** page, click the **RDS** tab.
5. On the **RDS** tab, click **Not authorized**.
6. Find the instance that you want SDDP to access and enter the required database username and its password in the **Username** and **Password** columns.

   You can also click **Batch password import** to import logon information for multiple data assets at a time. For more information, see Import the logon information for multiple data assets at the same time.

   > **Notice** If the username or password is not correct, the authorization fails. Make sure that the information you enter is correct.

7. Select the databases that you want SDDP to access and click **Batch operation**.

   You can also click **One-click authorization** in the Actions column of an instance to grant all its permissions.

8. In the Batch processing for selected assets dialog box, turn on the switches of detection, audit, and masking permissions, and configure the parameters that remain.

Parameter	Description
Identify permissions	The permissions to detect sensitive data in selected data assets.

Parameter	Description
Audit permissions	The permissions to audit data in selected data assets. SDDP allows you to collect audit logs that cover the data generation, update, and use of your data assets. The log information includes the audit rule that is triggered for a data asset, the type of the data asset, the type of the operation that triggers the audit rule, and the operator account. SDDP安全审计功能的使用，请参见Create an audit rule。
Desensitization permissions	The permissions to mask sensitive data in selected data assets.
Sensitive data sampling	The number of sensitive data samples to reserve after SDDP detects sensitive data. If you turn on the switch in **Identify permissions**, you must also specify this parameter. If SDDP detects sensitive data in a data asset, SDDP collects samples of the detected data. You can use the sensitive data samples for further analysis. Valid values: **0**, **5**, and **10**.
Audit log archiving	The duration to retain the audit logs of selected data assets. If you turn on the switch in **Audit permissions**, you must also specify this parameter. Valid values: **30 days**, **90 days**, and **180 days**.

9. Click **Ok**.

   > **Note** If the authorization fails, check whether the username and password are correct.

   After SDDP is authorized, SDDP scans the databases to detect sensitive data.

   In the list of databases on which SDDP has access permissions, you can modify or revoke permissions on the databases. You can modify only the username and password of a valid database account. If you revoke permissions on a database, SDDP no longer scans the database.

Authorize SDDP to access PolarDB-X databases

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **Cloud hosting** page, click the **DRDS** tab.
5. On the **DRDS** tab, click **Not authorized**.
6. Find the instance that you want SDDP to access and enter the required database username and its password in the **Username** and **Password** columns.

   You can also click **Batch password import** to import logon information for multiple data assets at a time. For more information, see Import the logon information for multiple data assets at the same time.

> **Notice** If the username or password is not correct, the authorization fails. Make sure that the information you enter is correct.

7. Select the databases that you want SDDP to access and click **Batch operation**.

   You can also click **One-click authorization** in the Actions column of an instance to grant all its permissions.

8. In the Batch processing for selected assets dialog box, turn on the switches of detection, audit, and masking permissions, and configure the parameters that remain.

Parameter	Description
Identify permissions	The permissions to detect sensitive data in selected data assets.
Audit permissions	The permissions to audit data in selected data assets. SDDP allows you to collect audit logs that cover the data generation, update, and use of your data assets. The log information includes the audit rule that is triggered for a data asset, the type of the data asset, the type of the operation that triggers the audit rule, and the operator account. SDDP安全审计功能的使用，请参见Create an audit rule。
Desensitization permissions	The permissions to mask sensitive data in selected data assets.
Sensitive data sampling	The number of sensitive data samples to reserve after SDDP detects sensitive data. If you turn on the switch in **Identify permissions**, you must also specify this parameter. If SDDP detects sensitive data in a data asset, SDDP collects samples of the detected data. You can use the sensitive data samples for further analysis. Valid values: **0**, **5**, and **10**.
Audit log archiving	The duration to retain the audit logs of selected data assets. If you turn on the switch in **Audit permissions**, you must also specify this parameter. Valid values: **30 days**, **90 days**, and **180 days**.

9. Click **Ok**.

> **Note** If the authorization fails, check whether the username and password are correct.

After SDDP is authorized, SDDP scans the databases to detect sensitive data.

In the list of databases on which SDDP has access permissions, you can modify or revoke permissions on the databases. You can modify only the username and password of a valid database account. If you revoke permissions on a database, SDDP no longer scans the database.

Authorize SDDP to access Tablestore instances

You can authorize SDDP to access one or more Tablestore instances.

1. Log on to Apsara Stack Security Center.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **Cloud hosting** page, click the **OTS** tab.
5. On the **OST** tab, grant the required permissions on instances or buckets.
   - If you want to grant permissions on a single instance or bucket, turn on the switches in the **Identify permissions**, **Desensitization permissions**, and **Audit permissions** columns of the instance or bucket. Then, configure the **Sensitive data sampling** and **Audit log archiving** parameters.

Parameter	Description
Identify permissions	The permissions to detect sensitive data in selected data assets.
Desensitization permissions	The permissions to mask sensitive data in selected data assets.
Audit permissions	The permissions to audit data in selected data assets.
Sensitive data sampling	The number of sensitive data samples to reserve after SDDP detects sensitive data. If you turn on the switch in **Identify permissions**, you must also specify this parameter. If SDDP detects sensitive data in a data asset, SDDP collects samples of the detected data. You can use the sensitive data samples for further analysis. Valid values: **0**, **5**, and **10**.
Audit log archiving	The duration to retain the audit logs of selected data assets. If you turn on the switch in **Audit permissions**, you must also specify this parameter. Valid values: **30 days**, **90 days**, and **180 days**.

   - If you want to grant permissions on multiple instances or buckets at the same time, perform the following steps:
     a. Select the required instances or buckets and click **Batch operation**.
     b. In the **Batch processing for selected assets** dialog box, turn on the switches of detection, audit, and masking permissions, and configure the parameters that remain.
     c. Click **Ok**.

   After SDDP is authorized, SDDP scans the instances to detect sensitive data.

Authorize SDDP to access self-managed databases hosted on ECS instances

A self-managed database hosted on an ECS instance must meet the following requirements before it can be scanned by SDDP:

- The ECS instance resides in a virtual private cloud (VPC).
- The database is a MySQL or SQL Server database.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **Cloud hosting** page, click the **ECS self-built database** tab.
5. On the **ECS self-built database** tab, click **Add data assets**.
6. In the **Asset authorization** dialog box, configure the parameters and click **Next**.

   The following table describes the parameters.

Parameter	Description
Region	The region of the self-managed database that you want to authorize SDDP to access.
ECS instance ID	The ID of the ECS instance on which the self-managed database is hosted.
Database type	The type of the self-managed database that you want to authorize SDDP to access. Valid values: MySQL and SQL Server.
Library name	The name of the self-managed database that you want to authorize SDDP to access. **Note** If you want to authorize SDDP to access other self-managed databases hosted on the same ECS instance, click **Add Database**.
Port	The port number used to connect to the self-managed database.
User name	The username of the account that you use to connect to the self-managed database.
Password	The password of the account that you use to connect to the self-managed database.

7. In the Batch processing for selected assets dialog box, turn on the switches of detection, audit, and masking permissions, and configure the parameters that remain.

Parameter	Description
Identify permissions	The permissions to detect sensitive data in selected data assets.

Parameter	Description
Audit permissions	The permissions to audit data in selected data assets. SDDP allows you to collect audit logs that cover the data generation, update, and use of your data assets. The log information includes the audit rule that is triggered for a data asset, the type of the data asset, the type of the operation that triggers the audit rule, and the operator account. SDDP安全审计功能的使用，请参见Create an audit rule。
Desensitization permissions	The permissions to mask sensitive data in selected data assets.
Sensitive data sampling	The number of sensitive data samples to reserve after SDDP detects sensitive data. If you turn on the switch in **Identify permissions**, you must also specify this parameter. If SDDP detects sensitive data in a data asset, SDDP collects samples of the detected data. You can use the sensitive data samples for further analysis. Valid values: **0**, **5**, and **10**.
Audit log archiving	The duration to retain the audit logs of selected data assets. If you turn on the switch in **Audit permissions**, you must also specify this parameter. Valid values: **30 days**, **90 days**, and **180 days**.

8. Click **Ok**.
   After SDDP is authorized, SDDP scans the databases to detect sensitive data.

Authorize SDDP to access MaxCompute projects

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **Cloud hosting** page, click the **MaxCompute** tab.
5. On the **MaxCompute** tab, grant the required permissions on instances or buckets.
   - If you want to grant permissions on a single instance or bucket, turn on the switches in the **Identify permissions**, **Desensitization permissions**, and **Audit permissions** columns of the instance or bucket. Then, configure the **Sensitive data sampling** and **Audit log archiving** parameters.

Parameter	Description
Identify permissions	The permissions to detect sensitive data in selected data assets.
Desensitization permissions	The permissions to mask sensitive data in selected data assets.

Parameter	Description
Audit permissions	The permissions to audit data in selected data assets.
Sensitive data sampling	The number of sensitive data samples to reserve after SDDP detects sensitive data. If you turn on the switch in **Identify permissions**, you must also specify this parameter. If SDDP detects sensitive data in a data asset, SDDP collects samples of the detected data. You can use the sensitive data samples for further analysis. Valid values: **0**, **5**, and **10**.
Audit log archiving	The duration to retain the audit logs of selected data assets. If you turn on the switch in **Audit permissions**, you must also specify this parameter. Valid values: **30 days**, **90 days**, and **180 days**.

- If you want to grant permissions on multiple instances or buckets at the same time, perform the following steps:
  a. Select the required instances or buckets and click **Batch operation**.
  b. In the **Batch processing for selected assets** dialog box, turn on the switches of detection, audit, and masking permissions, and configure the parameters that remain.

6. Click **Ok**.

> **Note** If the authorization fails, check whether the permission parameters are correctly configured and whether the SDDP account is added to the project.

After SDDP is authorized, SDDP scans the projects to detect sensitive data.

In the list of projects on which SDDP has access permissions, you can revoke permissions on the projects. If you revoke permissions on a project, SDDP no longer scans the project.

Authorize SDDP to access AnalyticDB for MySQL clusters or AnalyticDB for PostgreSQL instances

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **Cloud hosting** page, click the **ADS** or **GPDB** tab.
5. On the ADS or GPDB tab, click **Add data assets**.
6. In the **Add data assets** dialog box, configure the parameters and click **Ok**.

   The following table describes the parameters used to authorize SDDP to access an AnalyticDB for MySQL cluster.

Parameter	Description
Region	The region of the AnalyticDB for MySQL database that you want to authorize SDDP to access.
Instance Name	The name of the cluster to which the AnalyticDB for MySQL database belongs.
Database Name	The name of the AnalyticDB for MySQL database.
User name	The username and password of the account that you use to connect to the AnalyticDB for MySQL database.
Password	
Automatic scanning	The switch of triggering scans on the AnalyticDB for MySQL database each time identification rule settings are modified.

7. On the ADS or GPDB tab, grant the required permissions on multiple instances or buckets at the same time.
   - If you want to grant permissions on a single instance or bucket, turn on the switches in the **Identify permissions**, **Desensitization permissions**, and **Audit permissions** columns of the instance or bucket. Then, configure the **Sensitive data sampling** and **Audit log archiving** parameters.

Parameter	Description
Identify permissions	The permissions to detect sensitive data in selected data assets.
Desensitization permissions	The permissions to mask sensitive data in selected data assets.
Audit permissions	The permissions to audit data in selected data assets.
Sensitive data sampling	The number of sensitive data samples to reserve after SDDP detects sensitive data. If you turn on the switch in **Identify permissions**, you must also specify this parameter. If SDDP detects sensitive data in a data asset, SDDP collects samples of the detected data. You can use the sensitive data samples for further analysis. Valid values: **0**, **5**, and **10**.
Audit log archiving	The duration to retain the audit logs of selected data assets. If you turn on the switch in **Audit permissions**, you must also specify this parameter. Valid values: **30 days**, **90 days**, and **180 days**.

   - If you want to grant permissions on multiple instances or buckets at the same time, perform the following steps:
     a. Select the required instances or buckets and click **Batch operation**.

b. In the **Batch processing for selected assets** dialog box, turn on the switches of detection, audit, and masking permissions, and configure the parameters that remain.

c. Click **Ok**.

After SDDP is authorized, SDDP scans the databases to detect sensitive data.

Authorize SDDP to access ApsaraDB for OceanBase clusters

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **Cloud hosting** page, click the **OceanBase** tab.
5. On the **OceanBase** tab, click **Add data assets**.
6. In the **Add data assets** dialog box, configure the parameters and click **Next**.

   The following table describes the parameters.

Parameter	Description
Region	The region of the ApsaraDB for OceanBase database that you want to authorize SDDP to access.
Database type	The type of the ApsaraDB for OceanBase database. Valid values: MySQL and Oracle.
Cluster Name	The name of the cluster to which the ApsaraDB for OceanBase database belongs.
Tenant Name	The name of the tenant to which the ApsaraDB for OceanBase database belongs.
Database Name	The name of the ApsaraDB for OceanBase database. **Note** If you want to authorize SDDP to access other ApsaraDB for OceanBase databases hosted on the same ECS instance, click **Add Database**.
Link Address	The endpoint that you use to connect to the ApsaraDB for OceanBase database.
User name	The username and password of the account that you use to connect to the ApsaraDB for OceanBase database.
Password	

7. In the Batch processing for selected assets dialog box, turn on the switches of detection, audit, and masking permissions, and configure the parameters that remain.

Parameter	Description
Identify permissions	The permissions to detect sensitive data in selected data assets.
Audit permissions	The permissions to audit data in selected data assets. SDDP allows you to collect audit logs that cover the data generation, update, and use of your data assets. The log information includes the audit rule that is triggered for a data asset, the type of the data asset, the type of the operation that triggers the audit rule, and the operator account. SDDP安全审计功能的使用，请参见Create an audit rule。
Desensitization permissions	The permissions to mask sensitive data in selected data assets.
Sensitive data sampling	The number of sensitive data samples to reserve after SDDP detects sensitive data. If you turn on the switch in **Identify permissions**, you must also specify this parameter. If SDDP detects sensitive data in a data asset, SDDP collects samples of the detected data. You can use the sensitive data samples for further analysis. Valid values: **0**, **5**, and **10**.
Audit log archiving	The duration to retain the audit logs of selected data assets. If you turn on the switch in **Audit permissions**, you must also specify this parameter. Valid values: **30 days**, **90 days**, and **180 days**.

8. Click **Ok**.
   After SDDP is authorized, SDDP scans the databases to detect sensitive data.

Import the logon information for multiple data assets at the same time

SDDP allows you to upload an EXCEL file to import the logon information for multiple data assets, including RDS databases, PolarDB-X databases, and self-managed databases hosted on ECS instances, at the same time to improve authorization efficiency. The following procedure describes how to import the logon information for multiple data assets at the same time:

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Data Asset authorization**.
4. On the **Cloud hosting** page, click **Batch password import** in the upper-right corner.
5. In the **Batch password import** dialog box, click **SDDP Authorization File Template.xlsx**.
6. Open the downloaded file, enter the usernames and passwords used to access each data asset in the **username** and **password** columns, and then save the file.

   If you modify the existing usernames and passwords in the downloaded file and upload the file to

SDDP, the logon information saved in SDDP is updated.

7. In the **Batch password import** dialog box, click **File Upload** to upload the template file that you have edited.
8. Click **Ok**.
   After you upload the Excel file, the usernames and passwords that you enter in the file are synchronized to the **Username** and **Password** columns for the relevant databases on the **RDS**, **DRDS**, and **ECS self-built database** tabs. Then, you can authorize SDDP to access these data assets without the need to manually enter the logon information on the **Cloud hosting** page.

10.2.2.2. Manage usernames and passwords of databases

Sensitive Data Discovery and Protection (SDDP) can detect sensitive data that is stored in a data source only after SDDP is authorized to access the data source. To authorize SDDP to access a data source, you must add the username and password that are used to connect to a database of the data source. This topic describes how to view and add the username and password that are used to connect to a database.

Context

SDDP allows you to manage the usernames and passwords that are used to connect to databases in ApsaraDB RDS and PolarDB-X.

View the username and password of a database

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Authorized account management**.
4. Click the tab that displays the required data source. In this example, click the **RDS** tab.
5. (Optional)Specify filter conditions to search for an ApsaraDB RDS instance.

   > **Note** If you want to view all ApsaraDB RDS instances, skip this step.

Filter condition	Description
Region	The region where the ApsaraDB RDS instance resides.
Instance/Bucket	The name of the ApsaraDB RDS instance.
Database type	The type of the database engine that is run by the ApsaraDB RDS instance. ApsaraDB RDS and PolarDB-X support the MySQL and SQL Server database engines.

6. In the instance list, view the usernames and passwords that are used to connect to the databases of the ApsaraDB RDS instance.

Add the username and password of a database

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data protection authorization > Authorized account management**.
4. Click the tab that displays the required data source. In this example, click the **RDS** tab.
5. Find the ApsaraDB RDS instance and configure the **Username** and **Password** parameters that are used to connect to a database.

   > **Notice** If the username or password is invalid, SDDP fails to be authorized. Make sure that the information that you enter is valid.

6. Click **Add**.
   After the username and password of the database are added, **Status** of the ApsaraDB RDS instance changes to **Added successfully**.

What's next

If you want to change the username or password of a database, find the instance and click **Edit** in the **Actions** column.

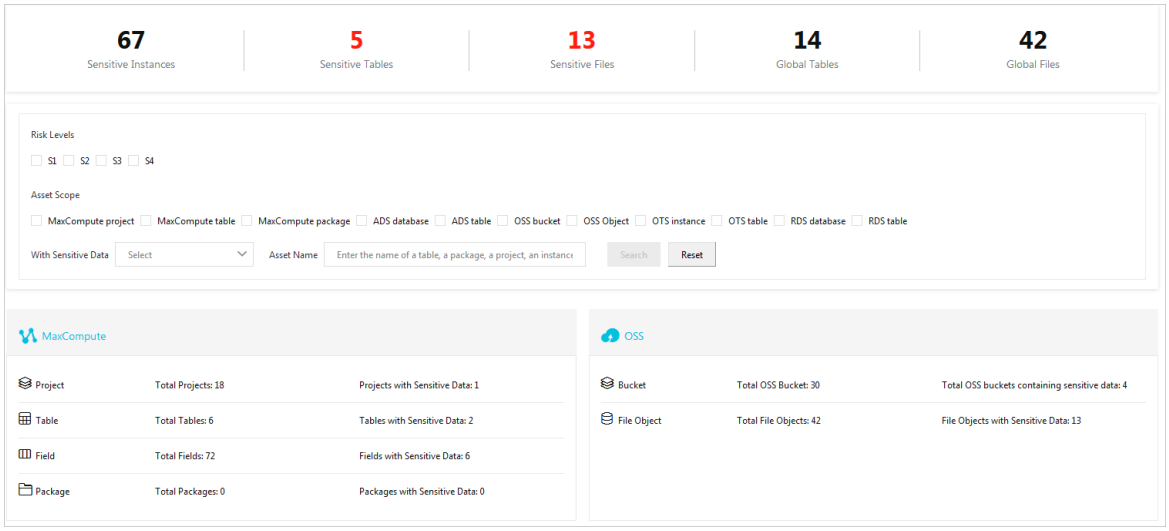
After you change the parameter values,**Save**.

10.2.3. Sensitive data discovery

10.2.3.1. Sensitive data overview

This topic describes the Sensitive Data Overview page that displays the overall security status of your data assets.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Identification > Sensitive Data Overview**.
4. On the **Sensitive Data Overview** page, view the overall security status of sensitive data.



- You can view the overall information about sensitive data. The information includes **Total number of instances**, **Sensitive Tables**, **Sensitive Files**, **Global Tables**, and **Global Files**.
- You can search for sensitive data based on conditions such as the risk level, asset scope, sensitive data type, and asset name.
- You can view the statistics on the access information and sensitive data of cloud services, such as **MaxCompute**, **OSS**, **AnalyticDB for MySQL**, and **Tablestore**, in real time.

10.2.3.2. View statistics on sensitive data

Sensitive Data Discovery and Protection (SDDP) can detect sensitive data in data sources, such as Object Storage Service (OSS) buckets, ApsaraDB RDS instances, and MaxCompute projects. This topic describes how to view statistics on sensitive data that is detected by SDDP.

View statistics on sensitive data detected in OSS

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **OSS** tab, find the OSS bucket whose details you want to view and click **File details** in the Actions column.
5. In the **OSS object query** panel, view the proportions of sensitive objects at each sensitivity level, the top five sensitive data detection rules that are most frequently hit, and the list of objects in which the sensitive data is detected.
   - **Proportions of sensitive objects**

     In the **Proportions of sensitive objects** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of objects at each level.
   - **Top five rules that are most frequently hit**

     In the **Hit Rule Top5** section, you can view the top five sensitive data detection rules that are most frequently hit and the number of times that each rule is hit.

- **List of objects in which the sensitive data is detected**

  In the object list, you can view the information about the objects in which the sensitive data is detected. The information includes the object name, size, type, and number of sensitive fields that are detected in the object. You can click **Hit details** in the Actions column of an object to view the details about the sensitive data detection rules that are hit by the object.

View statistics on sensitive data detected in ApsaraDB RDS

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **RDS** tab.
5. On the **RDS** tab, find the ApsaraDB RDS instance whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.
   - **Proportions of tables**

     In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.
   - **Top five rules that are most frequently hit**

     In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.
   - **List of tables in which the sensitive data is detected**

     In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

View statistics on sensitive data detected in MaxCompute

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **MaxCompute** tab.
5. On the **MaxCompute** tab, find the MaxCompute project whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.

- **Proportions of tables**

  In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.

- **Top five rules that are most frequently hit**

  In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.

- **List of tables in which the sensitive data is detected**

  In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

View statistics on sensitive data detected in self-managed databases that are hosted on ECS instances

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **ECS self-built database** tab.
5. On the **ECS self-built database** tab, find the database instance whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.
   - **Proportions of tables**

     In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.

   - **Top five rules that are most frequently hit**

     In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.

   - **List of tables in which the sensitive data is detected**

     In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

View statistics on sensitive data detected in PolarDB-X

1. Log on to Apsara Stack Security Center.

2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **DRDS** tab.
5. On the **DRDS** tab, find the database instance whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.
   - **Proportions of tables**

     In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.
   - **Top five rules that are most frequently hit**

     In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.
   - **List of tables in which the sensitive data is detected**

     In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

View statistics on sensitive data detected in Tablestore

You can view statistics on sensitive data detected in Tablestore.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **OTS** tab.
5. On the **OTS** tab, find the Tablestore instance whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.
   - **Proportions of tables**

     In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.
   - **Top five rules that are most frequently hit**

In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.

- **List of tables in which the sensitive data is detected**

  In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

View statistics on sensitive data detected in AnalyticDB for PostgreSQL

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **GPDB** tab.
5. On the **GPDB** tab, find the instance whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.
   - **Proportions of tables**

     In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.
   - **Top five rules that are most frequently hit**

     In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.
   - **List of tables in which the sensitive data is detected**

     In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

View statistics on sensitive data detected in AnalyticDB for MySQL

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **ADS** tab.

5. On the **ADS** tab, find the instance whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.
   - **Proportions of tables**

     In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.
   - **Top five rules that are most frequently hit**

     In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.
   - **List of tables in which the sensitive data is detected**

     In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

View statistics on sensitive data detected in DataWorks

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **DataWorks** tab.
5. On the **DataWorks** tab, find the DataWorks workspace whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.
   - **Proportions of tables**

     In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.
   - **Top five rules that are most frequently hit**

     In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.
   - **List of tables in which the sensitive data is detected**

In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

View statistics on sensitive data detected in ApsaraDB for OceanBase

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Sensitive Data Identification > Sensitive data assets** .
4. On the **Sensitive data assets** page, click the **OceanBase** tab.
5. On the **OceanBase** tab, find the instance whose details you want to view and click **Table Details** in the Actions column.
6. In the **Table Query** panel, view the proportions of sensitive tables, the top five sensitive data detection rules that are most frequently hit, and the list of tables in which the sensitive data is detected.
   - **Proportions of tables**

     In the **Proportion of tables** section, you can view the numbers of objects at the following sensitivity level: Highly sensitive, Medium sensitive, Low sensitivity, and Unrecognized. You can also view a pie chart that shows the proportions of tables at each level.
   - **Top five rules that are most frequently hit**

     In the **Hit Rule Top5** section, you can view the top five rules that are most frequently hit and the number of times that each rule is hit.
   - **List of tables in which the sensitive data is detected**

     In the table list, you can view the information about the tables in which the sensitive data is detected. The information includes the table name, total number of rows, total number of fields, number of sensitive fields, and rules that are hit. You can click **Column details** in the Actions column to view the field details, such as the fields that hit sensitive data detection rules and the sensitivity levels of the sensitive fields.

10.2.3.3. Query sensitive data

The Sensitive data search page displays all the sensitive data that is detected in your data assets. You can specify one or more types of sensitive data to query and view the distribution of the sensitive data across your data assets. This topic describes how to query sensitive data.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Identification > Sensitive data search**.

4. On the **Sensitive data search** page, specify filter conditions based on your business requirements.

   Sensitive Data Discovery and Protection (SDDP) provides the following filter conditions:

   - **Hit data**: the type of sensitive data. You can select multiple data types, such as email addresses and mobile phone numbers.
   - **Enter file name to search** or **Enter table name to search**: the name of the object or table in which the sensitive data is detected. Fuzzy match is supported.
   - **Region**: the region where the data assets reside.
   - **Bucket, Instance, or Project**: the name of the bucket, instance, or project in which the sensitive data is detected.

   > **Note** If you specify multiple filter conditions, SDDP returns the sensitive data that meets all the specified filter conditions.

5. Click **Search**.

   In the result list of the **Sensitive data search** page, you can view the information about the objects or tables in which the sensitive data is detected. You can group the objects or sort the tables by using the following methods:

   - **Group objects by sensitivity level**

     On the **OSS-file** tab, set the **Sensitivity level** parameter to S1, S2, or S3 to display the objects that contain sensitive data by sensitivity level.

   - **Sort tables based on the total number of rows or sensitive fields in ascending or descending order**

     On a tab such as the **RDS-table** tab, click the icon to the right of **Total number of rows** or **Sensitive column**. This way, tables that contain sensitive data are sorted based on the total number of rows or sensitive fields in ascending or descending order. The first time you click the icon, the tables are sorted in descending order. The next time you click the icon, the tables are sorted in ascending order.

6. Find the object or table that contains sensitive data. To view the details of sensitive data in an object, click **Details** in the **Operation** column. To view the details of sensitive data in a table, click **Column details** in the **Operation** column.

   In the **Hit query** panel for a bucket or the **Column details** panel for a table, you can view the following details of all the sensitive data that is detected in the object or table:

   - **Column name**: the name of the sensitive field that is detected in the table.

     > **Note** This parameter is displayed only in the **Column details** panel for a table in an ApsaraDB RDS instance, MaxCompute project, self-managed database that is hosted on an Elastic Compute Service (ECS) instance, PolarDB-X database, Tablestore instance, AnalyticDB for MySQL cluster, or AnalyticDB for PostgreSQL instance. This parameter is not displayed in the **Hit query** panel for an OSS bucket.

   - **Hit Rule**: the type and name of the sensitive data detection rule that is hit.
   - **Sensitivity level**: the sensitivity level of the detected sensitive data.
   - **Number of hits**: the number of times that the sensitive data detection rule is hit in the object.

> **Note** This parameter is displayed in the **Hit query** panel for an OSS bucket.

- **Data Sampling**: the samples that are collected from the sensitive data. To configure the **Sensitive data sampling** parameter, perform the following operations: Choose **Security > Data Security > Sensitive Data Discovery and Protection**. Then, choose **Data protection authorization** > Data Asset authorization. On the **Cloud hosting** page, set the Sensitive data sampling parameter to 0, 5, or 10. The number of samples displayed in Data Sampling does not exceed the value of **Sensitive data sampling** that you configure when you authorize SDDP to protect your data assets.

10.2.3.4. Manage scan tasks

Sensitive Data Discovery and Protection (SDDP) automatically scans for sensitive data in the data assets that SDDP is authorized to access. On the Identify task monitoring page, you can view the details of scan tasks for the data assets and rescan the data assets.

Context

SDDP can monitor scan tasks that detect sensitive data in Object Storage Service (OSS), ApsaraDB RDS, MaxCompute, self-managed databases that are hosted on Elastic Compute Service (ECS) instances, PolarDB-X, Tablestore, ApsaraDB for OceanBase, AnalyticDB for MySQL, and AnalyticDB for PostgreSQL.

After you authorize SDDP to access specific data assets, SDDP creates and runs scan tasks for these data assets to detect sensitive data. By default, the **automatic scan** feature is enabled for the scan tasks. This feature allows SDDP to run a full scan on the data assets that SDDP is authorized to access and scan the data that is newly written to or modified in these data assets at an interval of 4 hours. In addition, after you create or modify a sensitive data detection rule, SDDP automatically reruns scan tasks for which the automatic scan feature is enabled.

View the details of scan tasks

On the **Identify task monitoring** page, you can view the details of each scan task. The details include the related data asset, task status, and time when the task is complete. To view the details of scan tasks, perform the following steps:

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Identification > Identification task monitoring**
4. On the Identify task monitoring page, click the tab of the data source for which you want to view scan tasks.
5. (Optional)Select the region, enter the name of the data asset, specify the start and end of the time range to query, and then click **Search**. You can enter the name of a bucket or instance.
6. In the task list, view the details of each scan task. The details include the related data asset, task status, and time when the task is complete.

Rescan your data assets

You can rescan your data assets in the following scenarios:

- If the **automatic scan** feature is not enabled for a scan task, the scan task is not run after the task is

created. In this case, you must rescan your data assets.

- If you enable the **automatic scan** feature for a scan task, SDDP automatically scans the data that is newly written to or modified in the specific data asset at an interval of 4 hours. If you want to immediately scan the specific data asset after you modify the data in the data asset, you can rescan the data asset.

To rescan a data asset for sensitive data, perform the following steps:

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. On the Identify task monitoring page, click the tab of the data source for which you want to rescan data assets.
4. Find the required data asset and click **Rescan** in the **Operation** column.
5. In the **Confirm rescan** dialog box, click **OK**.

   In most cases, the rescan process requires approximately 10 minutes to complete. Wait until the data asset is scanned.

   After the rescan is started, Scan Status of the asset changes to **Scanning** or **Waiting**. The percentage that appears in the **Scan Status** column indicates the progress of the scan task.

What's next

After the scan is complete, Scan Status of the asset changes to **Complete**. If you want to view the latest scan results, you can perform the following operations: In the top navigation bar, choose **Security > Data Security > Sensitive Data Discovery and Protection**. In the left-side navigation pane, choose **Sensitive Data Identification** > Identify task monitoring. Then, click the tab of the data source for which you want to view the scan results.

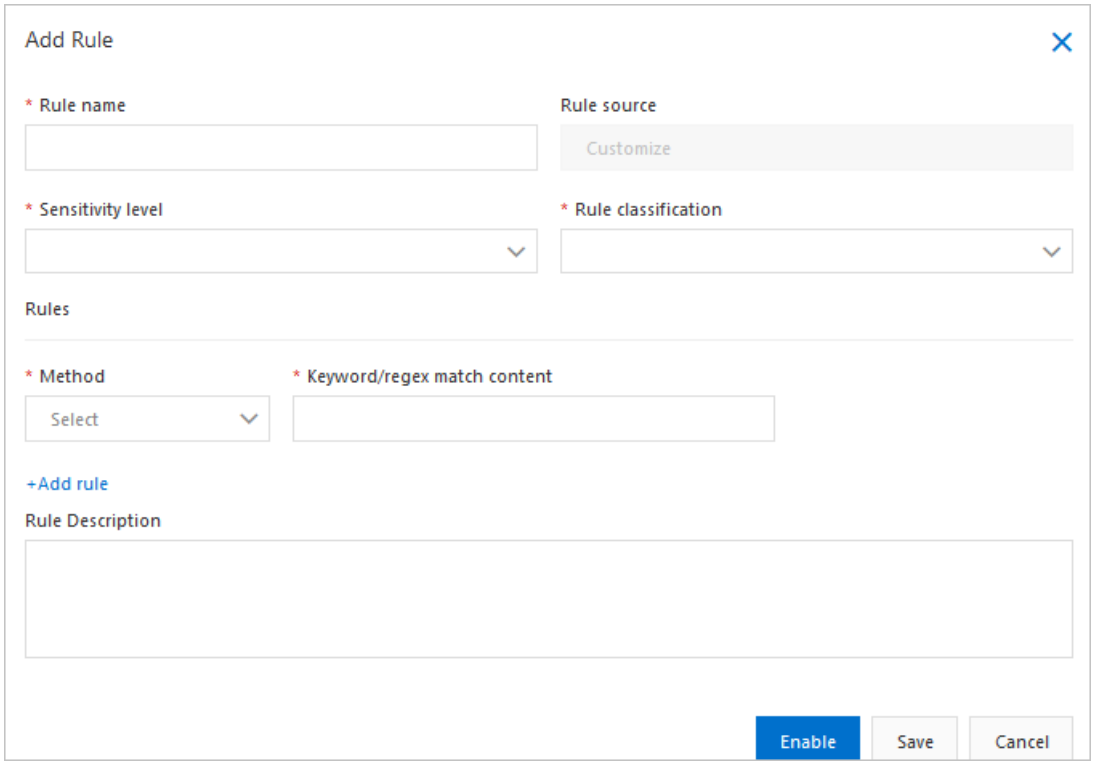
10.2.3.5. Manage detection rules

Sensitive Data Discovery and Protection (SDDP) allows you to customize the detection rules for classifying sensitive data. You can view and configure detection rules to detect sensitive data. This topic describes how to create and manage custom detection rules, view built-in detection rules, and modify sensitivity levels.

Create a custom detection rule

SDDP detects sensitive data in files or tables based on specified rules and generates alerts. You can customize detection rules to detect sensitive data based on your business requirements. To customize a detection rule, perform the following steps:

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Identification > Identification Rules**. On the **Identification Rules** page, click **Add rule**.
4. In the **Add Rule** dialog box, configure parameters.



The following table describes the parameters used to create a custom detection rule.

Parameter	Description
Rule name	The name of the detection rule.
Rule source	The source of the detection rule. The default value is **Customize** and cannot be changed.
Sensitivity level	The sensitivity level for the detection rule. Valid values: ○ **N/A: Public**: non-sensitive ○ **S1: Internal**: low sensitive ○ **S2: Secret**: moderately sensitive ○ **S3: Confidential**: highly sensitive
Rule classification	The class of the sensitive data that the detection rule can detect. Valid values: ○ Personal and sensitive information ○ Device sensitive information ○ Key sensitive information ○ Sensitive picture information ○ Sensitive corporate information ○ Location-sensitive information ○ Universal sensitive information

Parameter	Description
Rules	The content of the detection rule. The content is used to match sensitive fields or text. You must set the **Method** parameter and enter the keyword that is used to detect sensitive data in the **Keyword/regex match content** field. If you want to create a custom detection rule to detect the mobile phone number *1331234*****, you must set the **Method** parameter to **Contains** and enter *1331234***** in the **Keywords/regex match content** field. **Note** The keyword must be a precise value, such as a specific mobile phone number, email address, or ID card number. After a detection rule is created, the detection rule appears in the rule list. However, the rule list does not display the details of the rule. You can click **Details** in the Operation column to view the details of the detection rule.

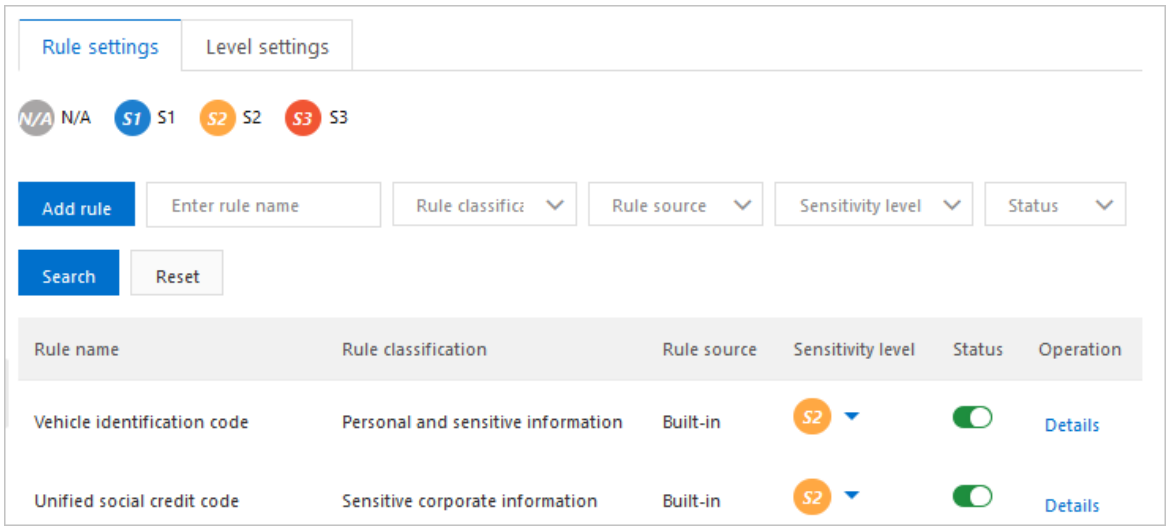
5. Click **Enable** or **Save**.
   - **Enable**: If you click **Enable**, the detection rule is created and enabled. SDDP starts to detect sensitive data based on the detection rule.
   - **Save**: If you click **Save**, the detection rule is created but is not enabled. To enable the detection rule, you must turn on the switch in the Status column for the detection rule in the rule list.

Note
- SDDP detects sensitive data based on all sensitive data detection rules that are enabled.
- A detection rule takes effect after it is created and enabled. If you want to temporarily exclude specific data from sensitive data, you can disable the specific detection rule. After you disable a detection rule, SDDP no longer detects sensitive data based on the detection rule. We recommend that you enable all detection rules to reduce risks.
- You can modify and delete custom detection rules. You can view built-in detection rules but cannot modify or delete them.

View built-in detection rules

The built-in detection rules that SDDP provides apply to various types of common sensitive data, such as mobile phone numbers and ID card numbers. You can view all information about a built-in detection rule, such as the rule type, rule name, and sensitivity level. You cannot view the rule definition. To view built-in detection rules, perform the following steps:

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Identification > Identification Rules**. On the **Identification Rules** page, select **Built-in** from the **Rule source** drop-down list.
4. View built-in detection rules in the list that appears.



You can view the information about each built-in detection rule, such as **Rule name**, **Rule classification**, and **Rule source**.

5. Find a built-in detection rule whose details you want to view and click **Details** in the Operation column.
6. In the **Rule details** dialog box, view the details of the built-in detection rule.

   You can view **Rule name**, **Rule source**, **Rule classification**, and **Sensitivity level** of a built-in detection rule.

Modify a sensitivity level

SDDP allows you to modify the name and description of a sensitivity level. To modify a sensitivity level, perform the following steps:

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Identification > Identification Rules**. On the Identification Rules page, click the **Level settings** tab.
4. Find the sensitivity level that you want to modify and click **Edit** in the Actions column.
5. In the **Sensitivity level** dialog box, modify the information in the Sensitivity level and Description fields.

   By default, SDDP marks sensitive data with the following sensitivity levels: **N/A**, **S1**, **S2**, and **S3**. **N/A** indicates an unknown risk level. The sensitivity levels of S1, S2, and S3 increase in sequence. You can customize the names and descriptions of the four sensitivity levels to classify the sensitive data detected in your data assets based on your business requirements. SDDP provides the following default descriptions for the S1, S2, and S3 levels:

   - **S1**: low risk.

- **S2**: medium risk.
- **S3**: high risk.

6. Click **Ok**.
   The modification immediately takes effect after you submit it. Refresh the **Data Security > Sensitive Data Discovery and Protection > Sensitive Data Identification > Identification Rules** page. You can view the new sensitivity level on the **Level settings** tab.

10.2.3.5.1. View detection rules

Sensitive Data Discovery and Protection (SDDP) allows you to customize detection rules for classifying sensitive data. This topic describes how to view detection rules.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive data discovery > Identification Rules**. On the **Identification Rules** page, click the **Overview** tab.
4. On the **Overview** tab, configure the **Sensitivity level** and **Status** parameters. Then, view the rules that meet the specified conditions.

   You can click **Table** or **Topology** to specify how the rules are displayed. You can also select a sensitive type in the **Sensitive Data** column to filter rules.

   On the **Overview** tab, you can perform the following operations:

   - Switch between templates: Click **Change Template** to go to the **Template Management** tab and switch between templates.
   - Save a new template: Click **Save as New Template** in the upper-left corner of the Overview page to save the detection rules that are displayed as a new template. The new template is displayed on the **Template Management** tab.
   - Change the status of a rule: Turn on or turn off the switch in the **Status** column of a rule to enable or disable the rule. An enabled rule is used first.
   - View the details of a rule: Click **Details** in the **Actions** column of a rule. In the panel that appears, you can view the details of the rule and modify related parameters.
   - Delete a rule: Click **Delete** in the **Actions** column of a rule to delete the rule.

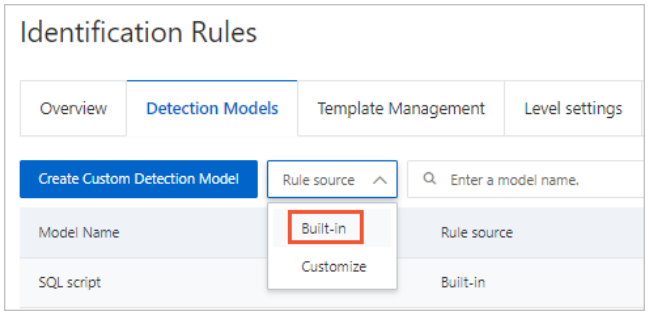
10.2.3.5.2. Manage detection models

Detection models define rules on how to detect sensitive data in your assets. Detection models are classified into custom detection models and built-in detection models. You can use built-in detection models to detect typical sensitive data. This topic describes how to view built-in detection models and how to create, edit, and delete a custom detection model.

View built-in detection models

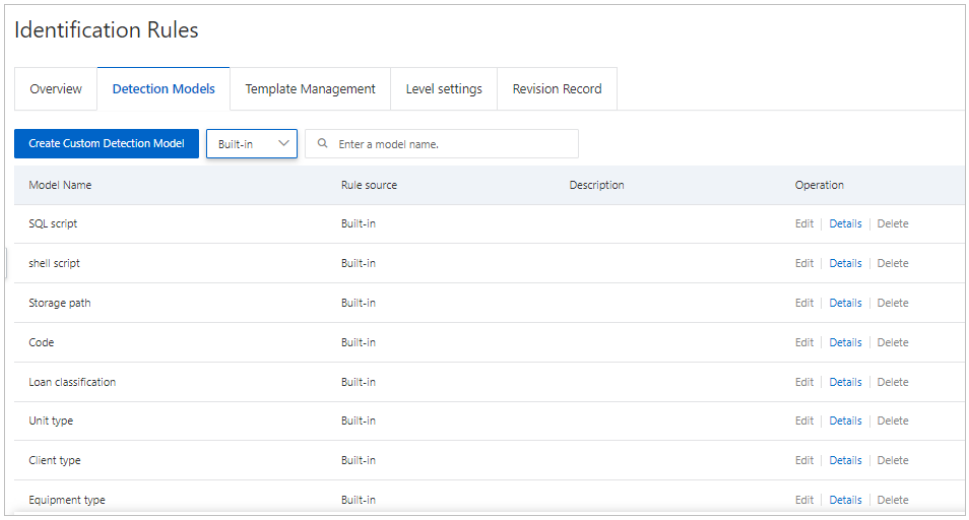
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive data discovery > Identification Rules**.

4. On the **Identification Rules** page, click the **Detection Models** tab.
5. Select **Built-in** from the **Rule source** drop-down list.



6. View the list of built-in detection models.

   You can view the information of built-in detection models, such as the names of the models.

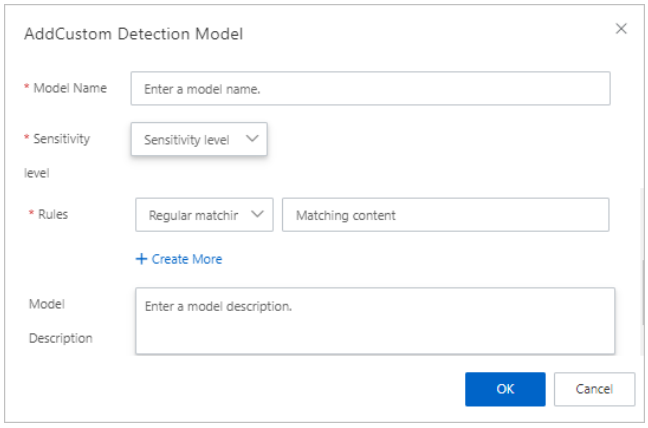


7. Find a built-in detection model and click **Details** in the **Actions** column to view the information of the model.

> **Note** You cannot modify or delete built-in detection models.

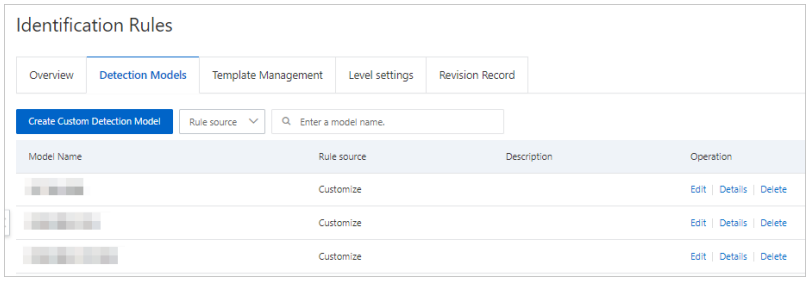
Create a custom detection model

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive data discovery > Identification Rules**.
4. On the **Identification Rules** page, click the **Detection Models** tab.
5. On the **Detection Models** tab, click **Create Custom Detection Model**.
6. In the **AddCustom Detection Model** dialog box, configure the following parameters.



Parameter	Description
Model Name	The name of the custom detection model.
Sensitivity level	The level of the sensitive data that is detected based on the rules in the detection model. Valid values: ○ **S1**: level 1 sensitive data ○ **S2**: level 2 sensitive data ○ **S3**: level 3 sensitive data ○ **S4**: level 4 sensitive data ○ **S5**: level 5 sensitive data
Rules	The rules that are used to detect sensitive data. Valid values: ○ **Does not contain**: detects data that does not contain the specified keyword. ○ **Contains**: detects data that contains the specified keyword. ○ **Regular matching**: uses a regular expression to detect sensitive data. Examples: ■ *Exampleoo+a*: Data such as Exampleooa, Exampleoooa, and Exampleooooooa is detected as sensitive. The plus sign (*+*) indicates one or more repetitions of the preceding character. ■ *Exampleoo*a*: Data such as Exampleoa, Exampleooa, and Exampleooooooa is detected as sensitive. The asterisk (***) indicates zero or more repetitions of the preceding character. ■ *Exampleo?a*: Data such as Examplea and Exampleoa is detected as sensitive. The question mark (*?*) indicates zero or one repetition of the preceding character. You can create multiple detection rules in a detection model. To create multiple detection rules, click **Create More**.
Model Description	The description of the detection model.

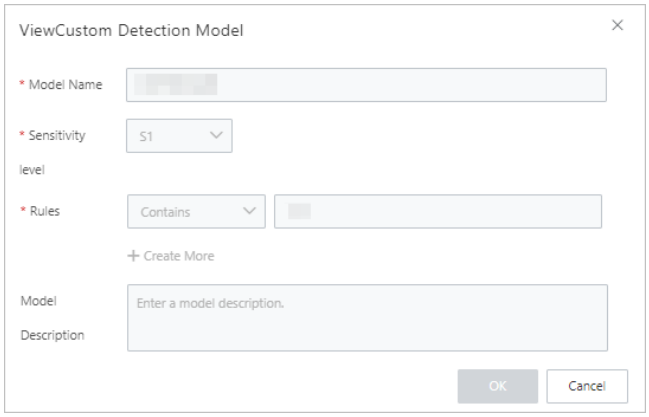
7. Click **OK**.
   After you create the detection model, you can view the model in the model list.



View, edit, and delete a custom detection model

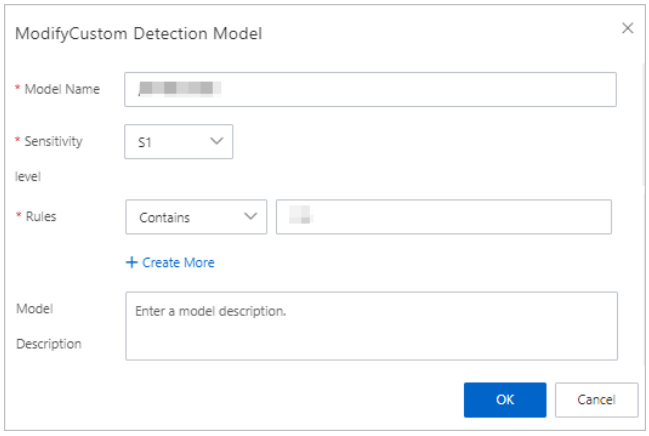
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive data discovery > Identification Rules**.
4. On the **Identification Rules** page, click the **Detection Models** tab.
5. Select **Customize** from the **Rule source** drop-down list.
6. Find the custom detection model that you want to manage and perform the following operations:
   - **View the details of the custom detection model**

     Click **Details** in the Operation column. In the **ViewCustom Detection Model** dialog box, view the details of the custom detection model.

   - **Edit a custom detection model**

     Click **Edit** in the Operation column. In the **ModifyCustom Detection Model** dialog box, modify the parameters and click **OK**.

- **Delete a custom detection model**

  Click **Delete** in the **Operation** column. In the message that appears, click **OK**.

10.2.3.5.3. Manage templates

This topic describes how to enable, view, and copy a template.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive data discovery > Identification Rules**. On the Identification Rules page, click the **Template Management** tab.
4. On the **Template Management** tab, view available templates.
   - Enable a template: Find the template that you want to enable and click **Enable**. If you want to switch between templates, you can also perform this operation. After you perform this operation, all data is scanned, and you cannot switch between templates within 10 minutes.
   - View the details of a template: Find the template whose details you want to view and click **Details**.
   - Copy a template: Find the template that you want to copy and click **Copy**.

10.2.3.5.4. Configure sensitivity levels

This topic describes how to configure the sensitivity levels of sensitive data.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Identification > Identification Rules**. On the Identification Rules page, click the **Level settings** tab.
4. On the **Level settings** tab, click **Create Level** and configure the **Sensitivity level** and Description parameters.

   By default, Sensitive Data Discovery and Protection (SDDP) marks sensitive data with the following sensitivity levels: **N/A** and S1 to S10. **N/A** indicates an unknown sensitivity level. S1 to S10 sensitivity levels indicate sensitivities based on the numbers. A larger number indicates a higher sensitivity. You can customize descriptions for the 11 sensitivity levels to classify the sensitive data detected in your assets based on your business requirements.
5. If you want to modify a sensitivity level, find the sensitivity level and click **Edit** in the **Operation** column.
6. In the **Modify Level** dialog box, modify the description of the sensitivity level.
7. Click **OK**.

10.2.4. Check data permissions

10.2.4.1. View permission statistics

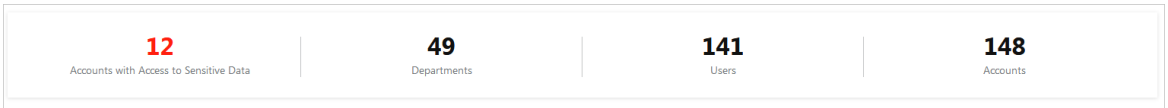
This topic describes how to view permission statistics.

Context

On the Permission Management page, you can view the overall permission distribution of Apsara Stack. You can also identify vulnerable accounts and users, and troubleshoot and handle security issues at your earliest opportunity.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data Permissions > Permission Management**.
4. View the overall permission statistics.

   - **Accounts with Access to Sensitive Data**: the number of accounts that can access sensitive data.
   - **Departments**: the number of departments in Apsara Stack.
   - **Users**: the number of users in Apsara Stack.
   - **Accounts**: the number of accounts in Apsara Stack.
5. View the department-level permission statistics.

   You can view the statistics on the users, accounts, and anomalous events that are related to permissions for each department.

10.2.4.2. View the permissions of an account

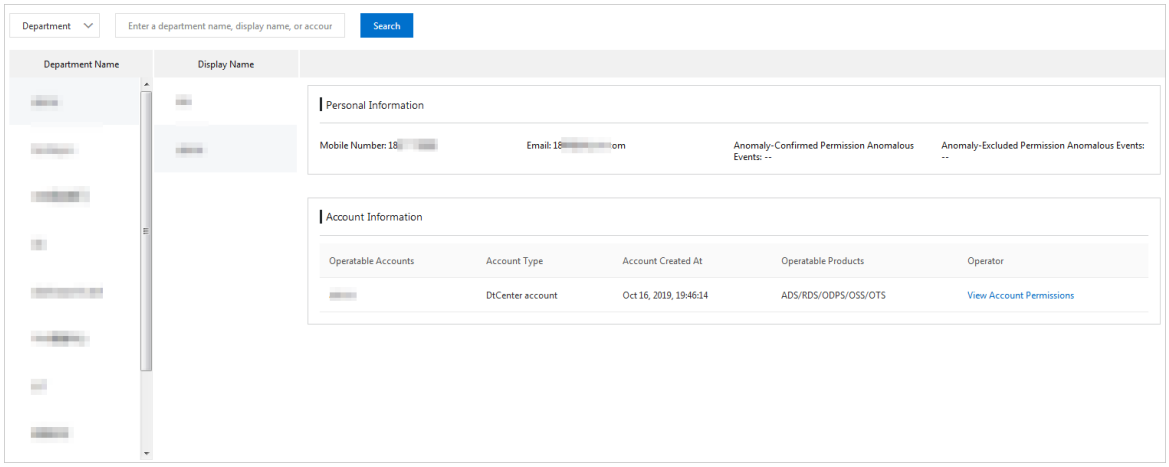
This topic describes how to view the permissions of an account.

Context

You can search for an account and view its information. This way, you can quickly find the owner of sensitive data.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Data Security** section, click **Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data Permissions > Permission Search**.



4. Search for a specific account.

   To search for an account, perform the following steps:

   i. Select **Department** or **Employee** from the drop-down list.

   ii. Enter a keyword, such as a department name or an account.

   iii. Click **Search**. You can view the search results in the **Display Name** column.

   > **Note** You can also click a department in the Department Name column. All accounts of the department are displayed in the Display Name column.

5. In the **Display Name** column, click the account whose details you want to view.
6. View information in the **Personal Information** and **Account Information** sections on the right.
   - **Personal Information**

     You can view the contact information about the account owner. You can also view the numbers of confirmed anomalous events that are related to permission access and excluded anomalous events that are related to permission access.
   - **Account Information**

     You can view the accounts that the owner can use and the details of each account. The details include the account type, time when the accounts are created, and Apsara Stack services that the accounts can access.

     You can click **View Account Permissions** in the Actions column of an account to view the resources, resource types, resource paths, and operation permissions.

10.2.5. Monitor data flows

10.2.5.1. View data flows in DataHub

This topic describes how to view data flows in DataHub.

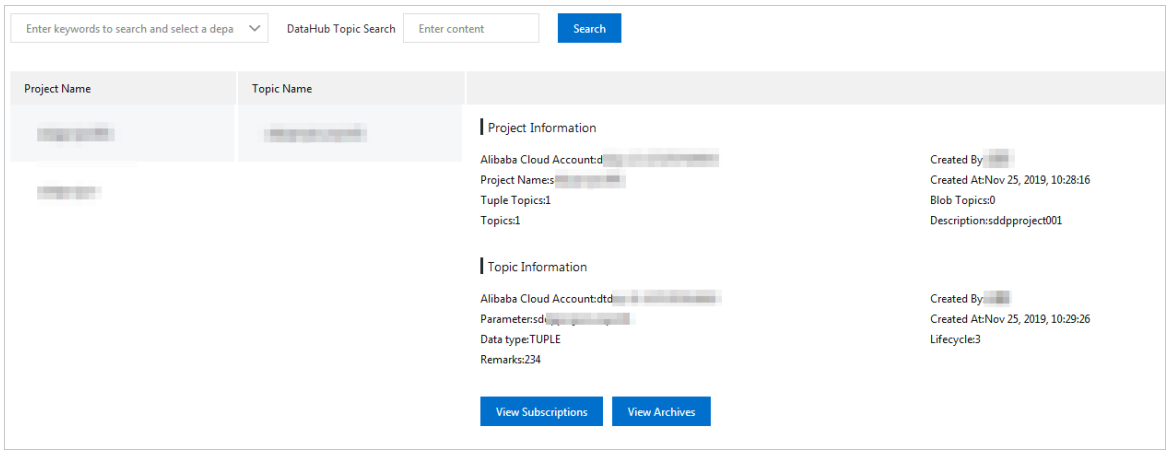
Context

DataHub is a platform that is designed to process streaming data. You can publish and subscribe to streaming data in DataHub. You can also distribute the data to other platforms. DataHub allows you to analyze streaming data and build applications based on the streaming data.

On the **DataHub** page, you can view the details of data flows in DataHub. The details include the relationships between DataHub projects and topics, and the relationships among topics, subscribed applications, and archive sources.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, choose **Security > Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane of the Sensitive Data Discovery and Protection page, choose **Data Flow Monitoring > DataHub**.
4. In the search box, enter a keyword and select a department from the drop-down list. Enter a topic keyword in the **DataHub Topic Search** field and click **Search**.



> **Note**
>
> You can also click the required project in the **Project Name** column and click the required topic in the **Topic Name** column.

In the **Project Information** and **Topic Information** sections, you can view the information about the project and the topic.

- **Project Information**

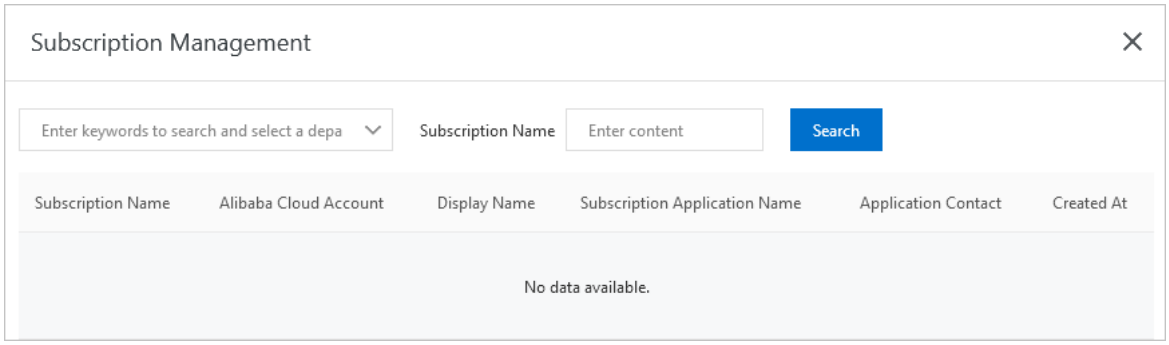
  Displays information such as the project name, Apsara Stack account, creator, creation time, and number of topics.

- **Topic Information**

  Displays information such as the topic name, Apsara Stack account, creator, creation time, and topic type.

5. Click **View Subscriptions** to view the subscription list.

   The subscription list provides information such as the subscription name, Apsara Stack account of the creator, display name, name of the subscribed application, and contact for the application.



i. Enter a keyword and select a department from the drop-down list.
ii. In the **Subscription Name** field, enter a keyword.
iii. Click **Search** to search for the required DataHub topic.

6. Click **View Archives** to view the archive list.

   The archive list provides information such as the name of the connected instance, Apsara Stack account of the creator, display name, source service, resource path, and risk level.

   i. Enter a keyword and select a department from the drop-down list.
   ii. In the **Instance Name** field, enter a keyword.
   iii. Click **Search** to search for the required instance.

10.2.6. Sensitive data masking

10.2.6.1. Create a static masking task

This topic describes how to create a static masking task and run the task to mask sensitive data.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Desensitization > Static Desensitization**.
4. In the upper-right corner of the **Desensitization task configuration** tab, click **Add Desensitization Task**.
5. On the **Add Desensitization Task** page, configure parameters.
   i. In the **Basic Task Information** step, configure **Task Name** and **Task notes**. Then, click **Next**.
   ii. In the **Desensitization Source Configuration** step, specify the source of data that you want to mask and click **Next**.

   You can use Sensitive Data Discovery and Protection (SDDP) to create masking tasks for different data sources, including tables in ApsaraDB RDS, MaxCompute, and ApsaraDB for OceanBase, and objects in Object Storage Service (OSS). The following table describes the parameters used to create a masking task for each data source.

Data source	Parameter	Description
MaxCompute	**Types of data storage**	Select **RDS Table / DRDS Table / MaxCompute Table / PolarDB Table / ADS-Table / OceanBase Table**.
	Source Product	Select **MaxCompute**.
	Source Database/Project	Select the source database or project whose data you want to mask from the drop-down list.
	Source table name	Select the source table whose data you want to mask from the drop-down list.
	Source Partition	Enter the name of the source partition whose data you want to mask. You can configure partitions when you create a MaxCompute table. Partitions define different logical divisions of a table. When you query data, you can specify partitions to improve query efficiency. **Note** **Source Partition** is optional. If you leave this parameter unspecified, SDDP masks sensitive data in all partitions of the source table.
ApsaraDB RDS, PolarDB-X, and ApsaraDB for OceanBase	**Types of data storage**	Select **RDS Table / DRDS Table / MaxCompute Table / PolarDB Table / ADS-Table / OceanBase Table**.
	Source Product	Select **RDS**, **DRDS**, or **OceanBase**.
	Source Database/Project	Select the source database or project whose data you want to mask from the drop-down list.
	Source table name	Select the source table whose data you want to mask from the drop-down list.
	Sample SQL	Optional. Enter an SQL statement and specify the data that you want to mask.
AnalyticDB for MySQL and PolarDB	**Source Type**	Select **RDS Table / DRDS Table / MaxCompute Table / PolarDB Table / ADS-Table / OceanBase Table**.
	Source Product	Select **ADS** or **PolarDB**.
	Source Database/Project	Select the source project whose data you want to mask from the drop-down list.

Data source	Parameter	Description
	Source table name	Select the source table whose data you want to mask from the drop-down list.
OSS	**Types of data storage**	Select **OSS files**.
	File source	Upload a file from your computer or select a bucket. Valid values: ■ **Uploaded Local File**: If you select this option, click **Select a local file** and select a source file from your computer. ■ **OSS Bucket**: If you select this option, select the OSS bucket to which the source object belongs.
	Source file description	Enter an informative description for the source file to help identify the task. **Note** This parameter is required only when you set **File source** to **Uploaded Local File**.
	OSS Bucket where the source file is located	Select the OSS bucket to which the source object belongs. **Note** This parameter is required only when you set **File source** to **OSS Bucket**.
	Source file names	Optional. Enter the name of the source object. **Note** This parameter is required only when you set **File source** to **OSS Bucket**. If you want to use wildcards to specify objects, turn on **Open the pass**. After you turn on Open the pass, you can use asterisks (*) as wildcards to specify multiple OSS objects at a time. However, you can use asterisks only in object names. For example, enter test*.xls. After you specify an object name by using an asterisk, SDDP masks the data of the matched objects. Make sure that these objects use the same column structure.
	Separator selection	Optional. Select a column delimiter based on the format of the object that you specify. This parameter is required for objects in the CSV or TXT format. Valid values: ■ **Semicolon ";" (MacOS/Linux default)** ■ **Comma "," (Windows default)**

Data source	Parameter	Description
	Table contains header rows	Optional. Specify whether the data to be masked contains header rows.

iii. In the **Desensitization algorithm** step, specify the algorithm to mask data and click **Next**.

In this step, you must specify the algorithm type, select an algorithm, and turn on the masking switch for the source field of data that you want to mask.

iv. (Optional)In the **Data Watermark** step, turn on **Open data watermark**. Specify the following parameters: Please select the field to embed the watermark, Please select a watermark algorithm, and Please enter watermark information. Then, click **Next**.

The Please select a watermark algorithm parameter has the following values:

- **Space Algorithm**: If you want to add watermarks for fields of a string type, select this value.
- **Modify the least significant bit algorithm**: If you want to add watermarks for fields of a numeric type, select this value.

v. In the **Destination Location Configuration** step, specify the destination table to store the data after masking, test and make sure that you have write permissions on the destination table, and then click **Next**. The parameters for the destination table include **Types of data storage** and **Target**.

vi. In the **Confirm Process Logic** step, configure the processing logic of the task.

Parameter	Description
How the task is triggered	Select a method to run the masking task. Valid values: ■ **Manual Only**: You must manually run the masking task on the Static Desensitization page. ■ **Scheduled Only**: The masking task is automatically run at a specific point in time on an hourly, daily, or monthly basis. ■ **Manual + Scheduled**: You can manually run the masking task or enable automatic running of the masking task at a specific point in time on an hourly, daily, or monthly basis.
Turn on incremental desensitization	Optional. Enable incremental masking based on your business requirements. If you turn on this switch, SDDP masks only the data that is added after the last masking task is completed. You must specify a field whose value is increased over time as the incremental identifier. For example, you can specify the creation time field or the auto-increment ID field as the incremental identifier. **Note** SDDP supports incremental masking only for data in ApsaraDB RDS.

Parameter	Description
Shard field	Optional. Select a field based on which SDDP divides the source data into multiple shards and concurrently masks the data in these shards. In this case, data masking is more efficient. You can specify one or more shard fields based on your business requirements. **Note** ■ SDDP supports incremental masking only for data in ApsaraDB RDS. We recommend that you use a primary key or a field on which a unique index is created as the shard field. ■ If you leave this parameter unspecified, a primary key is used as the shard field. SDDP divides the source data based on the primary key and masks the data. If the source data does not have a primary key, you must specify a shard field. Otherwise, the masking task fails. ■ If you specify excessive shard fields, query performance and data accuracy may deteriorate. Proceed with caution.
Table name conflict resolution	Select a method to handle a table name conflict. Valid values: ■ **Delete the target table and create a new table with the same name** ■ **Attach data to the target table**: This method is recommended.
Row Conflict Resolution	Select a method to handle a row conflict. Valid values: ■ **Keep conflicting rows in the target table and discard the new data**: This method is recommended. ■ **Delete conflicting rows in the target table and insert the new data**

vii. Click **Submit**.

After you create the masking task, you can view the task in the list of masking tasks on the **Desensitization task configuration** tab.

6. In the list of masking tasks, turn on the switch and run the masking task.
7. On the **Task Execution Status** tab, view **Execution Progress** and **Status** of the masking task.

10.2.6.2. View dynamic data masking tasks

Sensitive Data Discovery and Protection (SDDP) provides the dynamic data masking feature. You can call the ExecDatamask operation to dynamically mask sensitive data.

Context

When you call this operation, you must specify the ID of the data masking template to use. Static data masking and dynamic data masking can use the same template. To obtain the template ID, perform the following operations: Log on to Apsara Stack Security Center. In the top navigation bar, choose **Security > Data Security > Sensitive Data Discovery and Protection**. In the left-side navigation pane, choose **Sensitive Data Desensitization** > Desensitization Template. You can also create custom data masking templates. For more information, see Create a data masking template.

Limits

Before you can call the ExecDatamask operation to dynamically mask sensitive data, make sure that the size of the sensitive data is less than 2 MB. The `Data` parameter specifies the size.

View the call history of the ExecDatamask operation

Log on to Apsara Stack Security Center. In the top navigation bar, choose **Security > Data Security > Sensitive Data Discovery and Protection**. In the left-side navigation pane, choose **Sensitive Data Desensitization** > Dynamic desensitization. On the page that appears, you can view the call history of the ExecDatamask operation. Each record includes the name of the operation, the UID of the Apsara Stack tenant account or RAM user that called the operation, the IP address from which the call is initiated, the points in time at which the operation was first and last called, and the total number of calls.

Note Only one record is generated for calls that are initiated by the same Apsara Stack tenant account or RAM user from the same IP address. In this case, the cumulative number of calls is recorded.

10.2.6.3. Create a data masking template

Sensitive Data Discovery and Protection (SDDP) allows you to create data masking templates. You can create a data masking template and add data masking algorithms that are frequently used in the same scenario to the template. This avoids repeated configuration of data masking algorithms and makes sensitive data processing more efficient. This topic describes how to create and manage data masking templates.

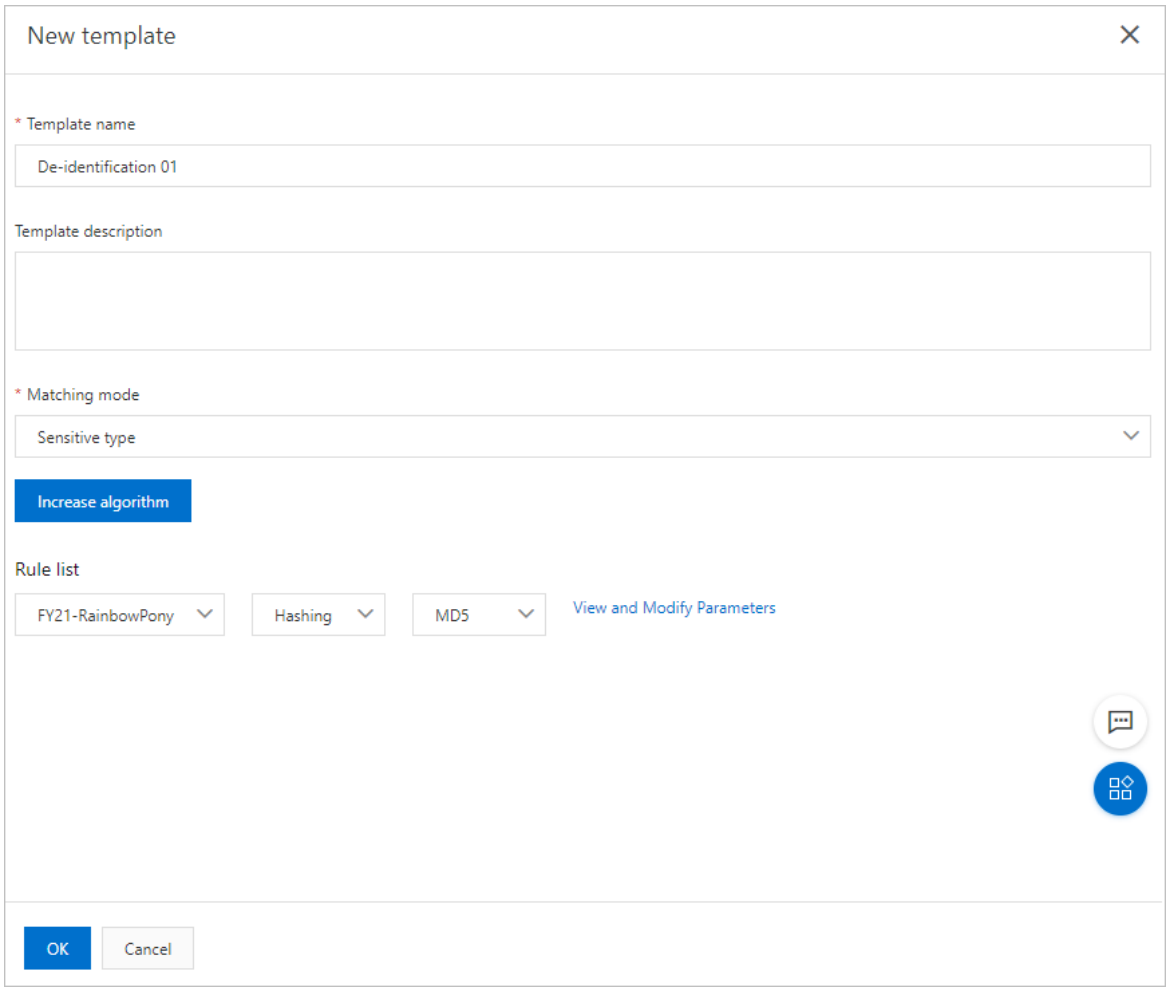
Create a data masking template

You can create an unlimited number of data masking templates.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security >**

Sensitive Data Discovery and Protection.

3. In the left-side navigation pane, choose **Sensitive Data Desensitization > Desensitization Template**.
4. On the **Desensitization Template** page, click **New template**.
5. In the **New template** panel, configure the following parameters.



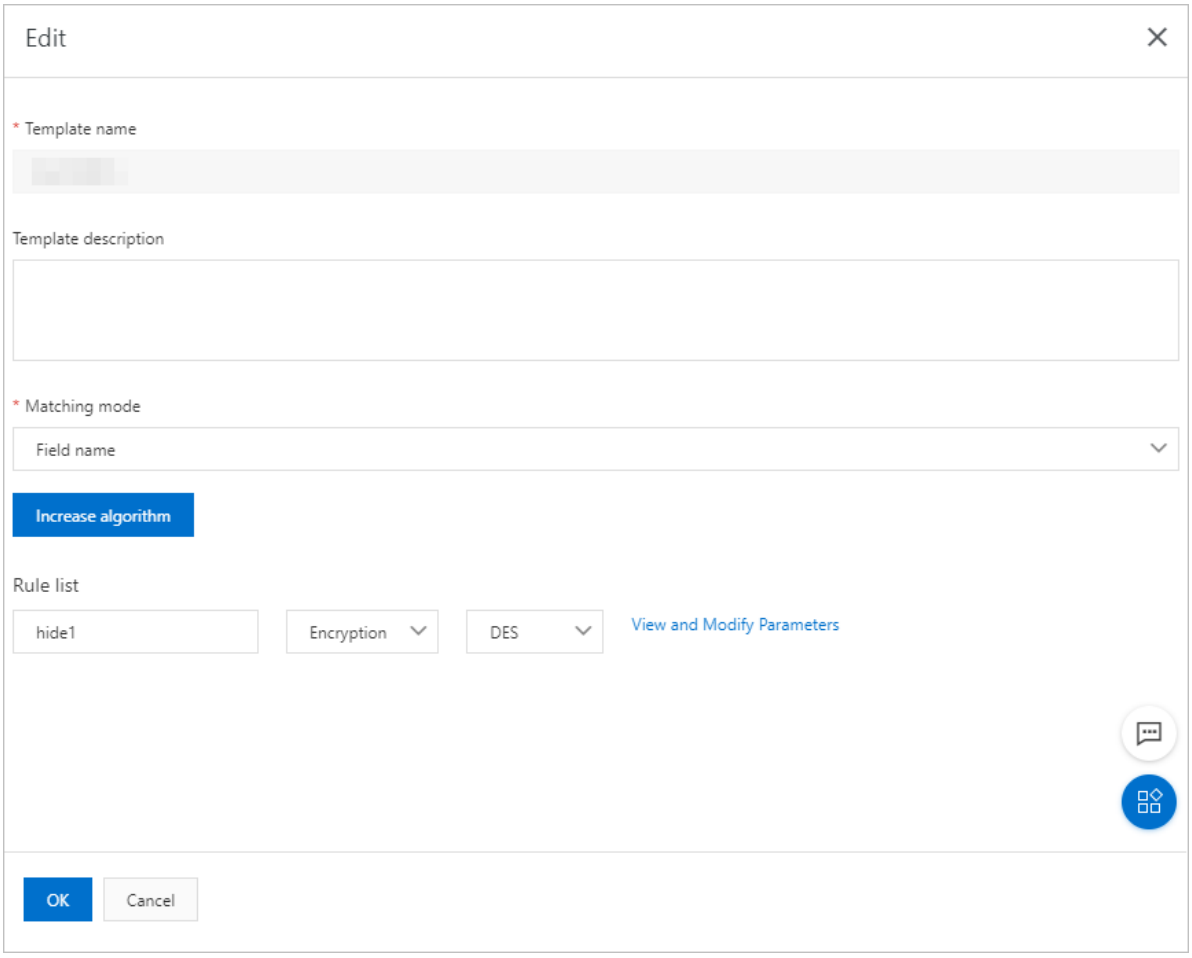
Parameter	Description
Template name	The name of the data masking template.
Template description	The description of the data masking template. You can enter information such as the scenario to which the template is applied.
Matching mode	The mode in which the data masking template handles its matched sensitive data. Valid values: ○ **Sensitive type**: If you select this option, select the types of sensitive data that you want to mask and the data masking algorithm for each type of sensitive data. The types of sensitive data include vehicle identification numbers and unified social credit codes. ○ **Field name**: If you select this option, specify the fields that you want to mask and the data masking algorithm for each field.

Parameter	Description
Rule list	The rules that are used to mask sensitive data. To configure a rule, select a sensitive data type or enter a field that you want to mask and specify a data masking algorithm. SDDP supports the following data masking algorithms: ○ Hashing ○ Redaction ○ Substitution ○ Rounding ○ Encryption ○ Shuffling ○ Data decryption For more information, see Configure data masking algorithms. You can configure multiple rules in a template. To configure more rules, click **Increase algorithm**.

Manage data masking templates

- **Edit a data masking template**

  To edit a data masking template, find the template on the **Desensitization Template** page and click **Edit** in the Actions column. In the **Edit** panel, modify the description or rules of the data masking template.



- **Delete a data masking template**

  To delete a data masking template that you no longer use, find the template on the **Desensitization Template** page and click **Delete** in the Actions column.

  > **Note** If you delete a data masking template, it cannot be restored. Proceed with caution.

10.2.6.4. Configure data masking algorithms

This topic describes how to configure data masking algorithms.

Context

The following table describes the data masking algorithms that are supported by Sensitive Data Discovery and Protection (SDDP).

Category	Description	Algorithm	Input	Suitable sensitive data and scenario

Category	Description	Algorithm	Input	Suitable sensitive data and scenario
Hashing	This type of algorithm is irreversible. This type of algorithm is suitable for password masking and the scenarios in which you must check whether data is sensitive by comparison. You can use common hashing algorithms and specify a salt value.	MD5	Salt value	• Sensitive data: keys • Scenario: data storage
		SHA-1	Salt value	
		SHA-256	Salt value	
		HMAC	Salt value	

Redaction by using asterisks (*) or number signs (#)	This type of algorithm is irreversible.
	This type of algorithm is suitable for the scenarios in which you need to show sensitive data on a GUI or share sensitive data.
	This type of algorithm masks specific content in sensitive data by using asterisks (*) or number signs (#).
		Keeps the first N characters and the last M characters	Values of N and M	• Sensitive data: sensitive personal information
				• Scenarios:
				  ○ Data usage
				  ○ Data sharing

		Keeps characters from the Xth position to the Yth position	Values of X and Y	
		Masks the first N characters and the last M characters	Values of N and M	
		Masks characters from the Xth position to the Yth position	Values of X and Y	
		Masks characters that precede a special character when the special character appears for the first time	At sign (@), ampersand (&), or period (.)	
		Masks characters that follow a special character when the special character appears for the first time	At sign (@), ampersand (&), or period (.)	
		Substitutes specific content in ID card	Mapping table for randomly	

Category	Description	Algorithm	Applicable values	Suitable sensitive data and scenario
Substitution (custom	Some of the algorithms are reversible. This type of algorithm can be used to mask fields in fixed formats. For example, you can use the algorithms to mask ID card numbers.	Randomly substitutes specific content in ID card numbers	Mapping table for randomly substituting IDs of administrative regions	• Sensitive data: ◦ Sensitive personal information ◦ Sensitive information of enterprises
		Randomly substitutes specific content in IDs of military officer cards	Mapping table for randomly substituting type codes	
		Randomly substitutes specified content in passport numbers	Mapping table for randomly substituting purpose fields	
		Randomly substitutes specific content in permit numbers of Exit-Entry Permit for Travelling to and from Hong Kong and Macao	Mapping table for randomly substituting purpose fields	
		Randomly substitutes specific content in bank card numbers	Mapping table for randomly substituting bank identification numbers (BINs)	
		Randomly substitutes specific content in landline telephone numbers	Mapping table for randomly substituting IDs of administrative regions	
		Randomly substitutes specific content in mobile phone numbers	Mapping table for randomly substituting mobile network codes	

ization Category supported)	This type of algorithm substitutes the	Algorithm	Input	Suitable sensitive data and scenario ◦ Sensitive information of devices
	entire value or a part of the value of a field with a mapped value by using a mapping table. In this case, data masking is reversible. This type of algorithm also substitutes the entire value or a part of the value of a field randomly based on a random interval. In this case, data masking is irreversible. SDDP provides multiple built-in mapping tables and allows you to customize substitution algorithms.	Randomly substitutes specific content in unified social credit codes	Mapping table for randomly substituting IDs of registration authorities, mapping table for randomly substituting type codes, and mapping table for randomly substituting IDs of administrative regions	• Scenarios: ◦ Data storage ◦ Data sharing
		Substitutes specific content in general tables with mapped values	Mapping table for substituting uppercase letters, mapping table for substituting lowercase letters, mapping table for substituting digits, and mapping table for substituting special characters	
		Randomly substitutes specific content in general tables	Mapping table for randomly substituting uppercase letters, mapping table for randomly substituting lowercase letters, mapping table for randomly substituting digits, and mapping table for randomly substituting special characters	

Category	Description	Algorithm	Input	Suitable sensitive data and scenario
Rounding	Some of the algorithms are reversible. This type of algorithm can be used to analyze and collect statistics on sensitive datasets. SDDP provides two types of rounding algorithms. One algorithm rounds numbers and dates, which is irreversible. The other algorithm bit-shifts text, which is reversible.	Rounds down a number to the Nth digit before the decimal point	N	• Sensitive data: general sensitive information • Scenarios: ◦ Data storage ◦ Data usage
		Rounds dates	Date rounding level	
		Shifts characters	Number of places by which specific bits are moved and shift direction (left or right)	
Encryption	This type of algorithm is reversible. This type of algorithm can be used to encrypt sensitive fields that need to be retrieved after encryption. Common symmetrical encryption algorithms are supported.	Data Encryption Standard (DES) algorithm	Encryption key	• Sensitive data: ◦ Sensitive personal information ◦ Sensitive information of enterprises • Scenario: data storage
		Triple Data Encryption Standard (3DES) algorithm	Encryption key	
		Advanced Encryption Standard (AES) algorithm	Encryption key	

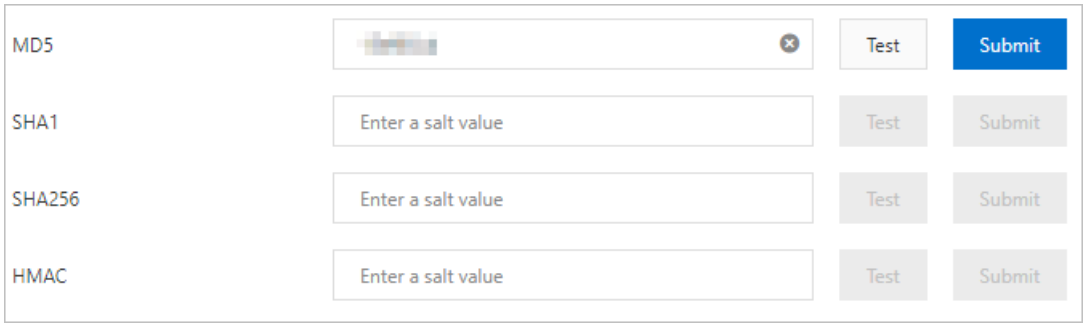
Category	Description	Algorithm	Input	Suitable sensitive data and scenario

Shuffling	This type of algorithm is irreversible.
	This type of algorithm can be used to mask structured data columns.
	This type of algorithm extracts values of a field in a specified range from the source table and rearranges the values in a specific column. Alternatively, this type of algorithm randomly selects values from a specific column within the value range and rearranges the selected values. This way, the values are mixed up and masked.
		Randomly shuffles data	Rearranged values or randomly selected values	• Sensitive data:
				  ◦ Sensitive information of devices
				  ◦ Location-sensitive information
				• Scenario: data storage

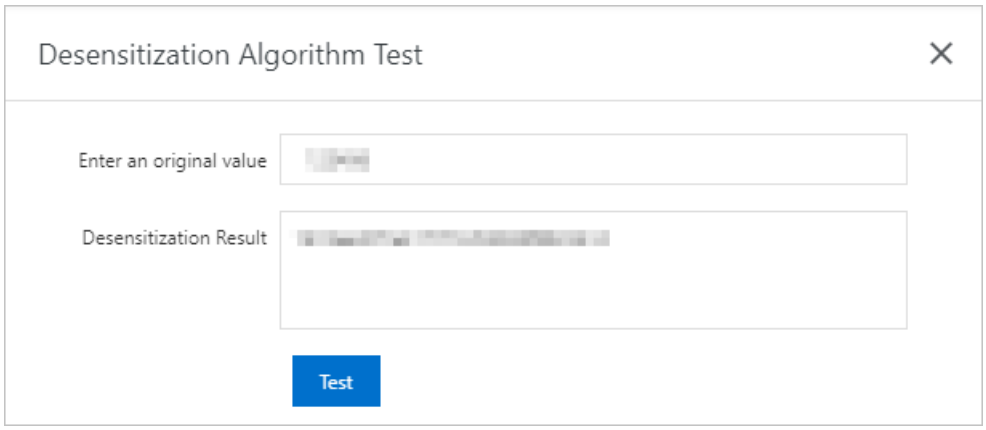
Hashing

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Desensitization > Desensitization algorithm**. On the **Desensitization algorithm** page, click the **Hashing** tab.
4. Specify a salt value for each algorithm.

> **Note** In cryptography, you can insert a specific string to a fixed position of a password to generate a hash value that is different from that of the original password. This process is called salting.
>
> A salt value is the specific string that you insert.



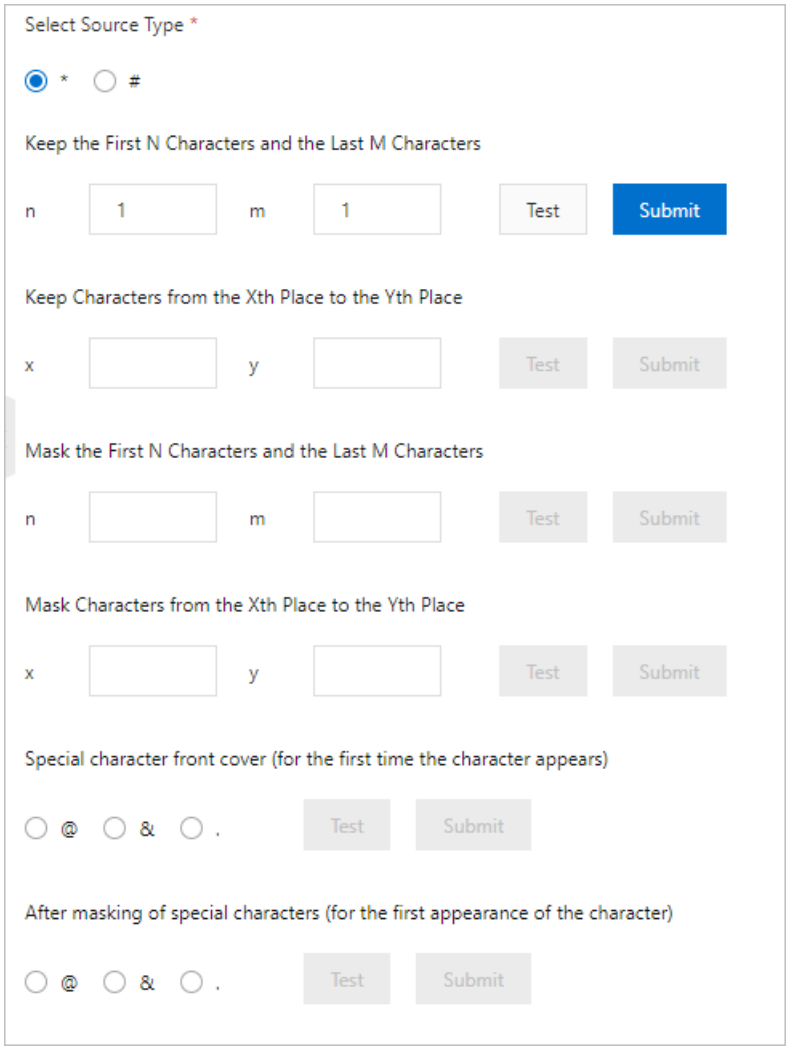
5. In the **Desensitization Algorithm Test** panel, enter the original value and click **Test** to check whether the algorithm works.



6. After the test is complete, click **Submit**.

Redaction

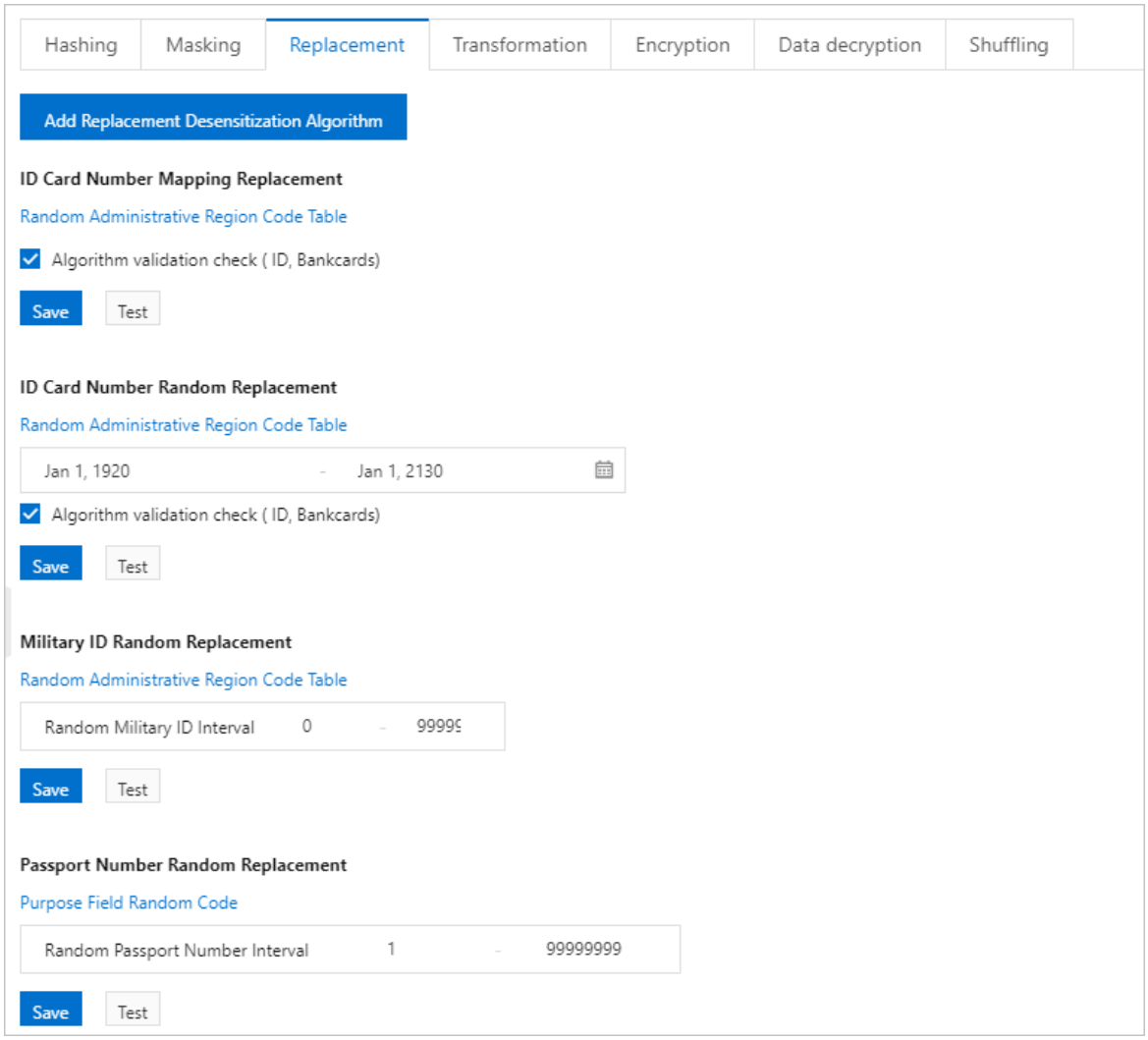
1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Desensitization > Desensitization algorithm**. On the **Desensitization algorithm** page, click the **Masking** tab.
4. Configure the parameters.



5. In the **Desensitization Algorithm Test** panel, enter the original value and click **Test** to check whether the algorithm works.
6. After the test is complete, click **Submit**.

Substitution

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Desensitization > Desensitization algorithm**. On the **Desensitization algorithm** page, click the **Replacement** tab.
4. Configure the parameters.



Note By default, SDDP provides multiple common substitution algorithms, such as ID Card Number Mapping Replacement and Telephone Number Random Replacement.

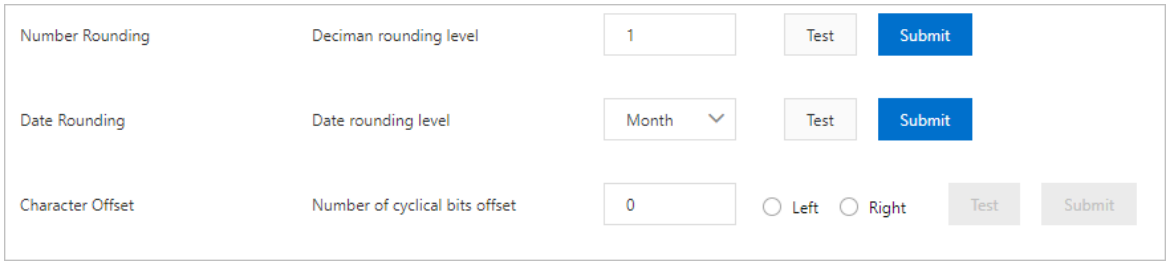
- If you want to customize a mapping table, click the required mapping table, replace the original content with your own mapping table, and then click **Save**.
- If you want to customize an algorithm, click **Add Replacement Desensitization Algorithm** and specify the interval and mapping table.

5. In the **Desensitization Algorithm Test** panel, enter the original value and click **Test** to check whether the algorithm works.
6. After the configuration is complete, click **Save**.

Rounding

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Data Desensitization > Desensitization algorithm**. On the **Desensitization algorithm** page, click the **Transformation** tab.

4. Configure the parameters.



5. In the **Desensitization Algorithm Test** panel, enter the original value and click **Test** to check whether the algorithm works.
6. After the test is complete, click **Submit**.

Encryption

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Desensitization > Desensitization algorithm**. On the **Desensitization algorithm** page, click the **Encryption** tab.
4. Specify a key for an algorithm.
5. In the **Desensitization Algorithm Test** panel, enter the original value and click **Test** to check whether the algorithm works.
6. After the test is complete, click **Submit**.

Shuffling

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Desensitization > Desensitization algorithm**. On the **Desensitization algorithm** page, click the **Shuffling** tab.
4. Select a shuffling method.

5. Click **Submit**.

10.2.6.5. Extract watermarks

You can add watermarks when you create a data masking task. If data is leaked after it is distributed, you can use watermarks to trace the data flow process. This way, the impacts of data leaks are reduced. Sensitive Data Discovery and Protection (SDDP) extracts and identifies watermarks from the leaked data to trace the data flow process and identify the organization or user that is responsible for the data leaks. This topic describes how to extract watermarks.

Procedure

1. Log on to Apsara Stack Security Center.

2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Sensitive Data Desensitization > Extract watermarks**.
4. On the **Extract watermark** page, configure the **Source Product**, **Source database/project name**, and **Source table name** parameters. Then, click **Extract watermark**.

Parameter	Description
Source Product	The name of the data source to which the table containing watermarks belongs.
Source database/project name	The name of the database or project to which the table containing watermarks belongs.
Source table name	The name of the table that contains watermarks.

   The extracted watermarks appear in the field below this parameter. If you want to copy the information, click **Copy Result**.

10.2.7. Report center

10.2.7.1. Comprehensive analysis report

Comprehensive analysis reports are generated based on the analysis results of databases. The analysis is performed from the following perspectives: asset management and security assurance, exception and audit events, sensitive data access and rule hits, and SQL statement execution. This topic describes how to export a comprehensive analysis report.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Report Center > Comprehensive Analysis Report**.
4. On the **Comprehensive Analysis Report** page, configure the **Asset** and **Time Range** parameters.

   Select the asset whose report you want to export from the Asset drop-down list, and select a value from the Time Range drop-down list. The valid values of Time Range are **Today**, **Last 7 days**, **MTD**, **Last 3 Months**, **Last 6 Months**, **Last 12 Months**, and **Yesterday**. You can also specify a custom time range.
5. Click **Export**.
6. In the **Export** message, click **Confirm download** to download the comprehensive analysis report.

10.2.7.2. Analysis report based on MLPS 2.0

You can obtain a risk analysis report for your asset. The report is generated based on the analysis results of your asset data. The analysis is performed based on the MLPS 2.0 standard from the following perspectives: database audit, intrusion prevention monitoring, and security audit monitoring. This topic describes how to export an analysis report based on MLPS 2.0.

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, choose **Report Center > Analysis Report Based on MLPS 2.0**.
4. On the **Analysis Report Based on MLPS 2.0** page, configure the **Asset** and **Time Range** parameters.

   Select the asset whose report you want to export from the Asset drop-down list, and select a value from the Time Range drop-down list. The valid values of Time Range are **Today**, **Last 7 days**, **MTD**, **Last 3 Months**, **Last 6 Months**, **Last 12 Months**, and **Yesterday**. You can also specify a custom time range.
5. Click **Export**.
6. In the **Export** message, click **Confirm download** to download the analysis report.

10.2.8. Grant access permissions

Before you use Sensitive Data Discovery and Protection (SDDP), you must grant access permissions to SDDP. This topic describes how to authorize SDDP to access the data of your department.

Prerequisites

The name and AccessKey pair of your department are obtained before you grant access permissions on the department. For more information, see the "Obtain the AccessKey pair of an organization" topic in *Apsara Uni-manager Management Console User Guide*. To find the topic, choose **Enterprise > Organizations > Obtain the AccessKey pair of an organization**.

Context

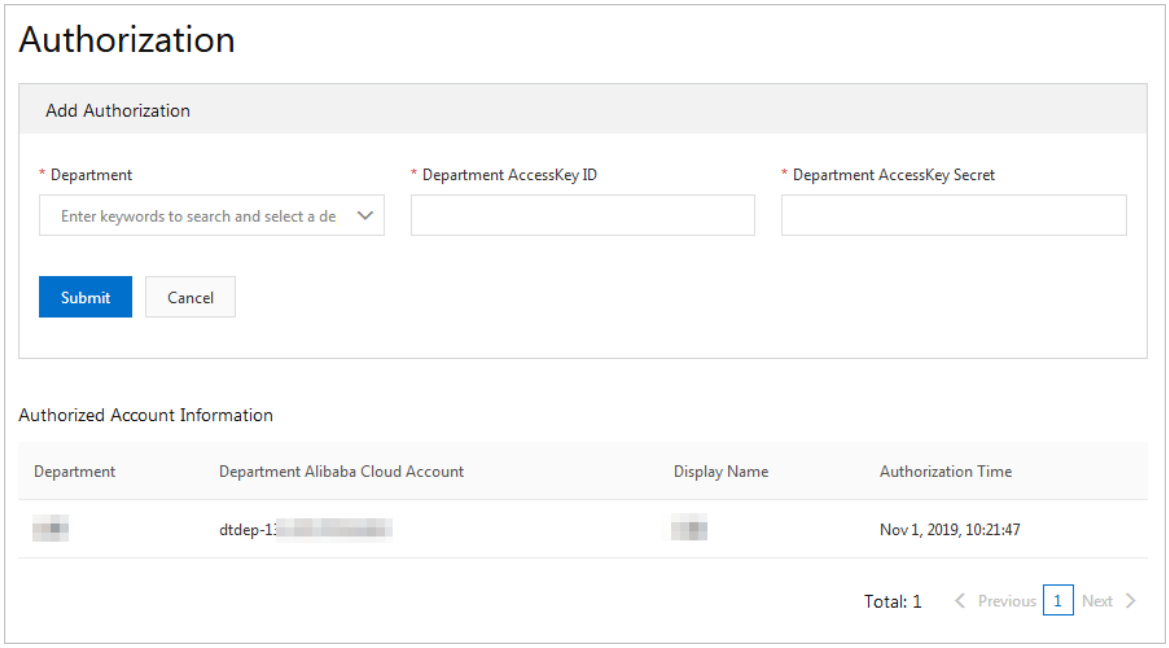
Before you use SDDP, you must complete the following operations:

- Authorize SDDP to access the data of your department.
- Authorize SDDP to access the data of Apsara Stack services of your department. The services include MaxCompute, Object Storage Service (OSS), and Tablestore.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Data Security > Sensitive Data Discovery and Protection**.
3. In the left-side navigation pane, click **Authorization**.

   > **Note** If SDDP is not authorized to access the data of your department, the **Authorization** page appears. You must configure the parameters on this page.



4. In the **Add Authorization** section, authorize SDDP to access the data of your department.
   i. In the **Department** drop-down list, enter a keyword and select the department.
   ii. Configure **Department AccessKey ID** and **Department AccessKey Secret**.
   iii. Click **Submit**.
5. In the **Authorized Account Information** section, view the departments that SDDP is authorized to access.

10.3. Container Protection

10.3.1. View the information about applications in Container Service for Kubernetes

This topic describes how to view the detailed information about applications in Container Service for Kubernetes (ACK).

Procedure

1. Log on to Apsara Stack Security Center.
2. In the top navigation bar, move the pointer over **Security** and choose **Server Security > Container Protection**.
3. On the **Container Protection** page, select a region from the **Region** drop-down list and click **Access with Authorized Role**.
4. In the left-side navigation pane, choose **Container Guard > Assets > Container**.
5. On the **Container** page, click **All applications**.

   The container list displays **Application name**, **Clusters**, **The creation time**, and **Risk Status** of each application.
6. Click the name of an application or click **Handle** in the **Actions** column of the application.

You can view **Vulnerabilities**, **Alerts**, and **Pods** of the application. You can also view the details of an alert and handle the alert.

10.3.2. View Container Registry images

This topic describes how to view Container Registry images.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the top navigation bar, move the pointer over **Security** and choose **Server Security > Container Protection**.
3. On the **Container Protection** page, select a region from the **Region** drop-down list and click **Access with Authorized Role**.
4. In the left-side navigation pane, choose **Container Guard > Assets > Image**.
5. On the **Images** page, click **Image** or **Images with risks**.

   The image list displays **Image Address/Label**, **Size**, **Latest Detection Time**, and **Risk State** of each image.
6. Find an image on which risks are detected and click **Handle** in the **Actions** column.

   You can view **Image System Vul**, **Image Application Vul**, **Image Baseline Check**, and **Mirror Malicious Sample** of the image. You can also click **Details** in the **Operation** column to view the details of a risk.

10.3.3. Use the feature of image security scan

Container Service for Kubernetes (ACK) allows you to scan Container Registry repositories. You can scan for image vulnerabilities, baseline risks, and malicious samples.

Context

The feature of image security scan can detect and identify high-risk system vulnerabilities, application vulnerabilities, malicious samples, configuration risks, and sensitive data. Vulnerabilities may exist in the basic system software, middleware, web applications, and databases that are in your images. The vulnerabilities include mining programs and backdoor programs. Containers that run based on vulnerable images pose threats to your assets. The feature allows you to check whether image vulnerabilities and malicious samples exist in your vulnerable assets, and provides suggestions on vulnerability fixing. This feature provides end-to-end vulnerability management capabilities and allows you to fix image vulnerabilities in a convenient manner.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the top navigation bar, move the pointer over **Security** and choose **Server Security > Container Protection**.
3. On the **Container Protection** page, select a region from the **Region** drop-down list and click **Access with Authorized Role**.
4. In the left-side navigation pane, choose **Container Protection > CI/CD Security > Image Scan**.
5. On the **Image system Vul** or **Image Application Vul** tab, click the **name of a vulnerability** or click **View** in the **Operation** column of the vulnerability.

You can view the details of the vulnerability and the affected images.

6. On the **Image Baseline Check** tab, click **Details** in the **Operation** column of a baseline.

   You can view **Image/Version** and **Check Details /Total Check Items** of the baseline. You can also click **Details** in the **Operation** column to view the status of a risk, and click **Whitelist** or **Remove** to add the risk to the whitelist or remove the risk from the whitelist.

7. On the **Mirror Malicious Sample** tab, click the name of a **malicious sample** or click **Details** in the **Operation** column of the malicious sample.

10.3.4. Use the Intrusion alert feature

Container Service for Kubernetes (ACK) allows you to monitor nodes and containers in ACK clusters. You can use this feature to monitor and block risks such as trojans, external intrusions, supply chain attacks, and container escapes that are caused by privilege escalation.

Context

The intrusion alert feature is developed based on the big data alerting model that is provided by Alibaba Cloud. This feature provides comprehensive intrusion detection capabilities that can inform you of risks in ACK and block external risks in an efficient manner.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the top navigation bar, move the pointer over **Security** and choose **Server Security > Container Protection**.
3. On the **Container Protection** page, select a region from the **Region** drop-down list and click **Access with Authorized Role**.
4. In the left-side navigation pane, choose **Container Protection > Runtime Detection > Alerts**.
5. On the **Alerts** page, click the name of an **affected asset**.

   You can view the details of the container. You can also move the pointer over the name of the **affected asset** to view the details.

6. On the **Alerts** page, click **Handle** in the **Actions** column of an alert.

   You can select **Add to Whitelist**, **Ignore**, **Handled manually**, or **Batch unhandled (combine the alert triggered by the same rule or type)** for the intrusion for which the alert is generated.

7. On the **Alerts** page, click the name of an alert or click **Details** in the **Actions** column of the alert.

   You can view the details of the intrusion for which the alert is generated.

10.3.5. Use the log retrieval feature

The log retrieval feature allows you to query the logs of process snapshots, network connections, and process startups of the containers in Container Service for Kubernetes (ACK). Prefix-based fuzzy match is supported.

Procedure

1. Log on to Apsara Stack Security Center.

2. In the top navigation bar, move the pointer over **Security** and choose **Server Security > Container Protection**.
3. On the **Container Protection** page, select a region from the **Region** drop-down list and click **Access with Authorized Role**.
4. In the left-side navigation pane, choose **Container Guard > Log Retrieval** .
5. On the **Log Retrieval** page, specify the **log source**, **log field**, **query condition**, or **keyword**, and click **Search**.

   You can select **Within 24 Hours** or **Within 7 Days** for the Duration parameter. You can also select **Customize** to specify a time range based on your business requirements. The **custom time range** cannot exceed 30 calendar days.

11.Apsara Stack Security configurations

11.1. Rules

11.1.1. Create an IPS rule for traffic monitoring

This topic describes how to create an intrusion prevention system (IPS) rule for traffic monitoring in Cloud Firewall. Cloud Firewall has built-in IPS rules. This topic describes how to create custom IPS rules based on your business requirements and network environment.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Rules**.
4. On the Rules page, click the **Cloud Firewall IPS Rules** tab.
5. Click **Create Rule**.
6. In the **Create Rule** panel, configure the following parameters.

Parameter	Description
Rule Name	The name of the IPS rule. We recommend that you enter a name that can help you identify and manage the IPS rule in an efficient manner.
Rules Engine	The rules engine that you want to use. Valid values: **Basic Policies** and **Virtual Patches**.
Attack Type	The type of the attack that you want to detect by using the IPS rule
Severity	The severity of the attack. Valid values: **Low**, **Medium**, and **High**.
CVE	The Common Vulnerabilities and Exposures (CVE) ID of the vulnerability that you want to add to the rule. **Note** CVE provides a list of public security vulnerabilities. CVE IDs are allocated by a CVE Numbering Authority (CNA).
Application	The name of the attacked application.
Rule Mode	The mode of the IPS rule. Valid values: **Packet** and **Traffic**.

Parameter	Description
Direction	The direction of traffic that you want to monitor by using the IPS rule. Valid values: **Inbound and Outbound**, **Inbound**, and **Outbound**.
Rule Content	The content of the IPS rule. You must use the Snort syntax to specify the content. **Note** To prevent a negative impact on your business, make sure that the content you enter for the IPS rule is valid.
Rule Description	The description of the IPS rule. We recommend that you enter information that can help you identify the IPS rule, such as the purpose or impact of the rule.
Description	The additional description of the IPS rule. We recommend that you enter information that can help you identify the IPS rule, such as the purpose or impact of the rule.

7. Click **OK**.

11.1.2. Create an IDS rule for traffic monitoring

This topic describes how to create an intrusion detection system (IDS) rule for traffic monitoring.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Rules**.
4. On the Rules page, click the **Traffic Monitoring IDS Rules** tab.
5. Click **Create Rule**.
6. In the **Create Rule** panel, configure parameters.

Parameter	Description
Rule Name	The name of the IDS rule. We recommend that you enter a name that can help you identify and manage the IDS rule in an efficient manner.
Rules Engine	The rules engine that you want to use. Valid values: **Basic Policies** and **Virtual Patches**.
Attack Type	The type of the attack that you want to detect by using the IDS rule
Severity	The severity of the attack. Valid values: **Low**, **Medium**, and **High**.

Parameter	Description
CVE	The Common Vulnerabilities and Exposures (CVE) ID of the vulnerability that you want to add to the rule. **Note** CVE provides a list of public security vulnerabilities. CVE IDs are allocated by a CVE Numbering Authority (CNA).
Application	The name of the attacked application.
Rule Mode	The mode of the IDS rule. Valid values: **Packet** and **Traffic**.
Direction	The direction of traffic that you want to monitor by using the IDS rule. Valid values: **Inbound and Outbound**, **Inbound**, and **Outbound**.
Rule Content	The content of the IDS rule. You must use the Snort syntax to specify the content. **Note** To prevent a negative impact on your business, make sure that the content you enter for the IDS rule is valid.
Rule Description	The description of the IDS rule. We recommend that you enter information that can help you identify the IDS rule, such as the purpose or impact of the rule.
Description	The additional description of the IDS rule. We recommend that you enter information that can help you identify the IDS rule, such as the purpose or impact of the rule.

7. Click **OK**.

11.1.3. Manage IDS rules for traffic monitoring

This topic describes how to view, enable, and disable intrusion detection system (IDS) rules for traffic monitoring.

Context

On the **Traffic Monitoring IDS Rules** tab, you can view the built-in and custom IDS rules. You can also enable or disable the rules based on your business requirements.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Rules**.
4. On the Rules page, click the **Traffic Monitoring IDS Rules** tab.
5. Manage IDS rules for traffic monitoring.

In the list of IDS rules, you can view rule details, enable rules, and disable rules.

- View rule details

  Find the rule whose details you want to view and click **Details** in the **Actions** column to view the rule details.

- Enable a rule

  Find the rule that you want to enable and turn on the switch in the **Enable or not** column to change the status of the rule from **Disable** to **Enable**.

- Disable a rule

  If a rule is not suitable for your business, you can disable the rule.

  Find the rule that you want to disable and turn off the switch in the **Enable or not** column to change the status of the rule from **Enable** to **Disable**.

11.1.4. Specify custom thresholds for DDoS traffic scrubbing policies and traffic redirection

This topic describes how to specify custom thresholds for DDoS traffic scrubbing policies and traffic redirection. Default thresholds are provided. If you want to specify custom thresholds, perform the following steps:

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Rules**.
4. Specify a custom threshold for a DDoS traffic scrubbing policy.
   i. Click the **Anti-DDoS Service Rules** tab.
   ii. Then, click the **Scrubbing Policy** tab.
   iii. Find the policy for which you want to specify a custom threshold and click **Modify Threshold** in the **Actions** column.
   iv. In the **Modify Threshold** dialog box, enter a threshold value.
   v. Click **OK**.
5. Specify a custom threshold for traffic redirection.
   i. Click the **Anti-DDoS Service Rules** tab.
   ii. Then, click the **Scrubbing Policy** tab.
   iii. Find a rule for traffic redirection whose threshold you want to modify and click **Modify Threshold** in the **Actions** column.
   iv. In the **Modify Threshold** dialog box, enter a threshold value.
   v. Click **OK**.

11.1.5. View Server Guard rules

This topic describes how to view the operations of Server Guard rules. You can view vulnerabilities, baselines, and host exceptions.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Rules**.
4. On the **Rules** page, click the **Server Guard Rules** tab.
5. In the overview section, you can view the total number of **vulnerability libraries**, number of **baselines**, number of **host exceptions**, and the available **engines**.
6. View the vulnerability list.
   i. Click the **Vulnerabilities** tab.
   ii. In the overview section, you can view the total number of **Linux vulnerabilities**, total number of **Windows vulnerabilities**, total number of **Web-CMS vulnerabilities**, and total number of **urgent vulnerabilities**.
   iii. Specify search conditions to search for the vulnerabilities that you want to view.

   > **Note** If you want to view all vulnerabilities, skip this step.

   In the vulnerability list, you can view the **vulnerability name**, **CVE ID**, **vulnerability type**, **operating system**, **update time**, and **status**.
7. View the baseline list.
   i. Click the **Baselines** tab.
   ii. In the overview section, you can view the numbers of baseline types and the number of check items.
   iii. Specify search conditions to view the baselines that meet the search conditions

   > **Note** If you want to view all baselines, skip this step.

   In the baseline list, you can view the **baseline type**, **check item category**, **check item name**, **risk level**, **update time**, and **status**.
8. View the host exception list.
   i. Click the **Server Exceptions** tab.
   ii. In the overview section, you can view the number of **rule alert subcategories**, the number of webshells, and the number of malicious viruses.
   iii. Specify search conditions to search for the host exceptions that you want to view.

   > **Note** If you want to view all exceptions, skip this step.

   In the host exception list, you can view the **subcategory name**, **rule category**, **risk level**, **update time**, **source**, and **status**.

11.2. Threat intelligence

11.2.1. View the Overview page

This topic describes how to view the overall situation and statistics about threats to your assets over the last 30 days on the Overview page.

Prerequisites

The **service configuration** feature is enabled. For more information, see Enable the service configuration feature.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Overview**.
4. On the **Overview** page, view the statistics and threats that are detected on Apsara Stack services by the threat intelligence module.

   On the **Overview** page, you can perform the following operations:

   - View **Total malicious metric intelligence**

     In the **Total malicious metric intelligence** section of the **Overview** page, view the information about the detected threats on Apsara Stack services. The information includes the number of malicious IP addresses, the number of malicious domain names, and the number of malicious URLs.

   - View **Threat trends in the last 30 days**
   - Search for an IP address to check whether the IP address is malicious.

     In the upper-right corner of the search box, enter the IP address that you want to check and click the icon. Then, you are redirected to the details page of the IP address. For more information, see Search for an IP address.

   - View **Top 10 active IP malicious addresses**

     In the **Top 10 active IP malicious addresses** section of the **Overview** page, view the information about the top 10 malicious IP addresses. The information includes **IP address**, **First malicious observation**, **Last malicious observation**, and **Malicious label**. Find the malicious IP address whose details you want to view and click **View** in the Actions column. Then, you are redirected to the details page of the IP address. For more information, see Search for an IP address.

11.2.2. Search for and view the information about a suspicious or malicious IP address

The threat intelligence module allows you to search for threat intelligence. This module helps you handle suspicious or malicious IP addresses at the earliest opportunity.

Prerequisites

The **service configuration** feature is enabled. For more information, see Enable the service configuration feature.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Alibaba Cloud Security**.
3. In the left-side navigation pane, click **IP Address Search**.
4. In the search box on the **Search** page, enter the suspicious or malicious IP address that you want to query and click the icon.
5. On the details page of the IP address, view the values of **Threat Level**, **Basic Information**, **Threat Overview**, **IP Details**, and **Analysis of Attack Risk Degree** of the IP address.

   You can view the following information on the details page of the IP address:

   - **Threat Level**: View the threat level of the suspicious or malicious IP address.

     The threat intelligence module classifies IP addresses into the following threat levels: normal, suspicious, and high-risk. If the IP address is identified as high-risk, we recommend that you handle the IP address at the earliest opportunity.

   - **Basic Information**: View the basic information about the suspicious or malicious IP address.

     The basic information includes the server in a data center, Abstract Syntax Notation One (ASN.1), the country and city to which the IP address belongs, and the number of domain names for the IP address.

   - View the statistics about the suspicious or malicious IP address.

     You can view **Threat Overview**, **IP Details**, and **Threat Details** of the IP address.

     - The **Threat Overview** tab displays **Top5 Target Preference**, **Number of Attacks (Classified by Threat)**, and **Analysis of Attack Risk Degree** of the IP address.
     - The **IP Details** tab displays **WHOIS Information** and **IP Reverse Check Information** of the IP address.
     - The **Threat Details** tab displays the **threat tags** of the IP address. The tags include the intelligence source, the time when the IP address is first detected, the time when the IP address is last active, and the threat tag.

11.2.3. Enable the service configuration feature

The threat intelligence module integrates threat monitoring and big data analysis. You can use these features to obtain information about the latest developments in the threat intelligence field. After you enable the service configuration feature, the system starts to monitor and collect threat intelligence. This topic describes how to enable the service configuration feature.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform**

Security > Alibaba Cloud Security.

3. In the left-side navigation pane, click **Service Configurations**.
4. On the **Consumer product configuration** page, view the data types and descriptions on the Situation awareness and Web application firewall tabs.
5. Click the tab in which you want to enable threat monitoring and turn on **Activation status**.

   After you turn on **Activation status**, the system starts to monitor and collect threat intelligence for the data types listed on the tab.

What's next

After you enable the service configuration feature, you can view the overall situation and statistics of threats within the last 30 days on the **Overview** tab. For more information, see View the Overview page.

11.3. Alert settings

11.3.1. Configure alert contacts

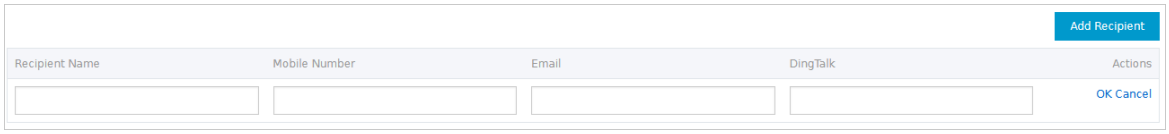
This topic describes how to configure and manage alert contacts.

Context

Apsara Stack Security sends alert notifications to alert contacts by text message or email. If the detected information matches an alert rule, Apsara Stack Security sends an alert notification to the alert contacts.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Alert Settings**.
4. On the **Alert Settings** page, click the **Alert Recipient** tab.
5. Click **Add Recipient**.
6. Enter the contact information and click **OK**.



7. Manage alert contacts.

   In the contact list, find a contact whose information you want to modify and click **Edit** in the Actions column.

11.3.2. Configure alert notifications

This topic describes how to configure alert notification methods for security events on tenants or platforms.

Context

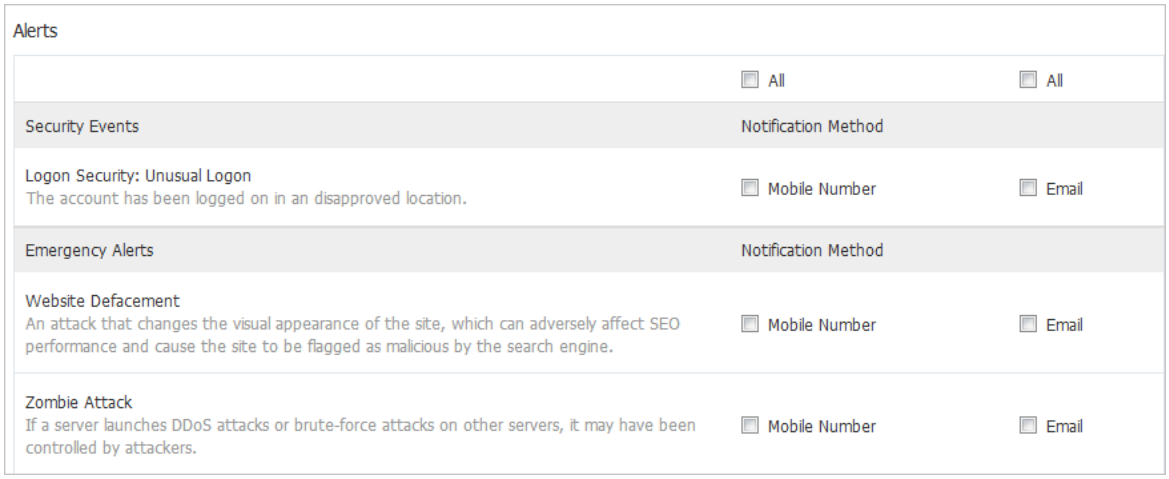
In the **Alerts** section, security administrators can configure the alert notification method for security events. When a security event occurs, the system notifies the alert contacts by email or text message. For more information about how to configure alert contacts, see Set alert recipients.

Alerts on tenants

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Alert Settings**.
4. On the **Alert Settings** page, click **Tenant Alerts**.
5. In the **Alerts** section, select notification methods for each security event.
6. Click **Confirm**.

Alerts on the platform

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Alert Settings**.
4. On the **Alert Settings** page, click **Platform Alerts**.
5. In the **Alerts** section, select notification methods for each security event.



6. Click **Confirm**.

11.4. Updates

11.4.1. Overview of the system updates feature

The system updates feature allows you to manually or automatically update the Apsara Stack Security and rule libraries for up-to-date protection.

The supported package import method depends on the Apsara Stack network environment.

- If Apsara Stack is connected to the Internet, you can choose **Automatically Download Update Packages**.
- If Apsara Stack is not connected to the Internet, you can choose **Manually Import Update Packages**.

The following table lists the update statuses of a rule library.

Update statuses of a rule library

Status	Description
To Be Updated	Indicates that a new version of the rule library is available for update.
Updating	Indicates that the rule library is being downloaded from Alibaba Cloud for update.
Updated	Indicates that the rule library has been updated.
Update Failed	Indicates that the rule library failed to be updated.

11.4.2. Enable automatic update check and update rule libraries

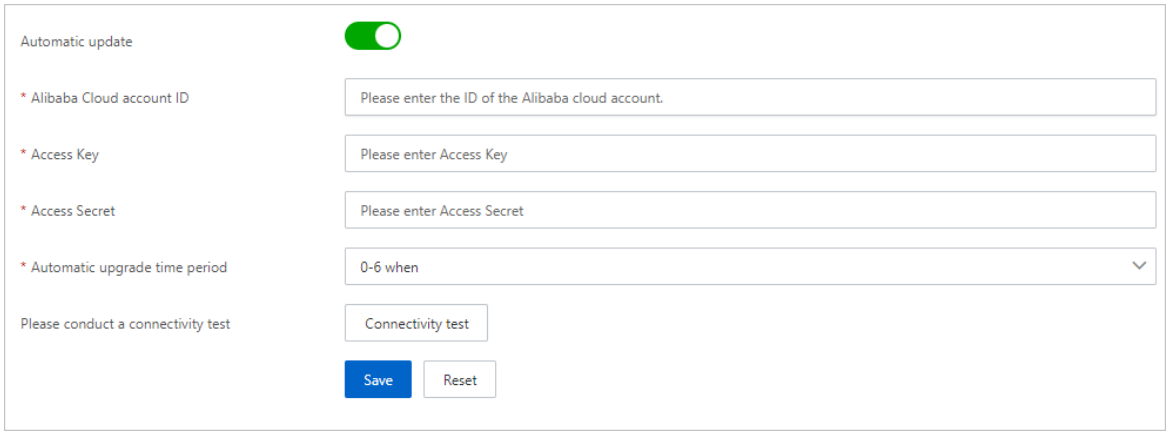
This topic describes how to enable automatic download of update packages and update rule libraries.

Context

If the Apsara Stack environment can connect to the Internet, you can enable automatic download of update packages to update the rule libraries.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Updates**.
4. Click the **Upgrade configuration** tab.
5. On the **Upgrade configuration** tab, click the **Automatic update** tab.
6. Turn on **Automatic update** to enable automatic download of update packages and configure the following parameters.



Parameter	Description
Alibaba Cloud account ID	Enter the ID of the Alibaba Cloud account.
Access Key	Enter the AccessKey ID.
Access Secret	Enter the AccessKey secret.
Automatic upgrade time period	Select a time period for automatic updates. Valid values: ○ 0-6 when ○ 0-8 when ○ 0-24 when ○ 22-6 when

7. Click **Connectivity test**.
8. Click **Save** to enable the automatic check for update packages.

   After this switch is turned on, the system automatically downloads update packages on a regular basis.

11.4.3. Manually import an update package and update your service

This topic describes how to manually import an update package and update your service.

Prerequisites

The security administrator obtained the offline update package.

Context

If the Apsara Stack environment cannot connect to the Internet, you can manually import an update package to update the rule libraries.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Updates**.
4. Click the **Upgrade configuration** tab.
5. Click the **Manual update** tab.
6. Manually import an update package.
   i. Click **Manually import offline upgrade packages**.
   ii. In the **Manually import offline upgrade packages** dialog box, click **Please select a file** to select an offline update package that is downloaded to your computer.
   iii. Click **Confirm**.

   After the update package is imported, the package appears on the **Version Update** tab. You can click Upgrade now in the Operation column of the update package to update your service.

11.4.4. Roll back a rule library

This topic describes how to roll back a rule library to a previous version.

Context

If an error occurs with an updated rule library, you can roll back the library to a previous version to prevent service interruption.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Updates**.
4. Click the tab of the specific rule library. Example: **Server Security**.
5. In the Actions column for the rule library, choose **More > Roll Back**.
6. In the **Version Rollback** dialog box, click **Confirm**.

11.4.5. View the update history of a rule library

This topic describes how to view the update history of a rule library.

Context

You can view the update history of a rule library. This way, if an error occurs with the latest version, you can identify the issue and roll back the rule library to an earlier version.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.

3. In the left-side navigation pane, click **Updates**.
4. Click the tab of the specific rule library. Example: **Server Security**.
5. In the **Actions** column of a rule library, click **History**.

   On the **Previous Updates** page, you can view the update history of the rule library. Click **Details** to view the details about an update package.

11.4.6. Download update packages

If you need to update the version of Apsara Stack Security or update Apsara Stack Security services, you can download the required update packages in the Alibaba Cloud Security Center console and upload the update packages in Apsara Stack Security Center to complete the update. This topic describes the update modes of Apsara Stack Security and how to download update packages in different update modes.

Update modes

Security Center provides two update modes: standard mode and advanced mode. The following table describes the two update modes.

Update mode	Description	References
Standard mode	In this mode, the system provides the update packages that are required for version update or service update based on the version of Apsara Stack Security that you entered, and encapsulates these update packages into a combined update package. In this mode, you do not need to manually select update packages. We recommend that you use the standard mode. In this mode, you can update the version of Apsara Stack Security or update Apsara Stack Security services in a more convenient and efficient manner.	Standard mode
Advanced mode	In this mode, you can select the version of Apsara Stack Security to obtain the latest update packages. You can also download update packages to update Apsara Stack Security services based on your business requirements. **Note** In advanced mode, you need to know the dependencies and update sequence between update packages.	Advanced mode

Standard mode

1. Log on to the Security Center consoleSecurity Center console.
2. In the left-side navigation pane, choose **Operation > Upgrade packages**.
3. In the **Upgrade Mode** section on the **Upgrade packages** page, click **Standard Mode**.
4. In the **Identifier of Apsara Stack Security Version** search box, enter the version of Apsara

Stack Security to which you want to update and click **Obtain Rule Package** to obtain update packages.

> **Note**
> - For more information about how to obtain the version identifier of Apsara Stack Security, click **How to Obtain Upgrade Package** below the search box.
> - If you use Apsara Stack Security V3.12, V3.13, or V3.14, you must enter the version identifier of Apsara Stack Security in the Identifier of Apsara Stack Security Version search box to obtain update packages.

5. In the **Download Upgrade Package** section, find the update packages that you want to download and click **Download** in the **Operation** column.
   After the update packages are downloaded, upload the update packages to Apsara Stack Security Center. In Apsara Stack Security Center, perform update-related operations to complete the update.

Advanced mode

1. Log on to the Security Center consoleSecurity Center console.
2. In the left-side navigation pane, choose **Operation > Upgrade packages**.
3. In the **Upgrade Mode** section on the **Upgrade packages** page, click **Advanced Mode**.
4. In the **Identifier of Apsara Stack Security Version** section, select Apsara Stack or Offine Version from the drop-down list on the left and select the version of the update packages that you want to download from the drop-down list on the right.
5.

11.5. Global configuration

11.5.1. Set CIDR blocks for traffic monitoring

11.5.1.1. Add a CIDR block for traffic monitoring

This topic describes how to add a CIDR block for traffic monitoring. Network Traffic Monitoring System of Apsara Stack Security monitors the traffic of a specific CIDR block.

Context

CIDR blocks are configured for Network Traffic Monitoring System. Security administrators can change the CIDR blocks for traffic monitoring based on business requirements. The settings of CIDR blocks apply only to a data center that is deployed in the region to which the specific CIDR block belongs.

> **Note**
> - Changes to CIDR block settings immediately take effect without the intervention of security administrators.
> - If you add the same CIDR block on the traffic collection CIDR block setting page and region setting page, make sure that you select the same region on both pages.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.
4. On the **Global Settings** page, click the **Traffic Collection IP Range** tab.
5. Click **Add**.
6. In the **Add CIDR Block for Monitoring** dialog box, configure parameters.

   - **CIDR Block**: Enter a CIDR block for traffic monitoring.

     > **Note** Make sure the CIDR block that you enter is valid and unique.

   - **Region**: Select the region of the data center.
7. Click **OK**.

11.5.1.2. Manage CIDR blocks for traffic monitoring

This topic describes how to modify or delete CIDR blocks for traffic monitoring.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.
4. On the **Global Settings** page, click the **Traffic Collection IP Range** tab.
5. Select a region, enter the CIDR block that you want to query, and then click **Search**.

   View the information about the CIDR block for traffic monitoring and the region in the search result.
6. In the **Actions** column, manage a CIDR block for traffic monitoring.
   - Modify the CIDR block for traffic monitoring

     Click **Modify** to modify the region of the CIDR block for traffic monitoring.
   - Delete the CIDR block for traffic monitoring

Click **Delete** to delete the CIDR block for traffic monitoring.

11.5.2. Region settings

11.5.2.1. Add a CIDR block for a region

This topic describes how to add CIDR blocks for regions that are detected and reported by using Server Guard.

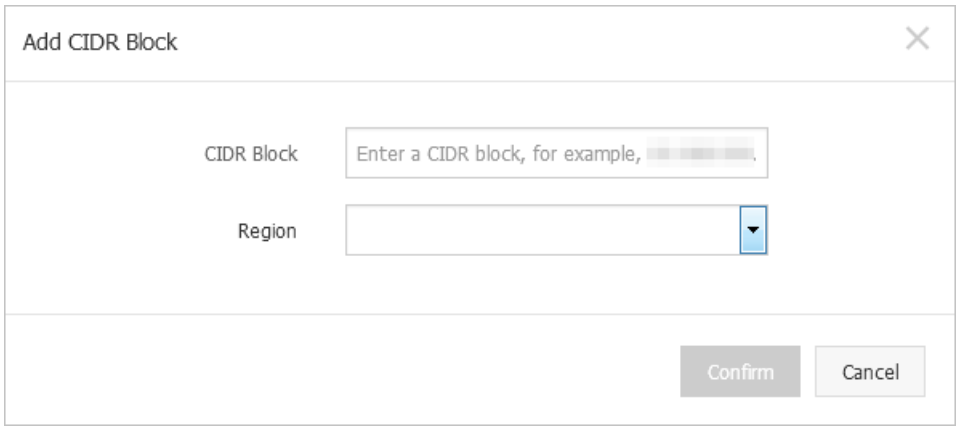
Context

Region settings are used for region detection of the Server Guard agent. Server Guard servers automatically detect and match the regions of servers based on the IP address information that is reported by the Server Guard agent.

> **Note** You can change the region of a CIDR block. After you change the region, you must also change the region for all assets in the CIDR block on the Asset Overview page.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.
4. On the **Global Settings** page, click the **Region** tab.
5. Click **Add**.
6. In the **Add CIDR Block** dialog box, configure parameters.



   - **CIDR Block**: Enter a CIDR block for the region.

     > **Note** Enter a valid CIDR block. You cannot enter a CIDR block that is configured for the region.

   - **Region**: Select a region.
7. Click **Confirm**.

11.5.2.2. Manage CIDR blocks for a region

This topic describes how to modify or delete CIDR blocks for a region.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.
4. On the **Global Settings** page, click the **Region** tab.
5. Select a region, enter the CIDR block that you want to modify or delete, and then click **Search**.

   You can view the information about the CIDR block for the region in the search result.
6. In the **Actions** column, click Modify or Delete to manage the CIDR block for the region.
   - Modify the CIDR block for the region

     Click **Modify** to modify the CIDR block for the region.
   - Delete the CIDR block for the region

     Click **Delete** to delete the CIDR block for the region.

11.5.3. Configure whitelists

This topic describes how to configure the whitelist for the feature that blocks brute-force attacks in Server Guard, and how to configure the whitelists in Threat Detection Service (TDS). These whitelists consist of IP addresses allowed by server brute-force attack blocking, IP addresses allowed by application attack blocking, and IP addresses allowed by web attack blocking.

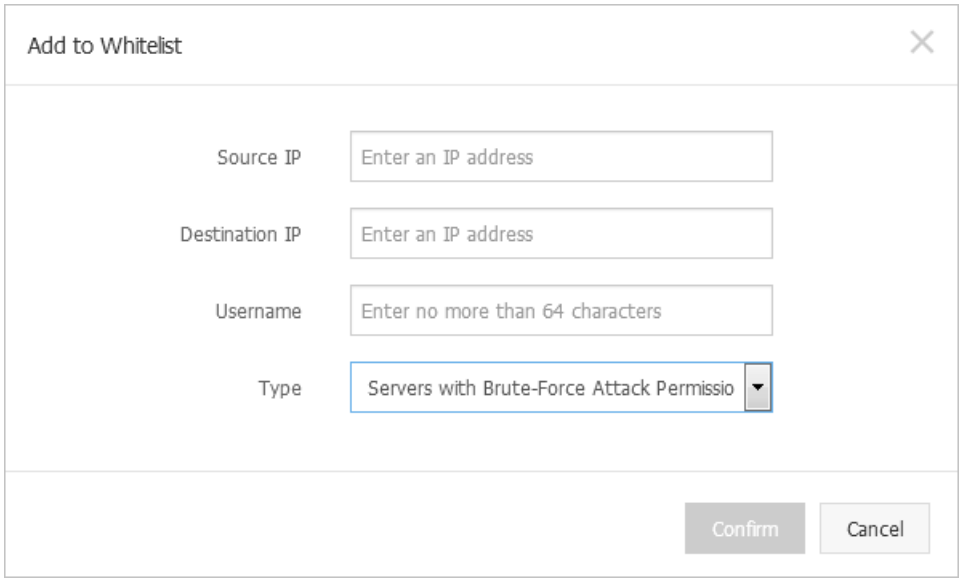
Context

If a normal request is identified as an attack by the attack blocking feature of TDS or the unusual logon detection feature of Server Guard, you can add the source IP address of the request to a whitelist to prevent further false positives.

> **Note** Make sure that the IP addresses in the whitelist are trusted.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.
4. On the **Global Settings** page, click the **Whitelist** tab.
5. Click **Add**.
6. In the **Add to Whitelist** dialog box, configure the parameters.



Parameter	Description
Type	○ **Global Login Whitelist**: Server Guard does not generate alerts for brute-force attacks or unusual logons from the IP addresses that are contained in this whitelist. ○ **Brute-Force Whitelist**: The attack blocking feature does not generate alerts for brute-force attacks from the IP addresses that are contained in this whitelist.
Source IP	Enter a source IP address or Classless Inter-Domain Routing (CIDR) block.
Destination IP	Enter a destination IP address or CIDR block.

7. Click **Confirm**.
   If you want to delete an existing whitelist, click **Delete** in the Actions column. In the **Delete Whitelist** message, click **Confirm**.

11.5.4. Configure policies that are used to block attacks

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

Context

The attack blocking features protect your servers against web attacks and brute-force attacks.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.

4. On the **Global Settings** page, click the **Policy Configuration** tab.
5. Turn on or off the switches in the Actions column to enable or disable **Web Attack Blocking** or **Brute-Force Attack Blocking**.

> **Note**
>
> In the Actions column, a red switch indicates that a feature is disabled. A green switch indicates that a feature is enabled.
>
> After you disable the blocking feature for an attack type, Apsara Stack Security only generates alerts for this type of attacks.

11.5.5. Block IP addresses

This topic describes how to manually block requests for an IP address with a few clicks.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.
4. On the **Global Settings** page, click the **Block IP Addresses** tab.
5. In the upper-right corner of the tab, click **Add**.
6. In the **Add** dialog box, specify the IP address to block.

Parameter	Description
IP Protocol	Specify the type of the IP address that you want to block. Valid values: **IPv4** and **IPv6**.
Source IP	Enter the source IP address that you want to block.
Destination IP	Enter the destination IP address that you want to block.
Destination Port	Enter the destination port that is used together with the specified destination IP address.
Blocking Duration	Select a time range during which you want to block requests. Valid values: **1 Day**, **7 Days**, and **30 Days**.
Type	Select the blocking mode. Valid values: **Whitelist** and **Blacklist**.
Remarks	Enter the reason for the block.

7. Click **Confirm**.

11.5.6. Configure custom IP addresses and locations

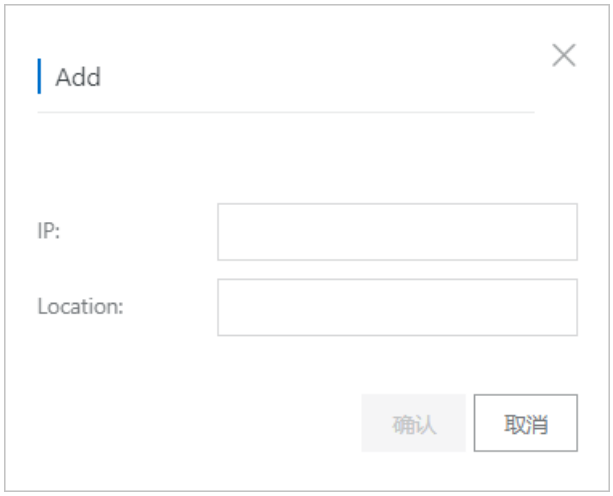
11.5.6.1. Add custom IP addresses and locations

This topic describes how to add custom IP addresses and locations. You can customize internal IP addresses based on your network plan. After you configure the internal IP addresses, IP addresses from the public address library do not match the addresses outside China.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.
4. On the **Global Settings** page, click the **Custom IP Location** tab.
5. Click **Add**.

   If you want to add multiple IP addresses and locations at a time, click **Batch Upload (.txt)**. Then, you can use Batch Upload (.txt) as a template to import multiple IP addresses and locations.
6. In the **Add** dialog box, configure the parameters.



7. Click **Ok**.

11.5.6.2. Manage custom IP addresses and locations

This topic describes how to modify and delete custom IP addresses and locations.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Global Settings**.

4. On the **Global Settings** page, click the **Custom IP Location** tab.
5. In the **Actions** column, manage custom IP addresses and locations.
   - To change a custom IP address and a location:

     Click **Modify**. In the **Modify** dialog box, change the custom geographical location.
   - To delete a custom IP address and a location:

     Click **Delete**. In the **Delete** message, click **OK**.

11.6. System monitoring

11.6.1. Inspect services

This topic describes how to inspect services such as Cloud Firewall and Network Traffic Monitoring System in Apsara Stack Security Center. You can monitor the status and features of the services.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **System Monitoring**.
4. In the **System Inspection** section of the **Network Security** tab, inspect the services in the inspection list.

   To inspect a single service or multiple services at a time, perform the following operations:
   - Inspect multiple services at a time: In the **System Inspection** section, click **One-Click Inspection** to inspect all services in the inspection list.
   - Inspect a single service: In the **System Inspection** section, click **Inspect Now** in the **Actions** column of the service that you want to inspect.

   After the services are inspected, the status of the services changes to **Complete** in the **Inspection Status** column.
5. View the inspection results.

   You can view the following information about a service:
   - In the inspection list, view the service name, last inspection time, number of inspection items, number of inspection items whose status is normal, number of inspection items whose status is abnormal, and inspection status.
   - Click **Details** in the **Actions** column of a service. In the **Inspection Result Details** panel, view the number of inspection items whose status is normal, number of inspection items whose status is abnormal, and details of each item.
   - Click **Download** in the **Actions** column of a service. Download the inspection results to your computer as prompted for backup and reference.

11.7. Account management

11.7.1. View and modify an Apsara Stack tenant account

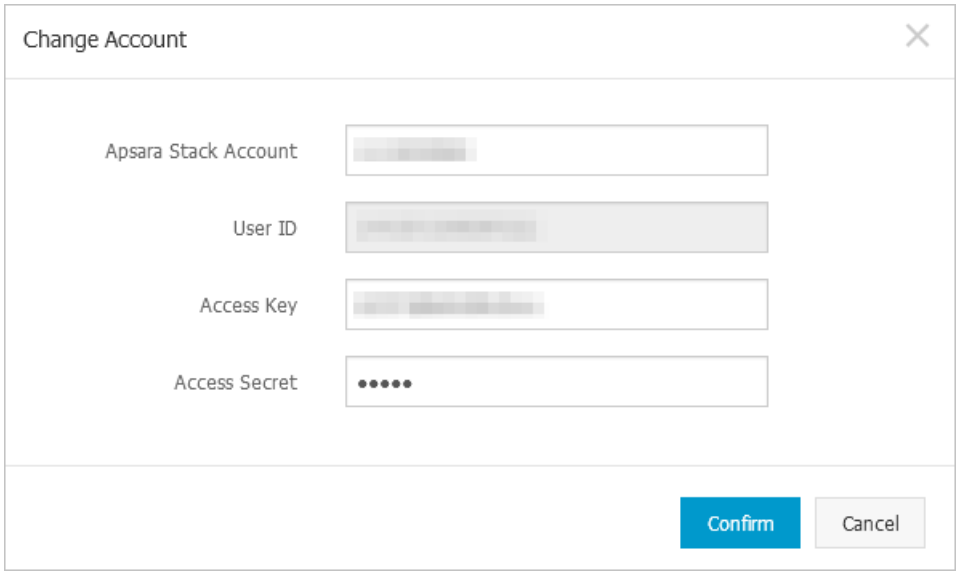
This topic describes how to view and modify the information about your Apsara Stack tenant account that is bound to the system.

Context

Note All assets in Apsara Stack Security are bound to your Apsara Stack tenant account. You can modify the account information. Proceed with caution.

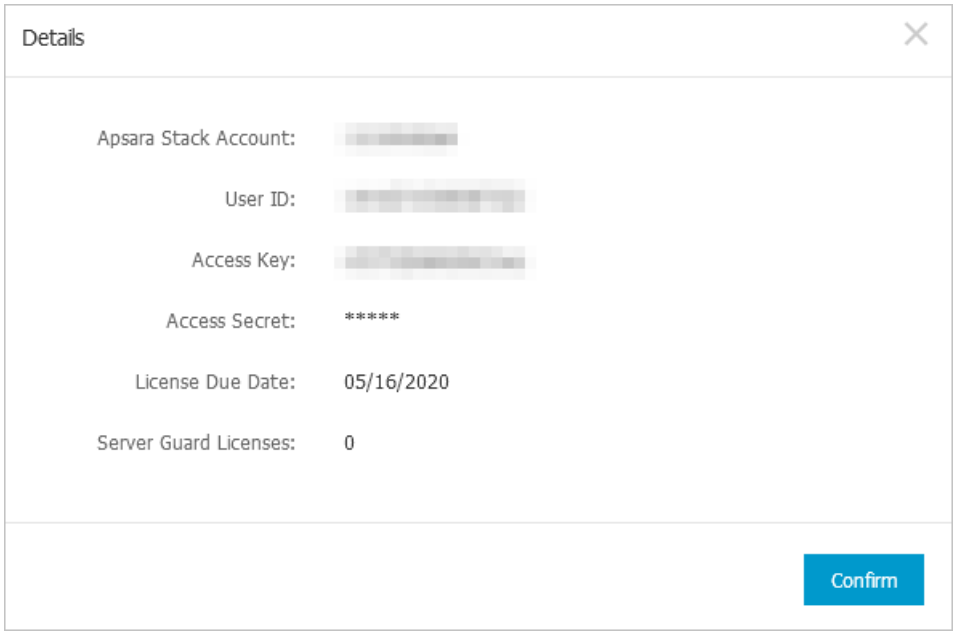
Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**.In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Accounts**.
4. On the **Accounts** page, click the **Apsara Stack Account** tab.
5. Modify the information about your Apsara Stack tenant account.
   i. In the Actions column, click **Modify**.
   ii. In the **Change Account** dialog box, modify the account information.



   iii. Click **Confirm**.
6. View the details of your Apsara Stack tenant account.

   In the Actions column, click **Details** to view the details of your Apsara Stack tenant account.



11.7.2. Add an Alibaba Cloud account

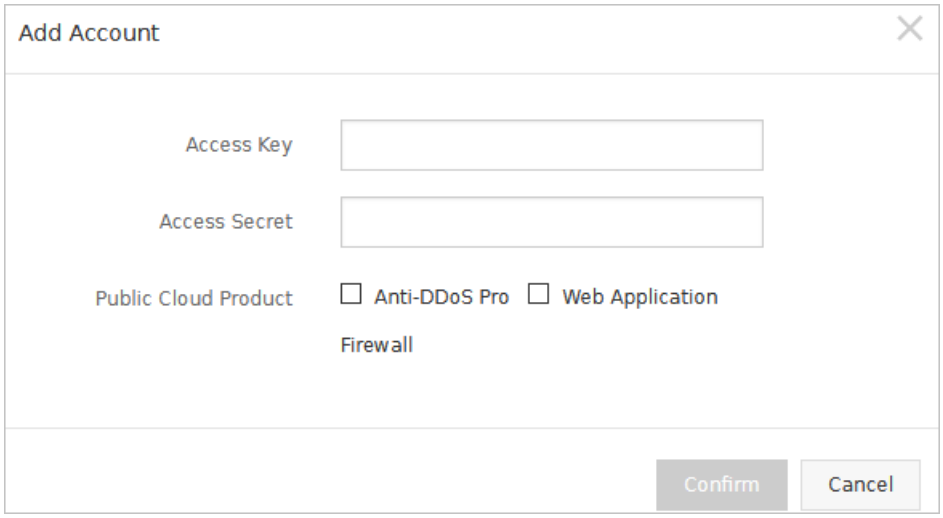
This topic describes how to add an Alibaba Cloud account in Apsara Stack Security Center. After you add the account, you can use features in a hybrid cloud.

Context

After you add an Alibaba Cloud account in Apsara Stack Security Center, you can manage the Anti-DDoS Pro, Anti-DDoS Premium, and Web Application Firewall (WAF) instances that belong to the Alibaba Cloud account in Apsara Stack Security Center. This way, you can use features in a hybrid cloud.

Procedure

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. In the **Global Platform Security** section, click **Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Accounts**.
4. On the **Accounts** page, click the **Public Cloud Account** tab.
5. On the **Feature Integration** tab, click **Add**.
6. In the **Add Account** dialog box, enter the information about your Alibaba Cloud account and select Alibaba Cloud services to use.



- Enter the **AccessKey ID** and **AccessKey secret** of your Alibaba Cloud account.
- Select Alibaba Cloud services to use for Public Cloud Product. Valid values: **Anti-DDoS Pro**, **Web Application Firewall**, and both.

7. Click **Confirm**.

Result

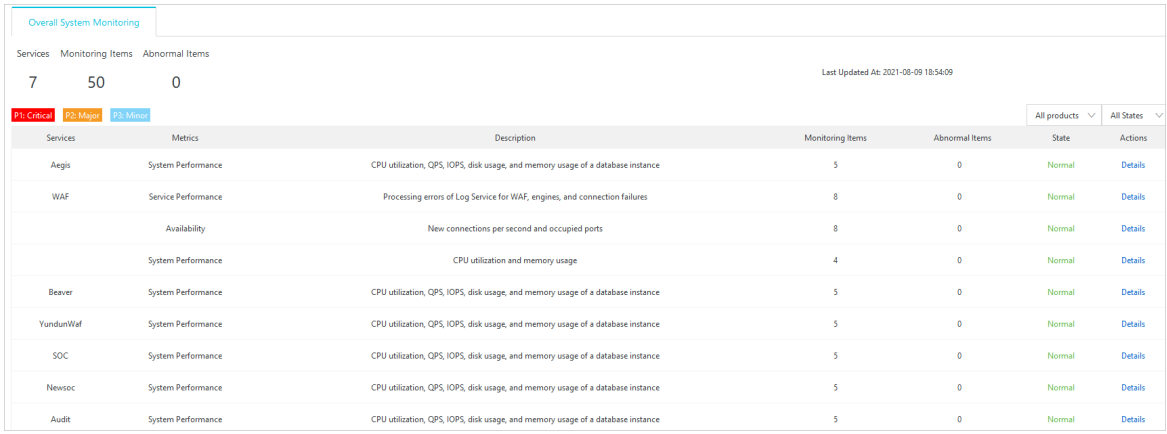
After the account is added, it is displayed on the **Public Cloud Account** tab. To modify or delete the account, you can click **Modify** or **Delete** in the Actions column.

11.8. View and manage metrics

Apsara Stack Security Center allows you to monitor security services. This helps find performance bottlenecks at the earliest opportunity. Then, you can scale out, scale up, or downgrade services to prevent system failures. This topic describes how to view the information about security services in Apsara Stack Security Center and how to manage metrics.

View information about overall system monitoring

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Alibaba Cloud Security**.
3. In the left-side navigation pane, click **Security Monitoring**.
4. On the **Security monitoring** tab, view the overall information about security services in Apsara Stack Security Center and the list of monitored security services.



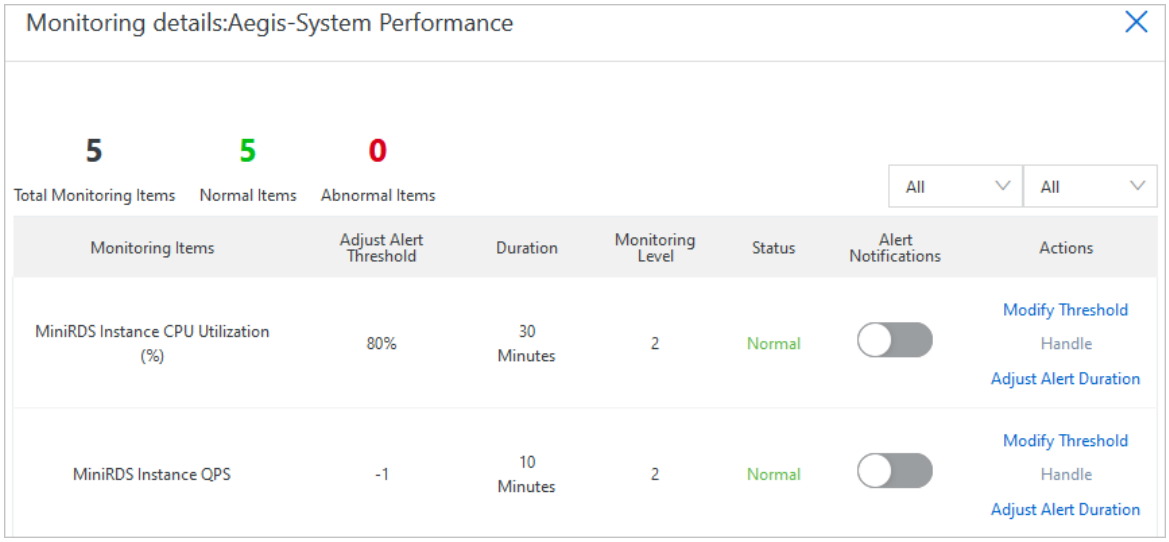
In the upper-left corner of the **Overall System Monitoring** tab, you can view the overall information about security services.

- **Services**: the total number of security services monitored in Apsara Stack Security Center.
- **Monitoring Items**: the total number of metrics.
- **Abnormal Items**: the number of metrics whose status is abnormal.

In the list of monitored security services, you can view the following information.

Parameter	Description
Services	The security service monitored in Apsara Stack Security Center.
Metrics	The monitoring indicator for the monitored security service.
Description	The description of the monitoring indicator.
Monitoring Items	The total number of metrics that belong to the monitoring indicator.
Abnormal Items	The number of metrics whose status is abnormal, and the number of metrics at each urgency level. The urgency levels are indicated by different colors. The red color indicates a critical exception, the orange color indicates an important exception, and the blue color indicates a moderate exception. 
State	The status of the monitoring indicator.

5. Click **Details** in the **Actions** column of a monitoring indicator. In the **Monitoring details** panel, view the details of metrics that belong to the monitoring indicator.



In the upper-left corner of the **Monitoring details** panel, you can view the overall information about the metrics.

- **Total Monitoring Items**: the total number of metrics that belong to the monitoring indicator.
- **Normal Items**: the number of metrics in the normal state.
- **Abnormal Items**: the number of metrics in the abnormal state.

In the metric list, you can view the following information.

Parameter	Description
Monitoring Items	The name of the metric.
Adjust Alert Threshold	The threshold for the metric. If the value of the metric reaches the threshold and lasts for the specified period of time, the status of the metric becomes abnormal.
Duration	The period of time. If the value of the metric reaches the threshold and lasts for the specified period of time, the status of the metric becomes abnormal.
Monitoring Level	The urgency level displayed when the status of the metric becomes abnormal.
Status	The status of the metric.
Alert Notifications	The switch of the alert notification feature. You can turn on or off the switch in the **Alert Notifications** column based on your business requirements. If the On icon appears in the Alert Notifications column, a notification is sent when the status of the metric becomes abnormal.

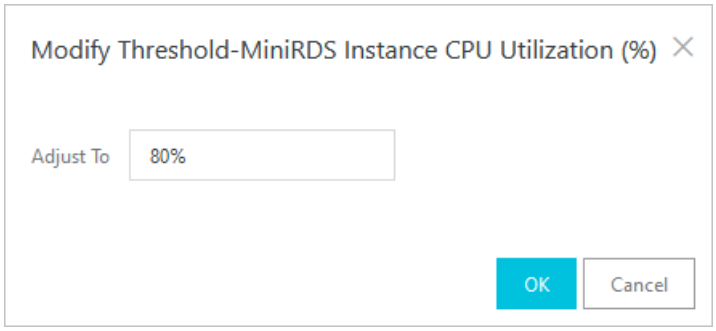
Manage metrics

1. Log on to Apsara Stack Security Center.
2. In the upper-right corner of Apsara Stack Security Center, click **Security**. Choose **Global Platform Security > Alibaba Cloud Security**.

3. In the left-side navigation pane, click **Security Monitoring**.
4. On the **Security monitoring** tab, find a monitoring indicator and click **Details** in the **Actions** column.
5. In the **Monitoring details** panel, find a metric and click **Modify Threshold**, **Handle**, or **Adjust Alert Duration** in the **Actions** column to manage the metric.

   You can perform the following operations on the metric:

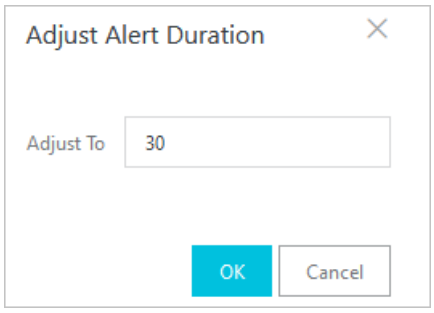
   - **Modify Threshold**: In the **Modify Threshold** dialog box, modify the threshold and click **OK**.

     After the threshold is modified, an alert is generated when the value of the metric reaches the new threshold.

   - **Handle**: You can configure the status of the metric based on your business requirements.
     - If you do not want to handle the alert generated from the metric, select **Ignore** from the drop-down list. The status of the metric becomes **ignored**.
     - After you handle the alert generated from the metric, select **Handled** from the drop-down list. The status of the metric becomes **handled**.

   - **Adjust Alert Duration**: In the **Adjust Alert Duration** dialog box, modify the period of time and click **OK**.

     When the value of the metric reaches the threshold and lasts for the specified period of time, the status of the metric becomes abnormal.