NSFOCUS Log Audit System
User Guide

Version: V2.0R02IB00 (2026-06-16)

Confidentiality: Restricted

■ Statement

The purchased products, services, or features are stipulated in the contract made between NSFOCUS and the customer. Part of products, services, and features described in this document may not be within the purchased scope or the usage scope.

All information in this document is provided "AS-IS" without guarantees of any kind, express or implied. The information in this document is subject to change without notice. It may slightly differ from the actual product due to version upgrade or other reasons.

■ Disclaimer

Please read the disclaimer carefully before using the product. Once you use the product, you acknowledge and agree to all the contents of this disclaimer. NSFOCUS shall not assume any responsibility for any loss or damage in the following circumstances:

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.
- Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.
- Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).

Contents

Preface

This document describes main functions and usage of the web-based manager of NSFOCUS Log Audit System ("LAS" for short).

This document is provided for reference only. It may slightly differ from the actual product due to version upgrade or other reasons.

Organization

Chapter	Description
Product Overview	Introduces the product functions, management methods, and device onboarding guide for the hardware version of LAS.
Message Center	Introduces how to view system messages.
User Center	Introduces methods for managing user accounts and roles.
Home	Describes how to view various statistical information on the homepage and access the homepage dashboard.
Log Analysis	Introduces methods for searching log information and viewing log monitoring information.
Log Source Management	Introduces how to view log source monitoring information and configure log source topology.
Event Alerts	Describes how to configure event rules and alert rules, and how to view event information.
Report Management	Introduces report generation and management methods.
Asset Management	Describes methods for configuring and managing assets.
System Management	Describes how to configure data collection, data management, system-related information, and fault diagnosis.
Audit Log	Introduces the methods for viewing and managing system audit logs.
Console Management	Describes the serial port management methods for LAS.
Default Parameters	Introduces the default configurations.
Device Access	Introduces the method for connecting linkage devices to LAS.
Communication Matrix	Describes devices supported by LAS for access and their version numbers.

Change History

Version	Description
V2.0R02IB00	Initial release.

Conventions

Convention	Description
Bold Font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
Italic Font	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
	Reminds users to take note.
	Indicates a tip to make your operations easier.
	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Technical Support

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Netherlands Toll: +31 85 208 2673 or +31 85 208 2NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Middle East: +973 1619 7607
- Hong Kong, China: +852 5803 2673 or +852 5803 2NSF

- Macao, China: +853 6825 8594
- Chinese Mainland: +86 10 5387 5981

Documentation Feedback

For any query regarding the usage of the documentation, you can contact us:

Email: info-support@nsfocus.com

1 Product Overview

With the continuous development of enterprise informatization, the number of corporate IT assets continues to increase, and the interconnectivity and complexity of systems continue to grow. However, the current information security landscape is becoming increasingly severe, and information security protection faces unprecedented difficulties and challenges. Currently, national policies, regulations, and industry standards have explicitly imposed requirements for log auditing. Log auditing has become an essential function for enterprises to meet compliance and internal control requirements. Log auditing can help users better monitor and safeguard the operation of information systems, timely identify intrusion attacks and internal violations targeting information systems, and provide necessary information for POST-event analysis and forensic investigation of security events.

The main contents of this chapter are as follows:

Function	Description
Product Introduction	Briefly describes the functionality of LAS.
Device Onboarding	Introduces the relevant steps and notes for installing and deploying LAS hardware devices.
Management Method	Introduces the management methods supported by LAS.

1.1 Product Introduction

NSFOCUS Log Audit System (LAS) is a comprehensive log management platform that can effectively manage various log data output from network assets. The main functions of LAS are as follows:

- Performs unified normalization on scattered, heterogeneous logs and provides multi-dimensional analysis tools to enable users to conduct comprehensive and efficient log O&M.
- Helps users identify various security risks hidden in logs, enabling users to locate, track, and investigate security issues in the network, ensuring smooth operation of user networks and business services.

1.2 Device Onboarding

This section is for the hardware version of LAS only. If you are using the virtualized version of LAS, please ignore this section.

1.2.1 Checking Accessories

Before installing LAS, unpack the accessory kit included with the device to verify that all accessories are included. The standard accessories vary by product model. For details, refer to the packing list. The main accessories are shown in Table 1-1.

Table 1-1 Main Accessories Included

Accessories	Description
Straight-through Cable (green)	When connecting to the network, a straight-through cable is required.
Crossover Cable (yellow)	When using a temporary computer to directly connect to the device's management interface and then log in to the web-based manager of LAS for configuration, it is recommended to use a crossover cable.
Power Cord	Each product is equipped with one or two power cords.
Foot Pad	Cut the rubber pad along the dotted line into 4 pieces. Peel off the non-stick paper and stick them to the four corners or marked positions on the bottom of the LAS hardware to prevent wear.
Rack Mount Ears	If you need to mount LAS on a rack, use the rack-mounting ears to secure it.
Rack Mounting Screws	Screws required for rack mounting.
Serial Cable	When configuring the serial console for LAS, the serial cable is required.

In addition to the items in the accessory kit, you need to complete the preparation items shown in Table 1-2.

Table 1-2 Preparation

Item	Description
IP Address	Reserve an IP address for LAS in the network.
Temporary Computer	Configuring LAS requires a computer for temporary management. When configuring, connect via network cable and log in to the web-based manager of LAS using HTTPS.
Endpoint Software	Terminal software capable of connecting to serial ports (such as hyper terminal software PuTTY).
Browser	• The screen resolution is recommended to be set to 1920*1080, with adaptive support for 1280*1024 and 1366*768. • Enable the browser property to allow popup Windows.

1.2.2 Environment Requirements

The environmental conditions required for operating the LAS device are shown in Table 1-3.

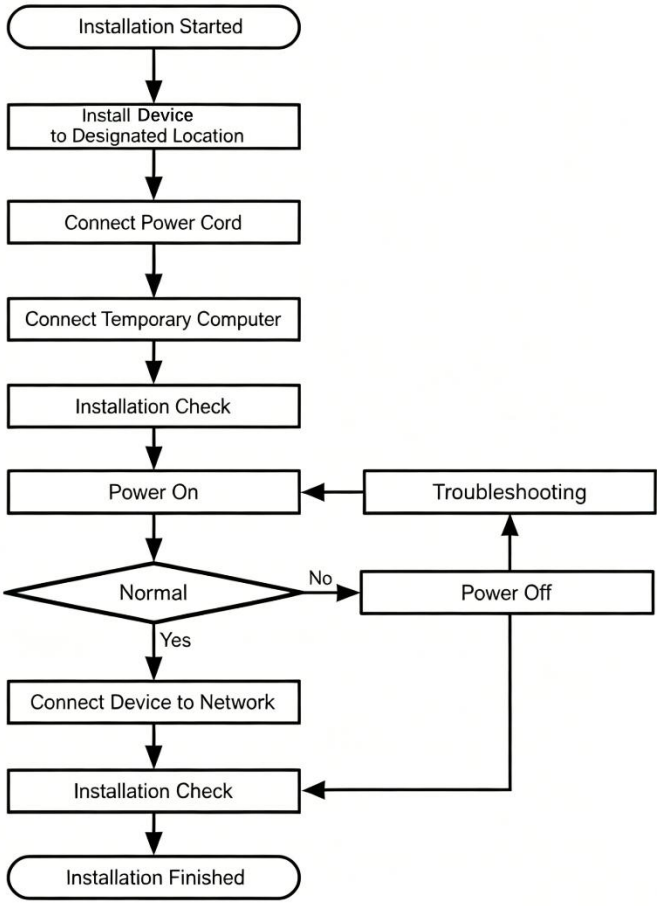
Table 1-3 Environment Requirements

Item	Description
Environment Requirements	• Ventilation and heat dissipation. • Temperature 0℃ to 45℃ • Relative humidity 10%~95% (non-condensing).
Anti-Static Requirements	• The equipment and floor are properly grounded. • Indoor dust protection. • Meets temperature and humidity requirements. • When handling circuit boards, wear anti-static gloves or an anti-static wrist strap.
Rack Installation Requirements	The rack is sturdy, with dimensions suitable for equipment installation.

1.2.3 Installation Process

The installation process of LAS device is shown in Figure 1-1.

Figure 1-1 Device Installation Process



1.2.4 Connecting Power

To connect an AC power cord, follow these steps:

Step 1 Set the switch of the power module to OFF.

Step 2 Plug one end of the supplied AC power cord into the AC power socket on the device, and the other end into an external AC power outlet.

Step 3 Set the power switch to ON.

Tip	Because the LAS device supports dual power supply, if only a single power supply is connected, the device will emit a beeping sound. To stop the beeping, press the button on the edge of the power interface.

Step 4 Check whether the status of the power indicator on the back panel of the device is normal; it displays when normal.

----End

1.2.5 Setting Default IP of Management Interface

In the factory default configurations, the default IP address and netmask of the LAS management interface are 10.1.1.1 and 255.255.255.0 respectively. During initial device setup, you can connect to your network and log in to the system after performing operations such as changing the default IP address of the management interface as needed (not mandatory), importing a certificate, and changing the administrator's initial password.

To modify the default IP address of the management interface, use the console user interface. For more details, see Network Configuration.

1.3 Management Method

Administrators can manage LAS devices using the following two methods:

- Web-based manager

  The web-based manager provides users with the most intuitive human-machine interaction management method and the most comprehensive function management interface. For details, see Web-based Manager.

- Console

  Perform simple configuration and management of LAS via the console. For details, see Console .

1.3.1 Web-based Manager

The following section describes the login method, page layout, and common operations of the web-based manager.

First-time Login

When logging in to LAS for the first time, follow the steps below:

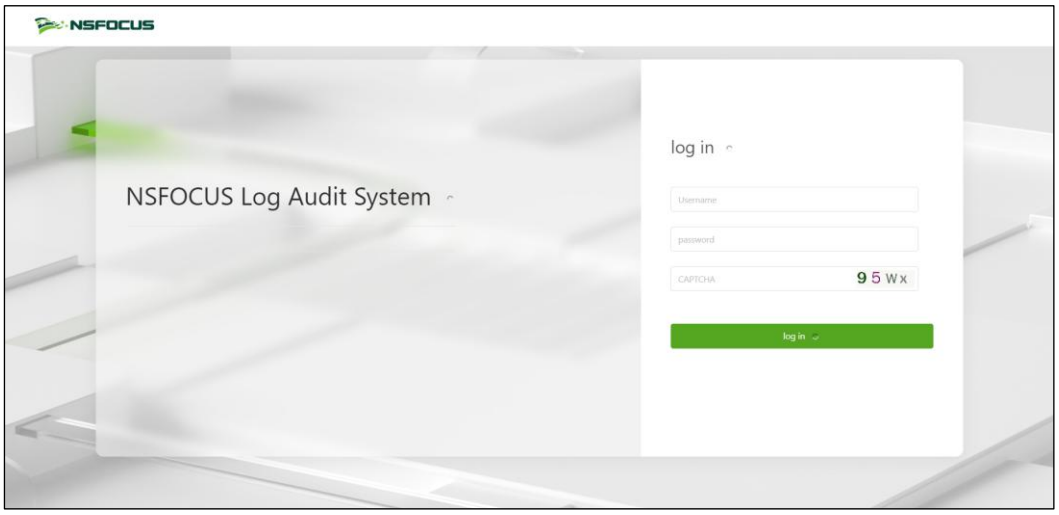
Step 1 Modify the IP address of the management computer so that the IP address is in the same network segment as the default IP address of the LAS management interface (for example: 10.1.1.2/24).

Step 2 Connect the network cable to the m interface of the LAS device, and directly connect the LAS device to the management computer.

Step 3 Open the browser, connect to the IP address of LAS management interface via HTTPS (for example: HTTPS://10.1.1.1), and after pressing **Enter**, a security alert appears.

Step 4 Click **Accept Risk and Continue** to enter the login interface shown in Figure 1-2.

Figure 1-2 Login Interface of LAS Web-based Manager



Step 5 Log in to LAS.

Enter the username and password of the default administrator, click **Log In**.

For default administrator username and password, see Initial User Account.

Step 6 (Optional) Modify the initial IP address of the management interface.

Log in to the console and modify this IP address. For details, see Console Login.

If no modification is required, skip directly to Step 8.

Step 7 (Optional) Log in to LAS using the new modified IP address.

Enter the default administrator's username and password and verification code, and click **Log In**.

Step 8 Import certificate when logging in for the first time.

a. Click **Import Certificate**.

b. Click **Select Certificate File**, and select a valid certificate file matching the device HASH value to finish the certificate import.

Step 9 Change the admin password when logging in for the first time.

Configure a new login password according to the password format and length requirements prompted on the interface, then click **Confirm Modification**.

Step 10 Log back in to the web-based manager of LAS using the new password.

----End

Web Page Layout

The page layout of each functional module is identical, as shown in Figure 1-3.

Tip	The menu and workspace in the page layout may vary depending on user permissions. Please refer to the actual page display for specific details.

Figure 1-3 Page Layout

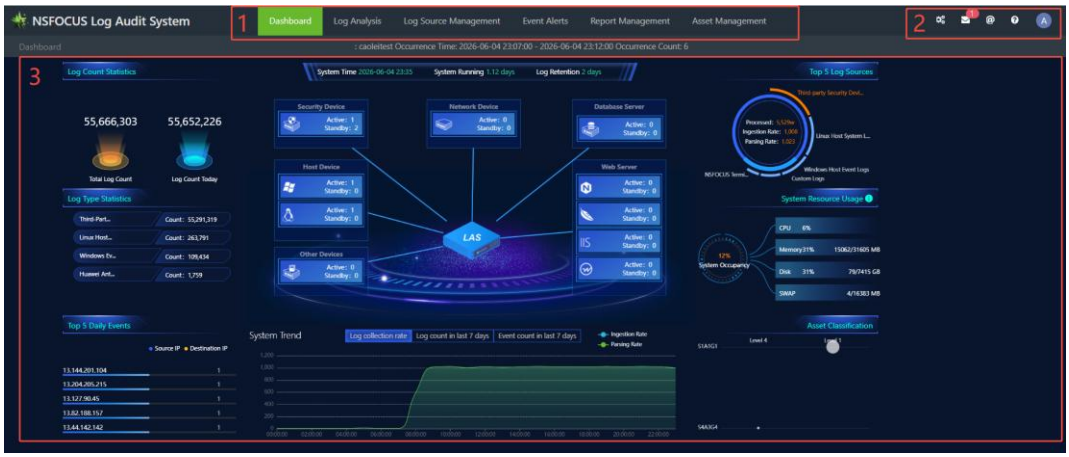


Table 1-4 Page Layout Description

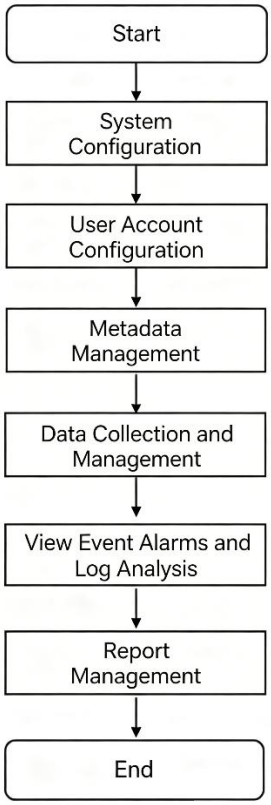
No.	Area	Description
①	Menu bar	The level-1 navigation of LAS. Hover over a menu to display the corresponding level-2 menu.
②	Quick access toolbar	The specific explanations from left to right are as follows: • : Only supports full-screen display of the homepage dashboard. Press the **Esc** key to exit full-screen mode. For more details, see Quick Operations. • : Enter the console for management operations. See System Management. • : Enter the Message Center. The number in red indicates the count of unread messages. For details, see Message Center. • : View more information. • : View online help. • : Includes the following three functions. ✓ Screen lock: locks the web-based manager of LAS, temporarily preventing other users from logging in; only the currently logged-in user can unlock it. ✓ Enter the User Center: manages the account information of the currently logged in user. For admin users, it also supports managing all accounts and roles. See User Center. ✓ Log out of the system.

No.	Area	Description
③	Workspace	Configuration, operation, and browse for various functions are all performed in this area. If alert rules are enabled, alert information will scroll at the top of the workspace. For how to configure alert rules, see Alert Rules.

Configuration Process

The recommended configuration process for LAS is shown in Figure 1-4.

Figure 1-4 Configuration Process



1.3.2 Console User Interface

By connecting to the console, users can access the serial management interface of LAS. This interface provides functions such as system initial configuration, status detection, and restoring initial configuration. Management operations that cannot be performed in the web-based manager can be performed here.

- For serial port communication parameters and initial username and password, see Console Communication Parameters.
- For the login and operations of the console, see Console Management.

2 Message Center

LAS Message Center displays notification messages requiring your attention. The following situations trigger these notification messages:

- Device registration, device status changes, and device deletion.
- Certificate expiration and notifications.
- Operations monitoring alerts.
- FTP/SFTP, email sending failures.

When notification messages are triggered, the number of notification messages will appear on the quick access toolbar. Click the message icon () to enter the **Unread Messages** page, as shown in Figure 2-1.

Figure 2-1 Message Center

Viewing Messages

Click **Read Messages**/**Unread Messages** to view the read messages or unread messages.

Configuring Message Notifications

Click **Notification Settings** to configure message notification policy parameters. Parameter descriptions are shown in Table 2-1.

Table 2-1 Message Notification Policy Parameters

Parameter		Description
Basic Settings	Message Type	The message type that generates notifications. Options include **System**, **Collection**, and **Certificate**. Multiple selection is allowed.
	Message Level	The message security level for generating notifications. Available options are **High**, **Medium**, and **Low**.
Notification	Email	Whether to enable email notifications. After enabling,

Parameter		Description
Method	Notification/Email Address	configure the email address for receiving notification emails. To enable email notifications, you must first complete Configuring Mail Server.
	SMS Notification/Mobile Number	Whether to enable SMS notifications. After enabling, configure the phone number for receiving SMS notifications. To enable SMS notifications, you must first complete Configuring SMS Server.
System/Collection Notification Suppression	Time Interval	When the message type is **System** or **Collection**, you must configure this item. The system consolidates notifications for identical message content of system/collection types. Within the configured time interval, when identical events occur, the system will not send repeated notification messages. Valid range is 5~60 minutes.
Certificate Notification Suppression	Time Interval	When the message type is **Certificate**, you must configure this item. The system consolidates notifications for certificate-related messages. Within the configured time interval, if identical events occur, the system will not send repeated notification messages. Set the time interval. Available options are: **Within Three Days**, **Within a Week**, and **Within a Month**.

3 User Center

A user account consists of two elements: role and permission.

- A single user account can contain permissions from multiple roles. When an account has multiple roles, its permissions are the combination of all role permissions.
- A role refers to a collection of users with a specific set of functions and permissions.

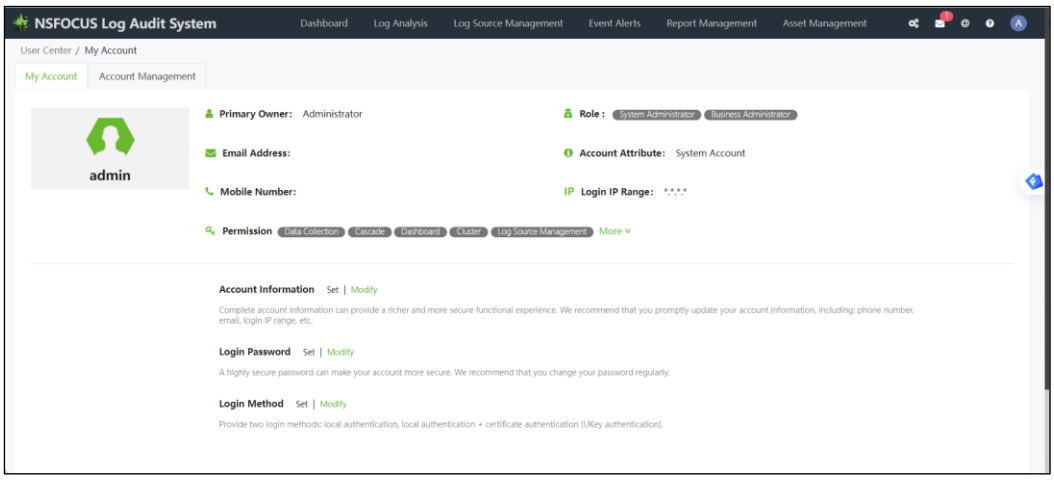
  The default system roles in LAS include audit administrator and system administrator. The default system account in LAS is the system administrator. These default system roles and system accounts cannot be deleted or edited.

3.1 My Account

The steps for the currently logged-in user to manage his or her own account information are as follows:

Step 1 Hover over the icon in the quick access toolbar, select **User Center** to enter the **My Account** page, as shown in Figure 3-1.

Figure 3-1 My Account



Step 2 Edit account information.

a. Click **Modify** in the **Account Information** area, and configure the account information. For parameter descriptions, see Table 3-2.

b. Click **OK**.

Step 3 Change the login password.

a. Click **Modify** in the **Login Password** area, and configure the old password, new password, and confirm the new password. For parameter descriptions, see Table 3-2.

b. Click **OK**.

Step 4 Modify the login method.

a. Click **Modify** in the **Login Method** area, and configure the login authentication method. For parameter descriptions, see Table 3-3.

b. Click **OK**.

----End

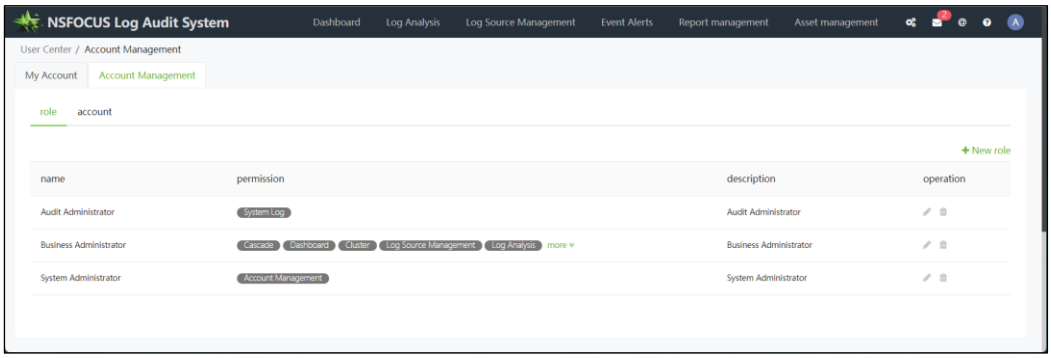
3.2 Account Management

Account management includes role management and account management.

3.2.1 Role Management

Hover over the quick access toolbar, select **User Center**, and navigate to **Account Management > Role**. By default, system built-in roles are displayed, as shown in Figure 3-2.

Figure 3-2 Role Management



Creating a Role

In the **Role** tab page, click **New Role** and configure role parameters. For parameter descriptions, see Table 3-1.

Table 3-1 Role Parameters

Parameter	Description
Name	Enter the role name.
Permissions	Select the operation permissions by system modules.
Description	Enter the role description.

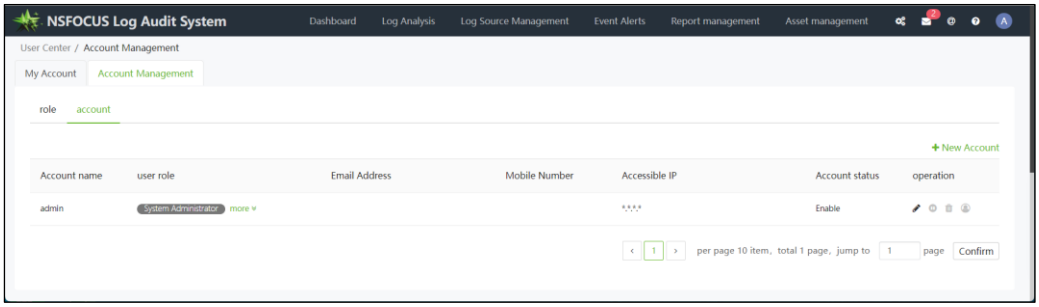
Caution	• After deleting a role, the bindings between the role and user accounts will also be deleted. • Built-in system roles cannot be edited or deleted.

3.2.2 Account Management

The user accounts of LAS consist of built-in system accounts and custom accounts. The built-in system account is admin, with default user roles of "system administrator" and "service administrator", and has account management permissions including creating custom accounts, modifying account information and passwords, modifying account login methods, enabling/disabling accounts, and unlocking accounts.

Hover over the quick access toolbar, choose **User Center**, and navigate to **Account Management > Account**, which displays system built-in accounts and custom accounts, as shown in Figure 3-3.

Figure 3-3 Account Management



Creating an Account

In the **Account** tab page, click **New Account**, and configure account parameters. Parameter descriptions are shown in Table 3-2.

User accounts with account management permissions can add new user accounts, modify account information and passwords, modify account login methods, enable/disable accounts, and unlock accounts. The icon descriptions are shown in Table 3-3.

Table 3-2 Account Parameters

Parameter	Description
Account Name	The account name must be unique in the system. The value range is from 6~20 characters, consisting of letters, numbers, and underlines, and must start with a letter.
Password	Account passwords support two methods: • **Default Password**: use the default password as the account's log-in password. The default password is the configured account name.

Parameter	Description
	• **Custom Password**: use a user-defined password as the account's login password. The value ranges from 8 to 32 characters, consisting of uppercase letters, lowercase letters, numbers, and special characters, and must contain both letters and numbers.
Primary Owner	Name of the primary owner for this account.
Email Address	Email address bound to the account.
Mobile Number	Mobile phone number bound to the account.
Role & Permission	Roles and permissions bound to the account. After selecting a role, proceed to select permissions for the selected role. Multiple selection is supported. When an account has multiple roles, the account's permissions are the combination of the permissions from those roles.
Login IP Range	Restricts the IP address range for account logins, supporting both IPv4 and IPv6. Separate multiple IP ranges or independent IPs using ",", ";", the enter or space key. The format of IP address and range is as follows: • 192.168.0.1 • 192.168.1.1/8 • 2001:470:23:a23:0:0:0:3 • ::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Account Management Operations

Account management operations are shown in Table 3-3.

Table 3-3 Account Management Operations

Icon	Description
	Configure parameters other than account name. • Accounts with account management permissions can reset passwords for all custom accounts. • Accounts without account management permissions can only modify their own passwords.
	Activate/Deactivate accounts. Only activated accounts can log in to LAS. To avoid frequent deletion and addition of accounts, if an account is temporarily not needed, you can deactivate it.
	Delete accounts. After deletion, account-related data permissions will be automatically revoked.
	If the number of failed login attempts for an account exceeds the threshold, the account will be locked. Other accounts with account management permissions can unlock locked accounts and restore them to active status.
	Set the login authentication method for the account. Available options include **Local Authentication**, **Local Authentication + Certificate Authentication**. For how to switch the authentication methods, see Switching Authentication Method.

Caution	The account information and login methods of system built-in accounts cannot be edited. System built-in accounts cannot be deleted.

4 Homepage

The main contents of this chapter are as follows:

Function	Description
Quick Operations	Introduces quick operation methods for the dashboard.
Dashboard	Describes how to view the dashboard.

4.1 Quick Operations

After successfully logging in to LAS, click on the upper-right corner of the Homepage to enter the full-screen display mode for the dashboard. When entering full-screen mode for the first time, the system will display a prompt showing how to find the **Esc** key to exit full-screen mode; click **OK** to continue.

4.2 Dashboard

Navigate to the homepage to view various statistics of LAS, as shown in Figure 4-1. The information displayed in the dashboard is described in Table 4-1.

Figure 4-1 LAS Dashboard

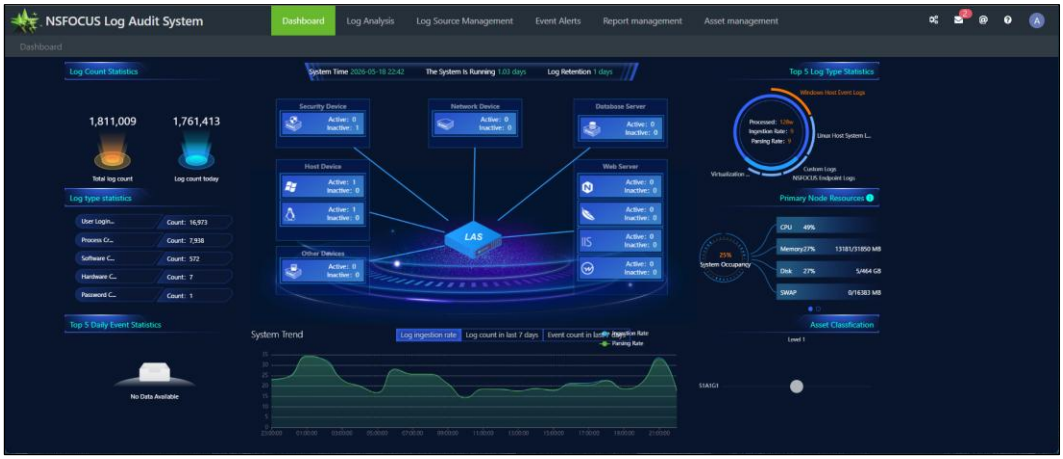


Table 4-1 Homepage Dashboard Display Information

Display Item	Description
Comprehensive Data Statistics	The top center of the large screen displays comprehensive statistical data, including the current system time, system uptime, and log retention days.
Topology Diagram	Display custom network topology diagrams.
Log Count Statistics	• **Total Log Count:** displays the total number of all logs received by LAS up to the current time. • **Log Count Today:** displays the total number of logs received by LAS on the current day.
Log Type Statistics	Scrolling display of log types ingested into LAS in real-time and their total counts.
Top 5 Daily Event Statistics	Display the 5 most recent LAS events in a list, in descending order by event time. Click **Source IP**/**Destination IP** to switch between the source IP/Destination IP display page.
Top 5 Log Type Statistics	Displays the top 5 log ingestion status by type in a ring chart, including processed log count, log ingestion rate, and log parsing rate. Click the legend to display statistics for the corresponding category.
System Resource Usage (Standalone Mode Only)	Display real-time usage of system resources, including CPU, memory, disk, and SWAP usage percentages and storage space usage. To view the log storage duration, you must perform log integration. For details, see Log Ingestion.
Asset Classification	Displays MLPS levels of assets in a scatter chart. Hover over the scatter chart to view specific statistical data.
System Trend	Displays the following content in a line chart. Hover over the chart to view specific statistical data. • **Log Ingestion Rate:** displays the trend of log ingestion and log parsing rate changes over the last 24 hours. • **Log count in last 7 days:** displays the trend of daily log count changes over the last 7 days. • **Event count in last 7 days:** displays the daily event count changes over the last 7 days.
Primary Node Resources (Cluster Mode Only)	Displays real-time resource usage of LAS primary node, including CPU, memory, disk, and SWAP usage.
Secondary Node Resources (Cluster Mode Only)	Displays real-time resource usage of LAS secondary node, including CPU, memory, disk, and SWAP usage.

5 Log Analysis

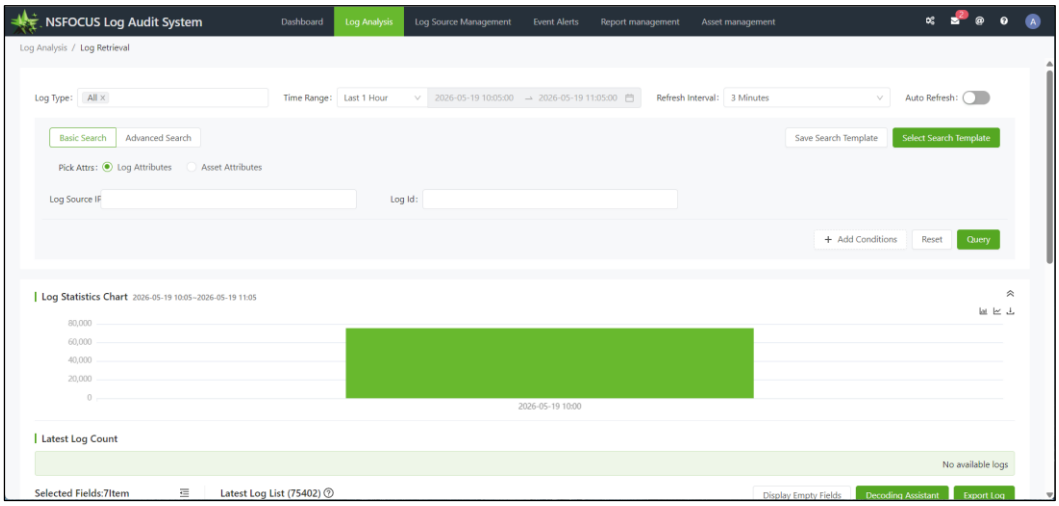
The main contents of this chapter are as follows:

Function	Description
Log	Introduces log search methods, including basic search, advanced search, quick search by selecting search templates, saving search conditions, configuring log list, and exporting logs.
Host Audit Analysis	Introduces methods for analyzing host audit logs and viewing analysis results.
Web Server Log Analysis	Describes methods for analyzing web server logs and viewing analysis results.
Configuring Custom Dashboard	Introduces methods for customizing dashboards.

5.1 Log Retrieval

Choose **Log Analysis > Log Retrieval**, which by default displays all logs retrieved in the last 1 hour, as shown in Figure 5-1.

Figure 5-1 Log Retrieval



Tip	You can click **Decoding Assistant** to quickly escape strings in the original log text that need to be decoded.

Table 5-1 Log Retrieval Page Layout Description

Area	Description
Log Type	All log types are selected by default. You can also select log types to search. Multiple selection and fuzzy search by log type name are allowed.
Time Range	Select the time range for log generation. Options include **Last 1 Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, and **Customize**.
Refresh Interval	The auto-refresh function is disabled by default. Press the **F5** key to manually refresh page information. To enable the auto-refresh function, first select a refresh interval (available options are **3 Minutes**, **5 Minutes**, **10 Minutes**, and **30 Minutes**), then turn on the auto-refresh switch.
Log Search Conditions	• Set search conditions via basic search and advanced search. After setting search conditions, you can click **Save Search Template** to save the current search conditions as a template. For details, see Basic Search/Advanced Search. • Supports selecting search templates for quick retrieval. For details, see Using Search Template. Fuzzy search is allowed.
Log Statistics Chart/Latest Log Count/Latest Log List	After log retrieval, the log statistics chart, latest log count, and latest log list are displayed. • **Log Statistics Chart:** displayed by default. Click the expand icon to display a trend chart showing the number of logs matching the criteria by time; hovering over the chart displays specific times and their corresponding log counts. Click the collapse icon to hide the log statistics

Area	Description
	chart. Click the icon on the right side of the statistics chart to perform the following operations. -  : Switch to column chart. -  : Switch to line chart. -  : Save the current log statistics chart as a PNG file. • **Latest Log Count:** click **Export Log**. When export is complete, click **Download Log** to download the exported logs to your local machine. • **Latest Log List:** displays log details matching the search criteria. For details, see Log Management Operation.

5.1.1 Basic Search/Advanced Search

LAS log retrieval supports both basic search and advanced search.

Choose **Log Analysis** > **Log Retrieval**, set the log query conditions, and then click **Query** to perform a search. The page displays search results by default in the form of a log statistics chart, latest log count, and latest log list. Query condition descriptions are shown in Table 5-2.

Table 5-2 Log Query Conditions

Querying Item		Description
Basic Search	Attribute	• **Log Attribute:** set log query conditions to query corresponding logs. Different log types have different query conditions. For details, see Table 5-3. • **Asset Attribute:** select the asset's IP address and asset tags to query logs.
	Add Condition	When the selected attribute is **Log Attribute**, you can add search conditions. Click **Add Condition**, select the search conditions, then click **OK** to add the conditions. Multiple selection is allowed.
	Asset IP	When the selected attribute is **Asset Attribute**, you can select an asset IP address for querying. Fuzzy search is allowed.
	Tag	When the selected attribute is **Asset Attribute**, you can specify asset tags for querying. Multiple selection is allowed.
Advanced Search	Customized Retrieval	To further refine query results, click the search text box and enter custom search criteria.

Table 5-3 Basic Query Conditions by Log Attribute (Regular Search)

Querying Item		Description
All	Log Source IP	IP address of the log source device.
	Log ID	ID of each log item.

Querying Item		Description
NSFOCUS Security Device Log	Log Source IP	IP address of the log source device.
	Source/Destination IP	Source/Destination IP addresses in logs.
NSFOCUS Terminal Log	Log Source IP	IP address of the log source device.
Third-Party Security Device Log	Log Source IP	IP address of the log source device.
	Source/Destination IP	Source/Destination IP addresses in logs.
	Source/Destination Port	Source/Destination port numbers in logs.
Network Device Log	Log Source IP	IP address of the log source device.
	Source/Destination IP	Source/Destination IP addresses in logs.
	Source/Destination Port	Source/Destination port numbers in logs.
Database Data	Log Source IP	IP address of the log source device.
Windows Host Event Log	Log Source IP	IP address of the log source device.
	User	User name in the log.
	Operation	Operation performed on the host in the log.
	Log Name	Name of the log.
Linux Host System Log	Log Source IP	IP address of the log source device.
	Log Name	Name of the log.
Web Server Log	Log Source IP	IP address of the log source device.
	Client IP	Client IP address recorded in the log.
	Protocol Version	Protocol version number in the log.
	Request Method	Method to send requests to the web server.
	Status Code	Status code of the web server's response to a request.
Virtualization Platform Log	Log Source IP	IP address of the log source device.
Network Device Traffic	Log Source IP	IP address of the log source device.
	Source/Destination IP	Source/Destination IP addresses in logs.
	Source/Destination Port	Source/Destination port numbers in logs.
Custom Logs	Log Source IP	IP address of the log source device.

Tip	The basic query parameters differ slightly depending on log types. Please refer to the web interface for specific parameters.

5.1.2 Saving Search Template

LAS supports manually saving the search conditions used for Basic Search/Advanced Search, allowing users to perform multiple searches on logs that meet those conditions.

Choose **Log Analysis > Log Retrieval**, and configure search conditions. Click **Save as Search Template**, configure the name of the search template (up to 30 characters). Click **OK**.

After saving log search criteria, quick search can be performed. For details, see Using Search Template.

5.1.3 Using Search Template

LAS supports using search templates as search criteria to quickly search for logs that match the conditions.

Choose **Log Analysis > Log Retrieval**, click **Select Search Template** on the right side of the page to select a template, and click **Query** to quickly search logs.

Searching templates support the following management operations:

- Click **Query** in the **Operation** column to search logs based on the search criteria of the current search template.
- Click **Pin to Top** in the **Operation** column to pin the corresponding search template and set the log type of focus for quick retrieval.
- Click **Delete** in the **Operation** column to delete the search template.

5.1.4 Log Management Operations

Choose **Log Analysis > Log Retrieval**. After performing a log query, you can view details and perform management operations in the latest log list at the bottom of the page.

Viewing Log Details

In the latest log list, click the add icon next to a log entry to expand and view its detailed content. Log details can be displayed in both table and JSON formats. The following operations are also supported:

- Extract fields from the log for configuring field extraction rules. For details, see Configuring Field Extraction Rules.
- Configure event rules and add filter conditions for unparsed logs. For details, see Creating Event Rule.

Configuring Fields for Log List Display

Click the  icon to control the display content of the log list by selecting fields. In the columns of the selected fields, hover over a field and drag up or down to adjust its order, which changes the display order of log fields in the latest log list.

Searching Logs Based on Log Fields

In the latest log list, click the search icon next to the log list header, enter search terms, click **Search**, to perform a search on the retrieved logs.

Showing/Hiding Empty Fields

Click **Show Empty Fields**, and the log list will display the empty fields of the retrieved logs, while it changes to **Hide Empty Fields**. Click this again, and the log list will hide the empty log fields.

Exporting Logs

Click **Export Log** and configure parameters to export all logs in the current log list. The log export parameter description is shown in Table 5-4.

Table 5-4 Log Export Conditions

Parameter	Description
Set Password	The decompression password for the exported log file. If not set, the default password is **las123456**.
Export Format	• **Generate a file daily for each log type:** one file is generated per day for each log type. • **Generate only one file for each log type:** only one file is generated for each log type.
Export Fields	This parameter is required only when a single log type is selected in the log retrieval. Select the log fields to export. Multiple selection is allowed.
Export Raw Log	This parameter is required only when all log types are selected in the log retrieval. Select whether to export the text of the "raw_data" field. • **Yes:** export the text of the "raw_data" field. • **No:** the "raw_data" field is empty.

Tip	• When all log types are selected, to ensure export efficiency, LAS with 16 GB memory supports exporting up to 500 log entries at one time; if the selected data exceeds 500 entries, only the most recent 500 entries can be exported. LAS with 32 GB memory supports exporting up to 1000 entries at one time; if the selected data exceeds 1000 entries, only the most recent 1000 entries are exported. • When a single log type is selected, to ensure log export efficiency, LAS with 16 GB memory supports exporting up to 500,000 log entries at one time. If the selected data exceeds 500,000 entries, only the most recent 500,000 entries can be exported. LAS with 32 GB memory supports exporting up to 1,000,000 entries at one time. If the selected data exceeds 1,000,000 entries, only the most recent 1,000,000 entries can be exported. • If you need to export more logs, it is recommended to export them in batches.

After enabling log export, the log export progress will be displayed in the **Latest Log Count** area. After the export is complete, click **Download Log** to download the exported logs locally.

5.2 Host Audit Analysis

LAS supports online analysis of host logs. The analysis results include login overview audit, critical file/folder monitoring, critical service monitoring audit, sensitive operation execution audit, abnormal network outbound connection audit, and account password changes.

Before using this function, click **Agent Data Collection** to add log collection policies, and obtain the host logs for analysis. For details, see Agent.

Choose **Log Analysis > Host Audit Analysis**, specify the time range, and click **Start Analysis**; after the log analysis is complete, the page displays log analysis results for the specified time range, as shown in Figure 5-2, with the description of host audit analysis results shown in Table 5-5.

Figure 5-2 Host Audit Log Analysis

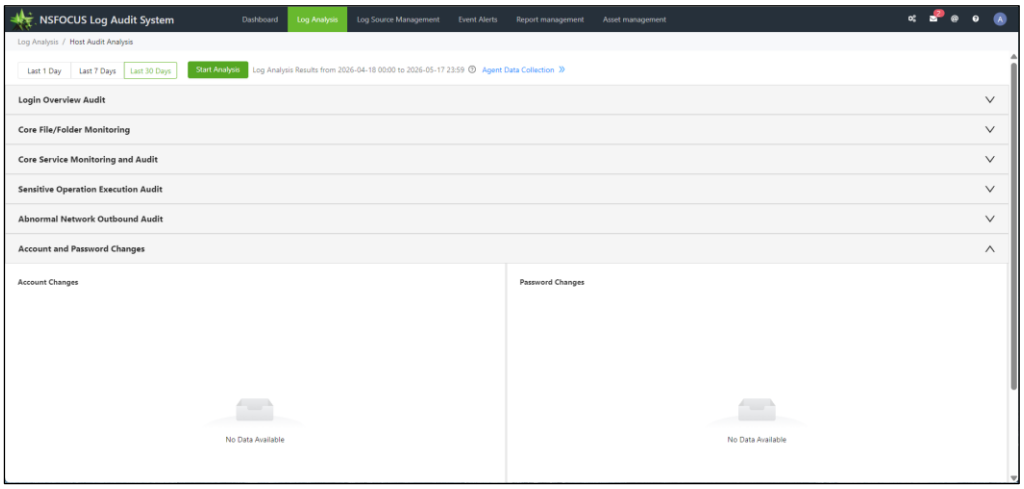


Table 5-5 Host Audit Analysis Results

Display Item		Description
Login Overview Audit	Top 10 IP Distribution of Failed Logins	For host logs, it displays the top 10 IP addresses and their counts of failed login attempts within a specified time frame, used to assist in detecting suspected password brute-force attacks. When a certain IP exhibits a large number of login failures, it is suspected to be a brute force attack.
	Top 10 IP Distribution of Logouts	For host logs, it displays the top 10 IP addresses and logout counts within the specified time frame to analyze current abnormal login/logout in a visualized way.
	Top 10 IP Distribution of Successful Logins	For host logs, it displays the top 10 IP addresses and their counts for successful system logins within a specified time frame to analyze the IP address distribution involved in successful logins in a visualized way.
	Top 10 Account Distribution of Successful Logins	For host logs, it displays the top 10 accounts and their counts of successful system logins within the specified time frame to analyze the account distribution involved in successful logins in a visualized way.
	Time Distribution of	For host logs, it displays the time distribution of frequent successful

Display Item		Description
	Frequent Successful Logins	logins within a specified time frame to analyze the time periods when successful logins concentrate.
	Time Distribution of Frequent Failed Logins	For host logs, it displays the time distribution of frequent failed logins within a specified time frame to assist in detecting the time periods when suspected brute-force attacks concentrate.
Core File/Folder Monitoring	Linux Host Startup File Monitoring	The auto-start file **/etc/rc.d/rc.local** is a sensitive core file on Linux. When the system boots, it automatically executes the relevant commands recorded in the file. For host logs, it displays detailed change records for the last 10 boot startup files within the specified time frame.
	Linux Host User Information File Monitoring	The user information file **/etc/shadow** is a sensitive core file on Linux, recording related information about host users. For host logs, it displays detailed change records of the most recent 10 changes to user information files within the specified time frame.
Core Service Monitoring and Audit	Registry Audit Monitoring	The registry is the host's core service configuration, used for service start/stop control and core permissions. It displays detailed change records for the most recent 10 registry modifications within the specified time frame.
	Linux Crontab Monitoring	The crontab file is the host's core service configuration, used for periodically executing commands in the crontab file. It displays detailed change records for the last 10 crontab file modifications within the specified time frame.
Sensitive Operation Execution Audit	User Distribution of su or sudo Privileged Command Execution	Displays the user distribution of su/sudo privileged command executions (for privilege escalation by non-root users) within a specified time frame, to help identify whether corresponding users are abusing command execution privileges.
	IP Distribution of chmod/chown Sensitive Operation Execution	Displays the IP distribution of chmod and chown command executions (used to modify access permissions and ownership of files or directories) within the specified time frame.
Abnormal Network Outbound Audit	Host Distribution of Network Outbound Behaviors	Displays the top 10 hosts and their counts for network outbound connections within the specified time frame. Network outbound connection refers to a special access scenario where a host may access IP addresses in external networks. If the current host belongs to an internal network system, such an outbound connection request is considered an anomalous scenario, suspected of involving attack behavior, and requires further analysis.
Account and Password Changes	Account Changes	For host logs, it displays detailed records of the last 10 account changes within the specified time range.
	Password Changes	For host logs, it displays detailed records of the last 10 user password changes within the specified time range.

5.3 Web Server Log Analysis

LAS supports online analysis of web server logs. The analysis results include overall overview analysis, visitor analysis, request key points, security audit analysis, and response result analysis.

Before using this function, ensure that LAS has been connected to web server logs. For details, see Collecting Web Server Logs.

Choose **Log Analysis > Web Server Log Analysis**, select a time frame, click **Start Analysis**, wait for the log analysis to complete; after completion, the page displays the web server log analysis results for the specified time frame, as shown in Figure 5-3, and the web server log analysis result description is shown in Table 5-6.

Figure 5-3 Web Server Log Analysis

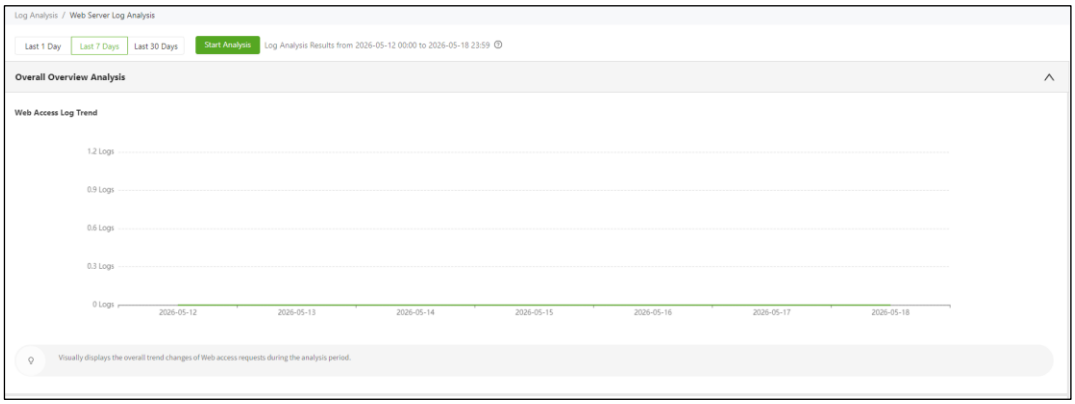


Table 5-6 Web Server Log Analysis Results

Display Item		Description
Overall Overview Analysis	Web Access Log Trend	Displays the overall trend of web access request count within a specified time frame.
	Top 10 Request Access Result Distribution	Displays the result types and counts of the top 10 web access request results within a specified time frame, used for analyzing the operating status of currently connected web servers.
Visitor Analysis	Visitor Request IP Distribution	Displays the top 10 IP addresses and their web access request counts within a specified time frame, used to analyze the list of most frequent visitors to currently connected websites.
	Top 10 Hot Resource URLs	Displays the top 10 popular resources and their request counts by web access request count within a specified time frame, used to analyze hotspot resources of currently connected websites.
Request Key Points	Top 10 Request Browser Type Distribution	Displays the top 10 browser types and their counts by web access requests initiated within a specified time frame, used to analyze the client type distribution of currently connected websites.
	Referer Distribution of Web Access Requests	Displays the distribution of the referer field in web access requests within the specified time frame. Referer is a field in the HTTP request header that describes the request source. It can be used to analyze user sources for the currently connected website.

Display Item		Description
	Forward Address Distribution of Web Access Requests	Displays the distribution of forwarding addresses for web access requests with 3XX response codes (generally serve request redirections) within a specified time frame.
Security Audit Analysis	Visitor IP Distribution of 404 Request Status	Displays the top 10 IPs and their counts by 404 responses within a specified time frame. In web access requests, if a visitor IP produces a large number of 404 access requests, that visitor IP is a suspected malicious scanning IP.
	Access Scope Distribution of Suspected Malicious Scanning IP	When a visitor IP generates a large number of 404 access requests in web access and exceeds the configured threshold, the access scope of the suspected malicious scanning IP will be analyzed.
Response Result Analysis	URL Request Distribution with Request Bytes Exceeding 5KB	In web access requests, the request byte size is typically below 5KB. When it exceeds 5KB, analysis is required to determine whether there is suspected ddos behavior. Displays URLs and request counts with size exceeding 5KB within a specified time frame.
	Successful URL Request Distribution with 0KB Response Bytes	For web access requests, if there are cases where requests succeed but the response byte count is 0, you need to analyze whether this is normal behavior. Display URLs and request counts with 0-byte responses within a specified time frame.

5.4 Configuring Custom Dashboard

LAS supports displaying key log analysis of interest through configuring dashboards.

Configuring a dashboard refers to adding statistical items to groups and configuring a statistical time frame for each statistical item to view logs. In addition to the system default groups, LAS supports up to 20 custom dashboards.

The steps for configuring a custom dashboard are as follows:

Step 1 Choose **Log Analysis > Custom Dashboard**. Initially, there is only one default group.

Step 2 Click the + icon at the upper-right corner of the page to add a group, fill in the group name (up to 10 characters), and click **Confirm**.

Step 3 Select **Edit Chart**, and configure the widgets of the dashboard.

a. Select statistical items.

Select statistics items from the list in the left pane (supports multi-select and fuzzy search). The selected statistics items are displayed in the list on the right side. Click **Next**.

b. Select time frame.

- Configure the statistics time frame separately for selected statistics items. Batch operations are supported.
- Click **Finish** to save the configuration.

Step 4 After the widget is created, hover over a group to display operation icons.

a. Click the icon to configure the refresh frequency for the corresponding widget (unit: seconds).
   - **0** indicates no auto-refresh.
   - Value range is 0~180 seconds.

b. Click the icon to display the corresponding widget in full screen.

----End

6 Log Source Management

The main contents of this chapter are as follows:

Function	Description
Monitoring Log Source	Introduces how to view log source monitoring information by collectors and assets.
Monitoring Collected Asset	Introduces monitoring and analysis methods for log source assets.
Log Source Topology	Introduces how to draw the topology diagrams of log sources.

6.1 Monitoring Log Sources

LAS supports log source monitoring by collectors and assets.

6.1.1 Collector-Level Monitoring

LAS supports selecting a collector and viewing monitoring data for the specified collector.

Choose **Log Source Management > Log Source Monitoring**. By default, the monitoring information for the collector is displayed. The top of the page supports switching between collectors, as shown in Figure 6-1. The description of log source monitoring information at the collector level is shown in Table 6-1.

Figure 6-1 Log Source Monitoring (Collector-Level)

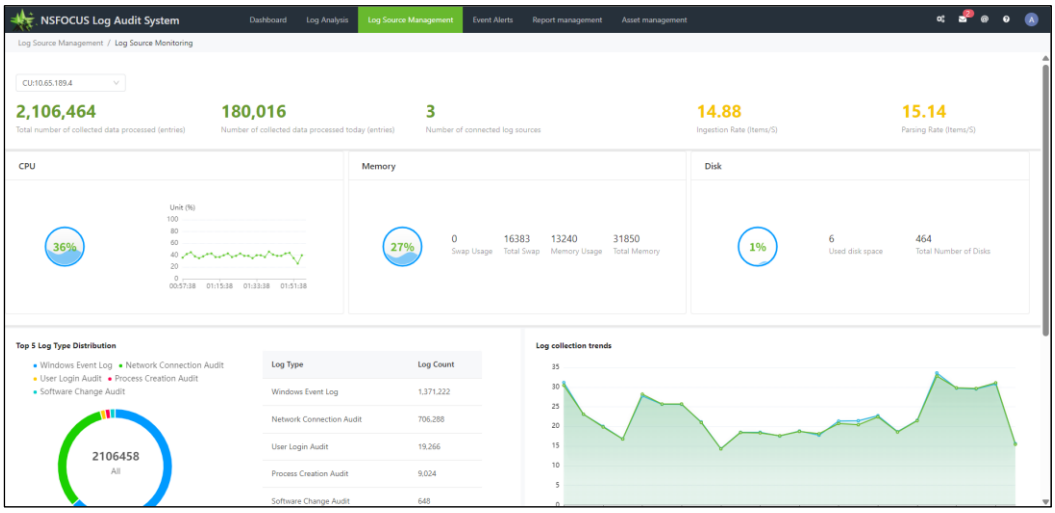


Table 6-1 Log Source Monitoring by Collector

Display Item	Description
Total Number of Collected Data Processed	Displays the total number of logs processed by the current collector (unit: entries).
Number of Collected Data Processed Today	Displays the total number of logs processed that has been processed by the current collector today (unit: entries).
Number of Connected Log Sources	Displays the number of log sources currently connected to the collector.
Ingestion Rate	Displays the current log ingestion rate of the current collector (unit: entries/second).
Parsing Rate	Displays the total log normalization rate for the current collector (unit: entries/second).
CPU	Displays the CPU usage of the current collector (unit: %), including the CPU usage percentage and a trend chart of CPU usage over the last hour.
Memory	Displays the memory usage of the current collector (unit: MB), including memory usage percentage, SWAP used, total SWAP, used memory, and total memory.
Disk	Displays the current disk usage of the collector (unit: GB), including disk usage percentage, used disk space, and total disk space.
Top 5 Log Type Distribution	Displays the top 5 log types by log count for the current collector, including the log type distribution chart and log type quantity list. Click the legend to hide/show the statistics for the corresponding category in the chart. Hover over the chart to view specific statistical data.
Log Collection Trend	Displays the log collection trend of the current collector as an area chart. Click the legend to toggle and display the following content: • **Ingestion Rate**: trend of log ingestion rate changes over the last 24 hours. • **Parsing Rate**: trend of log parsing rate changes over the last 24 hours.

Display Item	Description
	• **Total Log Count**: trend of log count changes over the last 30 days. Hover over the chart to view specific statistical data.
Monitoring Alerts	Displays the 5 most recently collected monitoring alerts from the current collector in list format, including risk level + alert name, alert content, and alert time. Click **View More** to go to the Message Center. For details, see Message Center.
Key Assets	Displays all connected log source assets. The displayed information includes asset IP, number of log sources, total number of logs (unit: entries), ingestion rate (unit: entries/s), parsing rate (unit: entries/s), and storage rate (unit: entries/s). Click an asset IP to view the asset-level log source monitoring information. For subsequent operations, see Asset-Level Monitoring.

6.1.2 Asset-Level Monitoring

Choose **Log Source Management > Log Source Monitoring**. In the key assets list, click an asset IP to view its log source information, as shown in Figure 6-2. The description of asset-level log source monitoring is shown in Table 6-2.

If the current asset belongs to multiple log sources, more collection information appears at the top of the page. Hover over it to view more source information.

Figure 6-2 Log Source Monitoring (Asset-Level)

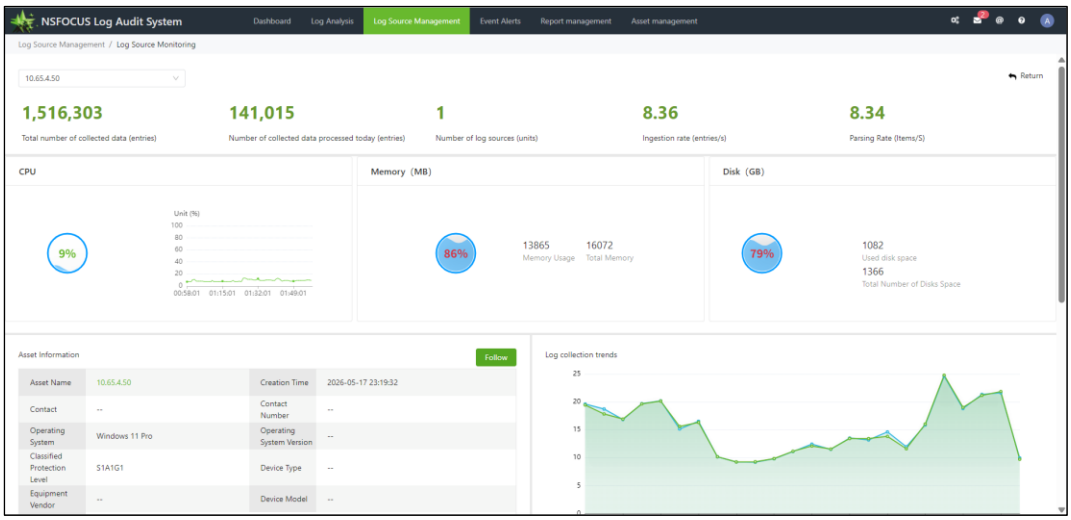


Table 6-2 Log Source Monitoring by Asset

Display Item	Description
Total Number of Collected Data	Displays the total number of logs for the current asset (unit: entries).
Number of Collected Data	Displays the number of collected data that has been processed for the current

Display Item	Description
Processed Today	asset today (unit: entries).
Number of Log Sources	Displays the number of log sources connected to the current asset.
Ingestion Rate	Displays the total log ingestion rate of the current asset (unit: entries/second).
Parsing Rate	Displays the total log normalization rate for the current asset (unit: entries/second).
CPU	Displays the CPU usage of the current asset (unit: %), including CPU usage percentage and a trend chart of CPU usage over the last 1 hour. Note This item is displayed only when CPU alert threshold monitoring is enabled for the current asset. For details, see Configuring Collection Monitoring.
Memory	Displays the memory usage of the current asset (unit: MB), including memory usage percentage, used memory, and total memory. Note This item is displayed only after memory alert threshold monitoring is enabled for the current asset. See Configuring Collection Monitoring for details.
Disk	Displays the disk usage of the current asset (unit: GB), including disk usage percentage, used disk space, and total disk space. Note This item is displayed only when disk alert threshold monitoring is enabled for the current asset. For details, see Configuring Collection Monitoring.
Asset Information	Displays basic information of the current asset. Click **Follow** to display this asset at the top of the **Key Assets** area in the collector-level log source monitoring.
Log Collection Trends	Displays the log collection trend for the current asset using an area chart. Click the legend to toggle the display of the following content: • **Ingestion Rate:** trend of log ingestion rate changes over the last 24 hours. • **Parsing Rate:** trend of log parsing rate changes over the last 24 hours. • **Total Logs:** trend of log count changes over the last 30 days. Hover over the chart to view specific statistical data.
Event Overview	Displays an overview of the 5 most recently generated events in list format, including event name, source/destination IP, generation time, and alert status.
Collection Overview	Displays the most recent collection time, alert time, and the latest 5 alert messages for the current asset. Click **View More** to go to the Message Center. For details, see Message Center.
Top 10 Associated Event Distribution in Last Week	Displays the top 10 event distribution and attack distribution chart associated with the log sources of the current asset for the past week.

6.2 Monitoring Collected Assets

LAS not only supports full lifecycle management of logs, but also provides real-time continuous monitoring and analysis of log source assets integrated through the Log Ingestion module, enabling timely detection of security events and abnormal assets in your network.

Choose **Log Source Management > Asset Monitoring**, which displays monitoring data for all collected assets by default. Click the collected asset type at the top of the page to display the corresponding asset access list, as shown in Figure 6-3, and the page display content description as shown in Table 6-3.

Figure 6-3 Collected Asset Monitoring

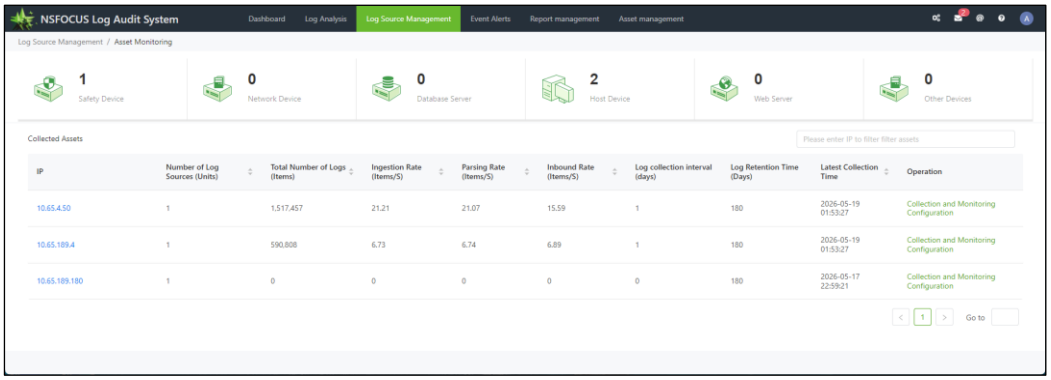


Table 6-3 Monitoring Asset

Display Item	Description
Asset Type	LAS supports monitoring and analysis of security devices, network devices, database servers, host devices, web servers, and other devices. The top of the page displays the numbers of collected assets. Click a number to view the asset information for the corresponding type in a list.
Collected Assets	Displays information including asset IP, number of log sources (units), total logs (entries), ingestion rate (entries/s), parsing rate (entries/s), storage rate (entries/s), log collection interval (days), log retention period (days), and last collection time. The following operations are allowed: • Click the sort icon next to the table header fields to sort by the corresponding field in ascending or descending order. • Supports filtering collected assets by asset IP address. • Hover over the log source count to display asset information and connected log source information. • Click the Asset IP address to view the asset-level log source information. For details, see Asset-Level Monitoring. • When an asset belongs to multiple collectors, click the asset IP address, select a collector to view the collector-level log source information. For subsequent operations, see Collector-Level Monitoring.

Display Item	Description
	• Click **Collection and Monitoring Configuration** in the list operation column to configure collection monitoring. See Configuring Collection Monitoring.

Configuring Collection Monitoring

In the **Asset Monitoring** page, click **Collection and Monitoring Configuration** in the **Operation** column, and configure the required parameters.

Table 6-4 Monitoring Configuration Parameters

Parameter		Description
Alert Level		Available options are **Low**, **Medium**, and **High**.
Resource Monitoring	CPU Alert Threshold/Duration	• **CPU Alert Threshold**: triggers an alert when CPU usage reaches the value. Drag the slider to configure the value. Value range: 10%~95%. • **Duration**: the duration of the CPU alert. Drag the slider to configure the value. Value range is 10~60 minutes.
	Memory Alert Threshold/Duration	• **Memory Alert Threshold**: triggers an alert when memory usage reaches the value. Drag the slider to configure the value. The value range is 10%~95%. • **Duration**: the duration of the memory alert. Drag the slider to configure the value. Value range is 10~60 minutes.
	Disk Alert Threshold	Triggers an alert when disk usage reaches the value. Drag the slider to configure the value. Value range is 10%~95%.
Collection Monitoring	Collection Idle Alert	When enabled, if no log data is received within the specified duration, LAS generates an alert (unit: minutes).
	Collection Surge Alert	When enabled, if the increase of collected log count within 5 minutes exceeds the value, LAS generates alerts (unit: entries).
	Collection Plunge Alert	When enabled, if the decrease of collected log count within 5 minutes exceeds the value, LAS generates alerts (unit: entries).
Collection Rate	Rate Limit	After enabling, configure the maximum asset ingestion rate (unit: entries per second). Note If the current asset has multiple log sources, the configured collection rate limit will be evenly distributed among all log sources that have collection rate limit enabled.

Note	The configuration parameters for collection monitoring vary slightly for different assets; please refer to the actual web interface for reference.

6.3 Log Source Topology

LAS allows configuring the topology diagrams of log sources. You can draw and manage topology diagrams based on the actual network distribution of log sources. After saving, the diagrams will be displayed in the dashboard.

Step 1 Choose **Log Source Management > Log Source Topology**.

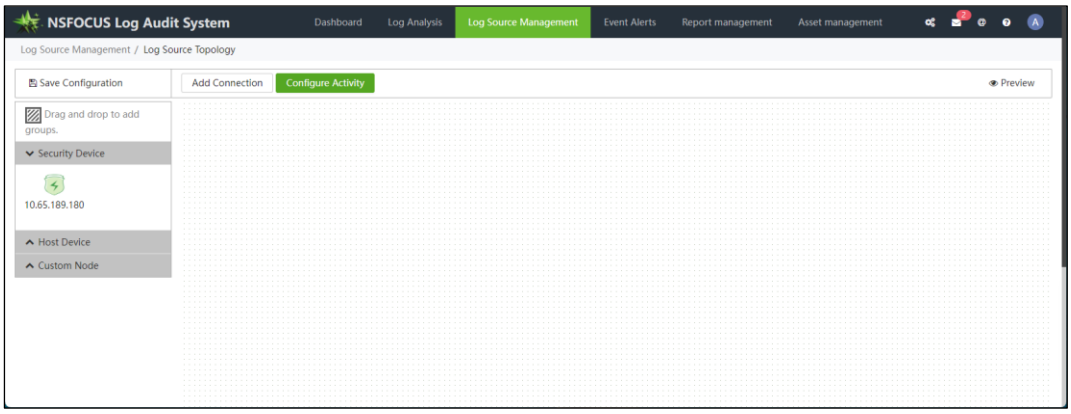
a. If the log source topology has not been configured, the page is empty. Click **Configure Topology** to proceed to step 2.

b. If a log source topology already exists, click the  icon to proceed to step 2.

Step 2 Navigate to the diagram page, as shown in Figure 6-4.

The left side of the page displays security devices, host devices, network devices, database servers, web servers, and custom nodes connected to LAS. The right side of the page is the drawing area for the topology diagram.

Figure 6-4 Log Source Topology - Diagram Creation Page



Step 3 Edit the topology diagram.

a. On the left side of the page, drag and drop icons to the drawing area. Right-click to perform the following operations on the group: rename, adjust text, adjust column count, adjust width, adjust height, and delete group.

b. Click on the left side of the page to expand the device list, then drag the device icon to the drawing area.

- Right-click the device to perform the following operations: adjust text, remove node.
- Right-click a custom node to perform the following operations: rename, adjust text, remove node.

c. Add connection lines between devices.

- Click **Add Connection**. The √ icon appears, which indicates the connection mode.
- Click device icons that needs to be connected.
- Hover over the other device icon and click to draw the connection line.
- Right-click the connection line to perform the following operations: connection line type, delete connection line.
- Click **Add Connection** again to exit the connection mode.

d. Click **Configure Activity** to configure the device activity threshold.

When the daily ingestion log count reaches the value, the device will be considered in active state.

e. Expand the device list on the left side of the page. Devices with the ✔ mark are already in the topology diagram.

Step 4 (Optional) Perform more operations in the topology diagram.

a. Click the  icon to center and display the topology diagram.

b. Click the  icons to zoom in/out the topology diagram.

Step 5 Click **Save** to save the current topology diagram.

a. Perform grouping adjustment and connection addition operations.

b. Set the homepage topology diagram. Available options include **System Built-in Topology** and **Custom Topology**.

c. Click **Confirm** to save the homepage topology diagram.

Step 6 (Optional) Click **Preview** to preview the current topology diagram online.

----End

7 Event Alerts

The main contents of this chapter are as follows:

Function	Description
Event Analysis	Introduces how to query events and view event details.
Event Rules	Introduces methods for managing event rules.
Alert Rules	Introduces methods for managing alert rules.

7.1 Event Analysis

Choose **Event Alerts** > **Event Analysis**. The top of the page displays event query conditions, the middle of the page displays event statistics charts, and the bottom displays the event list for the past week, as shown in Figure 7-1. The content description is shown in Table 7-1.

Figure 7-1 Event Analysis Page

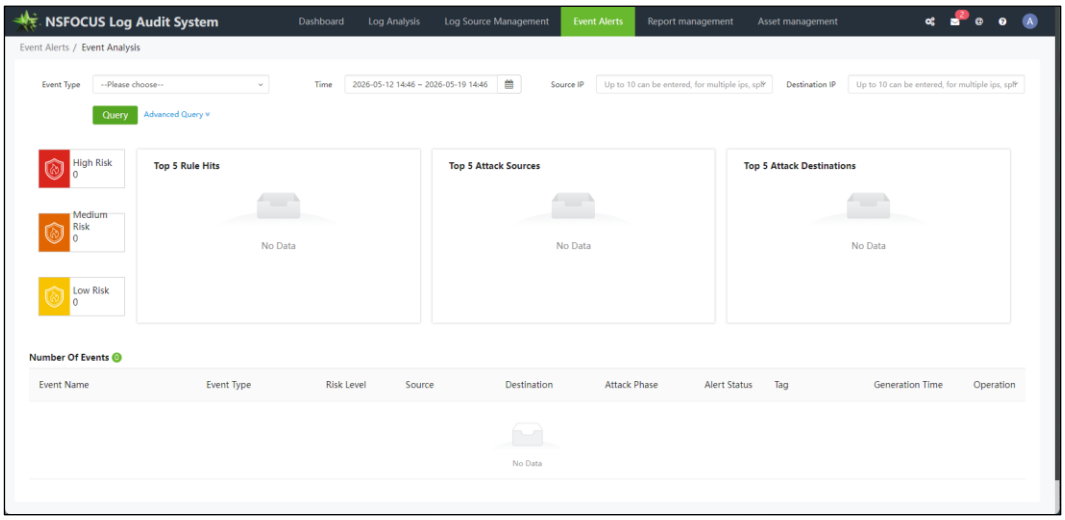


Table 7-1 Event Analysis Page Content

Display Item	Description
Event Query Conditions	Supports both simple query and advanced query modes. For details, see Querying Events.
Event Statistics Chart	Displays event statistical charts from different dimensions. For details, see Viewing Event Statistics.
Event List	Displays event information for the past week and supports the following operations: • View event details: see Viewing Event Details. • Add event tag: see Managing Event Tags.

7.1.1 Querying Events

In the **Event Analysis** page shown in Figure 7-1, simple query conditions are displayed by default. Click **Advanced Query** to perform more precise event queries. Query condition descriptions are shown in Table 7-2.

Table 7-2 Event Query Conditions

Querying Item		Description
Simple Query	Event Type	Event types and their subtypes.
	Time	The start and end time of the event.
	Source IP	The source IP where the event occurred. Both IPv4 and IPv6 are allowed. Up to 10 IPs can be selected. Separate multiple IPs with commas.
	Destination IP	The destination IP where the event occurred. Both IPv4 and IPv6 are allowed. Up to 10 IPs can be selected. Separate multiple IPs with commas.
Advanced Query	Event Name	The event name. Fuzzy query is allowed.
	Alert Status	The alert status of the event. Available options are: pending and alerted.
	Source IP Port	The source IP port number where the event occurred. Value range is 1~65535. Up to 10 ports can be selected. Separate multiple port numbers with commas.
	Destination IP Port	The destination IP port number of the event. Value range is 1~65535. Up to 10 ports can be selected. Separate multiple port numbers with commas.
	Is Invalid	Whether the event is invalid or not.
	Tag	Event tags. For details, see Managing Event Tags.
	Attack Phase	The attack phase of the attack event. Available options include **Reconnaissance**, **Weaponization**, **Delivery**, **Exploitation**, **Installation**, **Command and Control**, and **Malicious Activity**.
	Risk Level	The risk level of events. Available options are **Low**, **Medium**, and **High**. The matching methods include =, <, ≤, >, ≥.

7.1.2 Viewing Event Statistics

In the **Event Analysis** page shown in Figure 7-1, you can view event statistics from 4 dimensions described in Table 7-3. Clicking a statistics item in the chart allows you to filter corresponding events in the event list.

Click the legend to hide or show the statistics for the corresponding category in the chart. Hover over the chart to view specific statistical data.

Table 7-3 Event Statistics

Display Item	Description
High/Medium/Low Risk(s)	Displays the number of events with risks matching the risk levels.
Top 5 Rule Hits	Displays the top 5 events by matched rules in a ring chart, including event names and their event counts.
Top 5 Attack Sources	Displays the top 5 source IP addresses with the most attacks in a column chart, including the source IP addresses, risk levels, and event counts.
Top 5 Attack Destination S	Displays the top 5 destination IP addresses with the most attacks in a column chart, including destination IPs, risk levels, and event counts.

7.1.3 Viewing Event Details

In the **Event Analysis** page shown in Figure 7-1, the total number of events after query/filtering is displayed in the event list, with event name, event type, risk level, source IP, destination IP, attack phase, alert status, tag, and generation time.

Click the icon in the column to view the corresponding event details. The event details description is shown in Table 7-4.

Table 7-4 Event Details

Display Item	Description
Basic Information	Includes source IP, destination IP, generation time, risk level, attack phase, attack count, alert status, and event type. Click the icon next to the rule name to view matched event rules. For subsequent operations, see Event Rules.
Attacker Information	Includes source IP, country/region, and the owner.
Target Information	Includes the destination IP, country/region, and the owner.
Log List	Displays the log type, generation time, and log message of the triggered event. The following follow-up operations are supported: • View log details: click the icon before the log time/type to view the corresponding log details.

Display Item	Description
	• Configure log fields: click the icon to select fields. Up to 7 fields can be selected.

7.1.4 Managing Event Tags

Tagging is a classification method for events, enabling you to query and manage events in batches.

In the event list shown in Figure 7-1, click the icon in the **Operation** column, select an existing tag, or enter a tag name and click **Add Tag**.

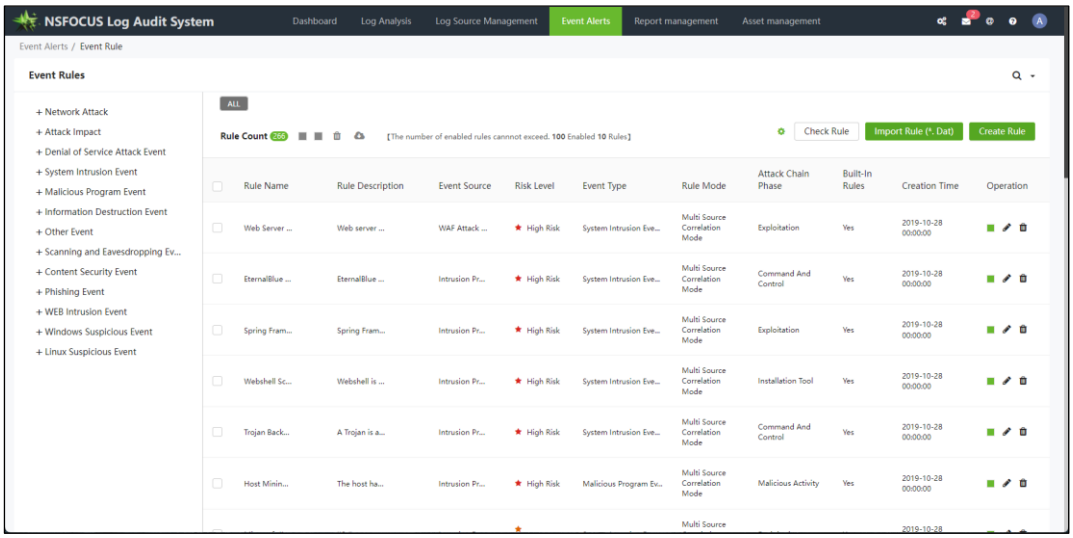
Tip	Added event tags are adaptively displayed in the **Event Details** page (displayed if events exist).

7.2 Event Rules

Upon receiving security logs, LAS checks whether the logs match event rules. If the logs meet the matching conditions specified in the event rules, events are generated.

Choose **Event Alerts > Event Rules**. The left side of the page displays event rule categories, and the right side displays built-in event rules for all categories by default, as shown in Figure 7-2.

Figure 7-2 Event Rules



7.2.1 Creating Event Rules

In addition to built-in event rules, LAS supports custom event rules. Newly created rules are enabled by default and take effect immediately.

The procedure for creating a custom event rule is as follows:

Step 1 In the **Event Rules** page, click **Create Rule**.

Step 2 Configure basic parameters for the event rule. Parameter descriptions are shown in Table 7-5.

Table 7-5 Event Rule Parameters

Parameter	Description
Rule Name	Enter the name of the event rule. Up to 100 characters are allowed. It cannot contain special characters or duplicate existing rule names.
Rule Mode	• **Single-source Filtering Mode:** in step 3, you can only select one event source and cannot configure a time window. • **Multi-source Correlation Mode:** in step 3, you can select multiple event sources. Within the time window, each log type must have been triggered at least once in any order. • **Multi-source Temporal Mode:** in step 3, you can select multiple event sources, where each log type is triggered sequentially at least once within the time window.
Attack Phase	Select the phase of the attack. Available options include **Reconnaissance**, **Weaponization**, **Delivery**, **Exploitation**, **Installation**, **Command and Control**, and **Malicious Activity**.
Event Type	Select the event type that this rule applies to.
Risk Level	Select the risk level for the rule. Available options are: **Low**, **Medium**, and **High**.
Attack Type	Select the attack type of the rule.
Attack Method	Select the attack method of the rule.
Rule Description	Enter the description of the rule. Up to 250 characters are allowed.

Step 3 Configure event rule parameters. Parameter descriptions are shown in Table 7-6.

Table 7-6 Event Rule Parameters

Parameter	Description
Event Source	Select the log types to apply this rule to, and set their respective filter conditions and association conditions. Select at least 2 event sources. They will be matched according to the order of selection.
Time Range	When the rule mode is **Multi-source Correlation Mode** or **Multi-source Temporal Mode**, fill in the time window for the rule (unit: seconds). When data meeting the conditions occurs within the specified time, an event will be generated.
Set as an Internal Event	When the rule mode is **Single-source Filtering Mode**, this rule serves as the event source for the next rule.

Step 4 Configure the parameters of event rule output result. For parameter descriptions, see Table 7-7.

a. Map the aggregated data to the attribute columns of the event list.

b. When mapped as "Focused content", it is recommended to select "Asset Matching" as aggregated form, and select "Source IP" or "Destination IP" as output fields.

c. Click **Add Output Attribute** to add attribute columns to the event list.

Table 7-7 Event Rule Output Result Parameters

Parameter	Description
Output Field	Raw data received by LAS.
Map To	The attribute column of the event list.
Aggregated Form	Data aggregation form.

Step 5 Click **Confirm**. After the custom event rule is added, the rule is enabled by default.

----End

7.2.2 Enabling/Disabling Event Rules

LAS with 32 GB of memory supports enabling up to 50 built-in event rules; with 64 GB of memory, it supports enabling up to 100 built-in event rules.

In the event rule list, the icon in the **Operation** column indicates that the corresponding rule is in enabled status, and the icon indicates that the corresponding rule is in disabled status. Only enabled rules take effect. The following two methods for modifying rule status are supported:

- Single operation

  In the event rule list, click the icon in the **Operation** column to enable/disable the corresponding rule.

- Batch operation

  In the event rule list, select multiple event rules, click the icon at the upper-left corner of the list to enable/disable the selected rules.

7.2.3 Querying Event Rules

In the **Event Rules** page shown in Figure 7-2, click the upper-right corner of the page to query event rules. Query conditions are described in Table 7-8.

Table 7-8 Event Rule Query Conditions

Querying Item	Description
Rule Name	Name of the event rule. Maximum of 100 characters. Fuzzy search is allowed.
Rule Description	Description of the event rule. Maximum of 250 characters. Fuzzy search is allowed.
Rule Mode	Mode of event rules. Available options include **Single-source Filtering Mode**,

Querying Item	Description
	Multi-source Correlation Mode, and **Multi-source Temporal Mode**.
Is Built-in	Whether the rule is built-in or not.
Attack Phase	The attack phase to which the rule belongs. Available options include **Reconnaissance**, **Weaponization**, **Delivery**, **Exploitation**, **Installation**, **Command and Control**, and **Malicious Activity**.
Attack Type	Attack type of the event rule.
Attack Method	Attack method of the event rule.
Is an Internal Event	Whether it is an internal event or not.
Risk Level	Risk level of the event rule.
Event Source	Log types to which event rules are applied.

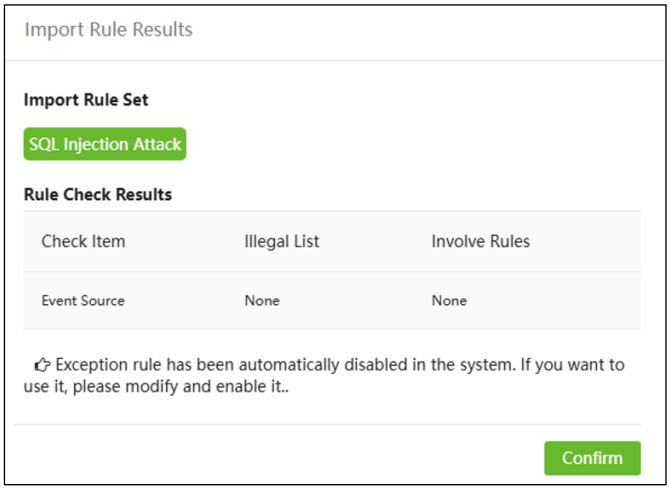
7.2.4 Exporting Rules

In the **Event Rules** page shown in Figure 7-2, select the event rules, then click the icon at the upper-left of the list to export the selected rules as a .dat file.

7.2.5 Importing Rules

In the **Event Rules** page shown in Figure 7-2, click **Import Rule (*.dat)**, select a rule file and upload it. After the import is complete, the import result is displayed as shown in Figure 7-3.

Figure 7-3 Importing Rule Results



Note

- If the imported rules conflict with existing rules, the existing rules will be automatically overwritten.
- If imported rules conflict with LAS event sources, LAS will automatically disable the conflicting rules after the import is complete.

7.2.6 Checking Rules

If no events are generated in LAS for an extended period, check whether the rules conflict with the event source.

In the **Event Rules** page shown in Figure 7-2, click **Check Rule** to display conflict items that conflict with the event source.

Note	Before performing rule checks, you must enable the anomaly rules. For details, see Enabling/Disabling Event Rules.

7.2.7 Editing Event Rules

In the event rule list shown in Figure 7-2, click the icon in the **Operation** column to modify rule parameters. For built-in rules, only some basic parameters and rule parameters can be modified.

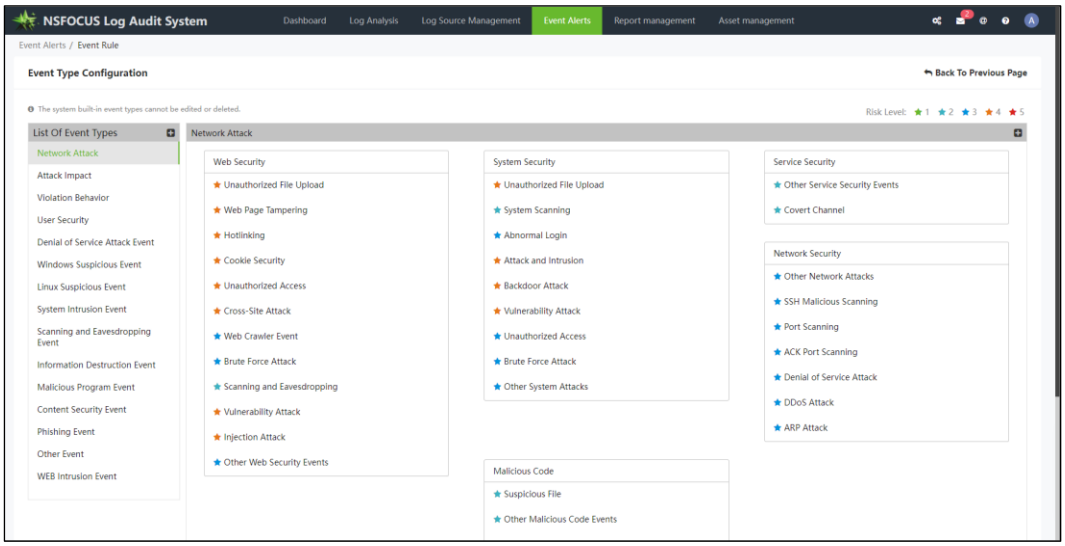
7.2.8 Deleting Event Rules

In the event rule list shown in Figure 7-2, click the icon in the **Operation** column, and after confirmation, delete the corresponding rule. Deleting rules supports batch operation.

7.2.9 Configuring Event Types

In the **Event Rules** page shown in Figure 7-2, click the icon to customize event types/sub-event types, as shown in Figure 7-4.

Figure 7-4 Configuring Event Type



Note	• System built-in event types cannot be edited or deleted. • Sub-event types support up to 2 levels.

Custom Event Type

In the page shown in Figure 7-4, click the icon in the event type list, enter the event type name (maximum 32 characters, and cannot contain special characters), click **Confirm**, and the new event type is added to the event type list.

Custom Sub-event Type

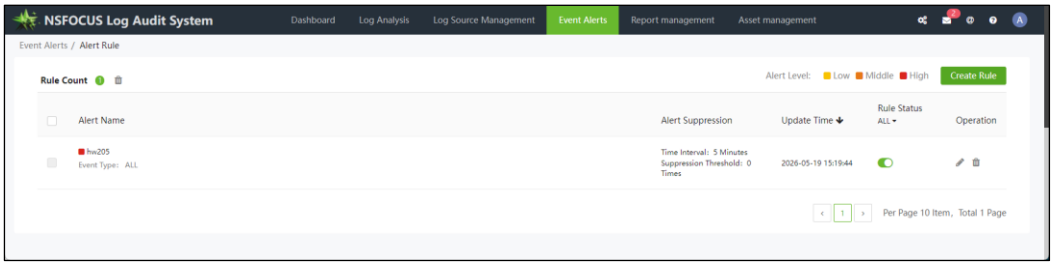
In the page shown in Figure 7-4, click an event type. The right side of the page displays the sub-event type list for that event type. Click the icon of the sub-event type list, enter the sub-event type name (maximum 32 characters, and cannot contain special characters), click **Confirm**, and the new sub-event type is added to the event type list.

7.3 Alert Rules

Alert rules are used to filter events that match the predefined criteria.

Choose **Event Alerts > Alert Rules**. As soon as an alert rule is enabled, the alert name, occurrence time, and occurrence count will be displayed scrolling at the top of the page, as shown in Figure 7-5.

Figure 7-5 Alert Rules



Click **Create Rule**, configure the alert rule parameters, and then click **Create** to save the configuration. The description of alert rule parameters is shown in Table 7-9.

After an alert rule is created, its status can be enabled or disabled. Only alert rules in disabled status can be edited or deleted.

If alert email notifications have been configured, LAS will send email notifications after an alert rule is enabled. For how to configure email notifications, see Configuring Mail Server.

Table 7-9 Alert Rule Parameters

Parameter		Description
Basic Settings	Alert Name	Name of the alert rule.
	Alert Level	Risk level of alerts triggered by the alert rule. Options include **High**, **Medium**, and **Low**.
	Description	Description of the alert rule.
Rule Settings	Event Type	Event types related to the alert rule. Select from the drop-down list, or click the icon to expand the event type list to select.
	Event Rules	Event rules related to the alert rule.
	Destination IP	Condition for matching the event's destination IP address. Select "=" or "!=" from the drop-down list, then enter the specific IP address in the text box on the right.
	Source IP	Condition for matching the event's source IP address. Select "=" or "!=" from the drop-down list, then enter the specific IP address in the text box on the right.
	Event Risk Level	Conditions for matching the event's risk level. Select "=", ">", ">=", "<", or "<=" from the drop-down list, then enter a level number ranging from 1 to 5 in the text box on the right.
Alert Method	Email Notification	Whether to send notification via email when an alert is triggered, The email server must be properly configured. For details, see Configuring Mail Server.
	SMS Notification	Whether to send notification via SMS when an alert is triggered. The SMS server must be properly configured. For SMS server configuration, see Configuring SMS Server.
	Scrolling Notification	Whether to display a scrolling notification in LAS when an alert is triggered.
	Sound Notification	Whether to notify with sound in LAS when an alert is triggered.
Alert Suppression	Time Interval	Set the time interval and suppression count for alert suppression. For identical alerts within the specified time interval (5~60 minutes), when the count exceeds the threshold (1~30 times), an alert will be triggered.
	Suppression Threshold	

8 Report Management

The main contents of this chapter are as follows:

Function	Description
My Reports	Describes how to view all reports successfully created in LAS.
Report Tasks	Describes how to create and manage report tasks.
Template Management	Describes how to create and manage report templates.

8.1 My Reports

Choose **Report Management > My Reports**. By default, it displays all reports that LAS has successfully created.

Viewing Reports

By default, the page displays all reports, including reports generated through immediate execution, scheduled execution, and periodic execution.

Click **Daily/Weekly/Monthly/Quarterly** at the top of the page to view the list of generated daily reports, weekly reports, monthly reports, or quarterly reports.

In the report list, click the  icon in the **File Format** column to preview reports in HTML/PDF/Word format online.

Downloading Reports

In the report list, select the reports you want to download, and click the  icon at the upper-left of the list to download the selected report files to your local machine.

Report Notification/Push

In the report list, click the  icon in the **Operation** column to configure notification parameters shown in Table 8-2.

Note	• Manual notification/report push are valid only for the current instance; it will not be saved. • Manual notification/report push is only for existing reports.

8.2 Report Tasks

Users can generate reports with specified content through report tasks as needed. After a report task is created, it may be in different statuses depending on its execution. The description of report task statuses is shown in Table 8-1.

Table 8-1 Report Task Status

Task Status	Description
	Scheduling
	Running
	Execution succeeded
	Execution failed
	Stopped

Creating Report Task

Choose **Report Management** > **Report Task**, click **Create Task**, configure the report task parameters, and then click **Create Task** to create a report task. The parameters for creating a new report task are described in Table 8-2.

Table 8-2 New Report Task Parameters

Parameter		Description
Task Scheduling	Execution Method	• **Immediate:** after creating the task, immediately execute the task to generate the report. • **Scheduled:** execute the report task at the specified time point and generate the report. • **Periodic:** periodically executes the report task based on the configured schedule. Available options include **Daily**, **Weekly**, **Monthly**, and **Quarterly**.
Report Settings (configuration for generating reports)	Start/End Time	Select which time frame's data to include in the report. Depending on the execution method of the task, the available start and end time options differ.
	Report Template	Content included in the generated report. Fuzzy search for report templates is allowed.
	Log Source IP	IP addresses or IP ranges of log sources. Both IPv4 and IPv6 are allowed. Separate multiple IPs with line breaks.

Parameter		Description
		After configuration, statistical reports are generated only for data with that IP or within that IP range.
Execution Settings	Task Name	Unique name of the report task, with a value range of 1 to 30 characters.
	Task Description	Description of the report task, with a value range of 1 to 250 characters.
	Report Format	Supports generating three types of reports: HTML, Word, and PDF. HTML type reports are generated by default. Users can select whether to also generate PDF and Word type reports. • : Generate reports in HTML format. • : Generate reports in PDF format. • : Generate reports in Word format.
Report Notification/Push	Email Notification	Whether to send reports via email. Before enabling it, you must configure the mail server. See Configuring Mail Server for details. • **Email Address**: enter the email address for receiving reports. • **Select Attachment**: select the report type for the email attachment. If not selected, notifications are sent without any attachments.
	SFTP Push	Whether to send reports to the SFTP server. Before enabling it, you must configure the SFTP server. For details, see Configuring SFTP Server. • **SFTP Address**: select the SFTP server that receives reports. • **File Format**: select the report type.

Managing Report Tasks

After a report task is created, choose **Report Management > Report Task** to manage report tasks in the list.

- View task: click the row of the report task to view the corresponding report task details.
- Delete task: report tasks with status "Scheduled" and "Running" as well as periodically executed report tasks cannot be deleted. Report tasks with other statuses can be deleted through the following two methods:
  - Single delete: click the icon in the **Operation** column to delete the corresponding report task.
  - Batch delete: select the report tasks to be deleted, click the icon at the upper-left of the list to delete the selected report tasks.
- Stop task: click the icon in the **Operation** column to stop report tasks with progress less than 100% or in scheduling status.
- Re-execute: click the icon in the **Operation** column to re-execute the corresponding completed or stopped report tasks.
- Report notification/push: click the icon in the **Operation** column to add notification/push content based on existing report tasks. Parameter descriptions are shown in Table 8-2. The notification/push is valid only for the current instance, meaning that the notification configuration will not be saved.

8.3 Template Management

LAS provides multiple built-in report templates by default. Editing, downloading, and deleting templates are not allowed.

You can copy templates or customize report templates as needed, facilitating direct reference when creating new report tasks.

8.3.1 Creating Report Template

The procedure for creating a new report template is as follows:

Step 1 Choose **Report Management > Template Management**.

Step 2 Click **New Template** to enter the **New Report Template** page.

Step 3 Click **Set Template Description**, and in the expanded text box, configure the description for the report template. A maximum of 250 characters are allowed.

Step 4 Configure the name of the report template.

Click the icon next to **New Report Template**, enter the name of the report template in the text box (maximum 30 characters and cannot be duplicate with existing report template names), then click the icon.

Step 5 (Optional) Add a report directory.

Configuring sub-headings with a maximum depth of 3 is allowed.

a. Click **Add Chapter** to add a new level-1 heading.

b. Hover over the level-1 heading and click the icon to add the corresponding level-2 heading.

c. Refer to the above operations, and continue to add corresponding level-3 headings or new directories.

Step 6 Configure report template content.

Hover over a heading in the table of contents area to display available operation icons, as shown in Table 8-3.

Table 8-3 Configuring Report Template Content

Icon	Description
	Configure the names for titles at each heading level.
	Configure the content to be displayed for each heading level.
	Select the corresponding area for each heading level to display the chart style. • Level-1 headings do not support configuring statistical items. • Click **To add new statistics items, go to statistics management** to configure new statistics items. For subsequent operations, see Statistics Management. Each report template supports a maximum of 100 statistics items.
	Delete unnecessary headings and the statistical items within them.
	Add a sub-heading.

Step 7 (Optional) Click the icon to preview the report.

Step 8 Save the report template.

a. Click **Save** to save the report template.

b. Click **Save and Create Task** to save the report template and use the report template to create a report task. For details, see Creating Report Task.

----End

8.3.2 Managing Report Templates

Choose **Report Management > Template Management** to manage report templates.

Viewing Report Templates

Click the icon in the **Operation** column to view the corresponding report template details.

Click the report template name to view the statistical items referenced by the report template.

Creating Report Tasks

Click the icon in the **Operation** column to use this report template to create report tasks. For details, see Creating Report Task.

Editing Report Templates

Click the icon in the **Operation** column, then click **Edit Template** to edit the corresponding report template.

Deleting Report Templates

The two methods for deleting report templates are as follows:

- Single delete: click the icon in the **Operation** column, then click **Delete Template** to delete the corresponding report template.
- Batch delete: select the report templates to be deleted, click the icon at the upper-left of the list, and the selected report templates will be deleted.

Copy Report Templates

Click the icon in the **Operation** column, then click **Copy Template** to generate a new report template with edits based on this template.

Downloading Report Templates

Downloading built-in report templates is not allowed. For custom report templates, you can:

- Single download: click the icon in the **Operation** column, then click **Download Template**.
- Batch download: select the report templates you want to download, click the icon at the top left of the list, then click **Batch Download**.
- Download all: click the icon at the upper-left of the list, then click **Download All**.

Importing Report Templates

Click **Import Template** to import the downloaded and modified report template back into LAS.

Viewing Execution Results

Click the icon in the **Execution Result** column to view the historical report files, where you can perform the following follow-up operations:

- View the execution time and results of report tasks using this template.
- Click the icon in the **Execution Result** column to preview report files in the corresponding format online.
- Select the report task, click the icon at the upper-left corner to download the selected report files to your local machine (including all generated formats).

9 Asset Management

LAS can manage up to 10,000 assets, including manually added log source assets, manually added assets, manually imported assets, and automatically discovered assets. If the number of assets to be added exceeds 10,000, the system will prompt that the limit has been exceeded.

The main contents of this chapter are as follows:

Function	Description
Concepts and Relationships	Introduces asset-related concepts and the relationships between these concepts.
Asset Overview	Introduces methods for creating assets and attribute groups, and asset management.
Asset Discovery	Introduces how to configure log analysis and asset onboarding.

9.1 Concepts and Relationships

The main concepts related to assets and the relationships between them are shown in Table 9-1. Assets, attributes, and tags have n-to-n relationships.

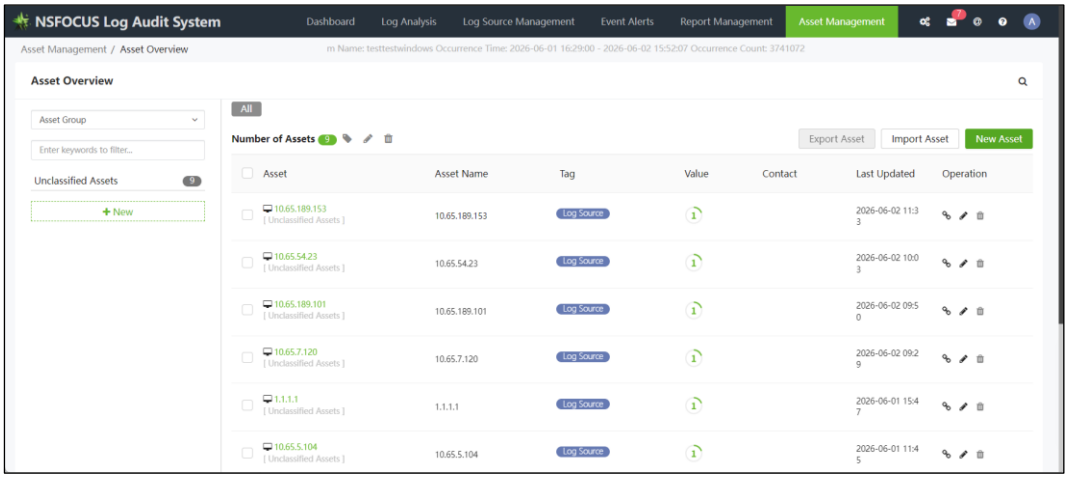
Table 9-1 Association Relationship

Noun	Description
Assets	Managed and valuable entities within the user network environment. Currently, LAS only supports importing, discovering, and managing host assets, which refers to a physical machine or virtual machine in the network, identified by an IP address.
Attribute	Attributes are a method of classifying assets. LAS provides built-in attributes and custom attributes. You can create new attribute groups under attributes to further classify assets.
Tag	Tags are a method for classifying assets; each tag is a subcategory. The same tag can be associated with one or more assets across different asset groups, enabling asset management from another dimension.

9.2 Asset Overview

Choose the **Asset Management** > **Asset Overview**. The left side of the page allows you to switch between different attributes and attribute groups, while the right side displays the asset list in list view. Device IP addresses collected will be automatically added to the asset list and assigned with a "Log Source" tag, as shown in Figure 9-1.

Figure 9-1 Asset Overview



9.2.1 Creating Attribute Groups

The following steps use asset group as an example to describe the steps to create an attribute group.

Step 1 Choose **Asset Management** > **Asset Overview**, and select **Asset Group** from the drop-down list on the left side.

Step 2 Click **New** on the left side of the page to open the **New Attribute** dialog box.

Step 3 Configure attribute group parameters. Parameter descriptions are shown in Table 9-2.

Table 9-2 Attribute Group Parameters - Asset Group

Parameter	Description
Name	Name of the attribute group, supporting up to 30 characters.
Contact	Contact for assets in the attribute group, supporting up to 30 characters. Special characters are not allowed.
Email	Email address of the asset contact. Only one email address is allowed, supporting a maximum of 64 characters.
Mobile Number	Mobile phone number of the asset contact. Only one mobile phone number is allowed.
Geographic View	Geographic location of assets in the attribute group.
Latitude and Longitude	Longitude and latitude of the asset in the attribute group.
Value	The larger the value, the higher the asset value in the attribute group, and the greater

Parameter	Description
	the impact on the risk.
Description	Description for the attribute group, supporting up to 255 characters. Special characters are not allowed.
IP Range	IP range of assets in the attribute group.
Collector	Collectors for asset discovery reported by assets in the attribute group. Multiple selection is allowed. For how to configure the collector, see Collection Terminal.

Step 4 Click **Create** to save the attribute group.

----End

9.2.2 Creating Assets

The steps to create a new asset are as follows:

Step 1 Choose **Asset Management > Asset Overview**, click **New Asset** on the right side of the page.

Step 2 Configure the basic information for the asset. For parameter descriptions, see Table 9-3.

Table 9-3 Asset Basic Information

Parameter	Description
IP Address	• By default, enter the IP address of a single asset. Both IPv4 and IPv6 are supported. • Click **Batch Add Assets** to switch to batch add asset. Enter the IP range for assets. Both IPv4 and IPv6 are supported.
Asset Name	Enter the asset name.
Tag	Select tags associated with the asset, or click **Add Tag** to create and associate a new tag with the asset.
Asset Group/Business System/Organizational Structure/Geographic Location	The asset group/business system/organizational structure/geographic location to which the asset belongs. For the tree type, you can select via the drop-down list or by clicking the icon.
Custom Asset Attribute	Custom asset attributes associated with the asset. For how to configure custom attributes, see Adding Attributes. For the tree type, you can select via the drop-down list or by clicking the icon.
Latitude and Longitude	Enter the longitude and latitude of the asset location.
Contact	Enter the contact person for the asset. Up to 30 characters are allowed.
Email	Enter the asset contact's email address. Only one email address is allowed, supporting up to 64 characters.
Mobile Number	Enter the mobile phone number of the asset contact. Only one mobile phone number is allowed.

Parameter	Description
Confidentiality	The larger the value, the higher the asset confidentiality, and the greater the impact on the risk.
Integrity	The larger the value, the higher the asset integrity, and the greater the impact on the risk.
Availability	The larger the value, the higher the asset availability, and the greater the impact on the risk.
Value	The larger the value, the higher the asset value, and the greater the impact on the risk. Click **Auto Calculate**, and then LAS will automatically calculate the numerical value based on the configured confidentiality, integrity, and availability.
MLPS Level	Select the classified protection level for the asset.
Description	Enter the asset description. Up to 255 characters are allowed.

Step 3 (Optional) Select the **Host Information** tab and configure the host information for the asset. The parameters are as shown in Table 9-4.

Table 9-4 Asset Host Information

Parameter		Description
System Information	Operating System Type	The operating system type of the asset. Fuzzy search is allowed.
	Operating System Version	The operating system version of the asset. Fuzzy search is allowed.
Device Information	Device Type	The device type to which the asset belongs. Up to 255 characters are allowed.
	Device Manufacturer	The manufacturer to which the asset belongs. Up to 255 characters are allowed.
	Device Model	The model of the asset. Up to 255 characters are allowed.
Login Information	Login IP Address/Port	The login IP address/port of the asset.
	Login Protocol	The login protocol of the asset.
	Login Account/Password	The login account/password of the asset.
Domain Information		Click **Add Domain** and enter the asset's domain name.

Step 4 (Optional) Select the **Service Information** tab, click **Add Service**, and configure the asset's service information. Parameter descriptions are shown in Table 9-5.

Table 9-5 Asset Service Information

Parameter	Description
Port Number	Enter the port number of the asset service. Valid range is 1~65535.

Parameter	Description
Service Name	Composed of letters (case-sensitive), numbers, or hyphens. Up to 128 characters are allowed.
Protocol	The protocol type running on the port. Available options are **TCP** and **UDP**.
Banner	Enter the version information of the service. Up to 255 characters are allowed.
Remark	Enter remarks for the service. Up to 255 characters are allowed.

Step 5 (Optional) Select the **Application Information** tab, click **Add Application**, and configure the asset application information. For parameter descriptions, see Table 9-6.

Table 9-6 Asset Application Information

Parameter	Description
Name	Select the application name within the asset. Fuzzy query is allowed.
Vendor	Enter the vendor to which the application belongs.
Version	Select the version number of the application. Fuzzy query is allowed.
Remark	Enter remarks for the application. Up to 255 characters are allowed.

Step 6 Click **Confirm** to save the configuration.

----End

9.2.3 Viewing Asset Details

In the page shown in Figure 9-1, select an asset attribute on the left side of the page, and the right side displays the asset list within the attribute. In the asset list, click an asset IP to view the asset's basic information, host information, service information, application information, firewall information, and account information. Click **Edit** to edit the asset details in the corresponding page.

9.2.4 Editing Assets

You can edit asset information through the following two methods:

- Single edit

  On the **Asset Details** page, click **Edit**.

  In the asset list, click the icon in the **Operation** column.

- Batch edit

  Select multiple assets from the asset list, and click the icon at the upper-left of the list.

Note	• Batch edit assets only supports editing basic information of assets. It does not support editing host information, service information, or application information. • For how to edit asset information, see Creating Asset.

9.2.5 Deleting Assets

Deleted assets will no longer be managed by LAS. You can delete assets through the following two methods:

- Single delete

  In the asset list, click the icon in the **Operation** column.
- Batch delete

  Select multiple assets in the asset list, click the icon at the upper-left of the list.

9.2.6 Associating Assets

Asset association includes viewing logs, associating logs, and associating events. Viewing logs, associating logs, and associating events are supported only after manually added or imported host assets have downloaded and installed the agent (see Agent). Host assets with the agent successfully installed are displayed as connected assets in the Agent page and counted as host devices.

Choose **Asset Management > Asset Overview** and perform the following operations.

Viewing Logs

By viewing logs, you can view log information originating from the corresponding assets.

Click the icon in the **Operation** column of the asset list, select **View Log** to view log information of this asset. For details, see Log .

Associating Assets with Logs

By associating assets with logs, you can view log information related to a specific asset.

Click the icon in the **Operation** column of the asset list, select **Associate Log** to view logs with the source IP or destination IP matching this asset. For details, see Log .

Associating Assets with Events

By associating assets with events, you can view event information by asset.

Click the icon in the **Operation** column of the asset list, select **Associate Event** to view event information related to this asset. For details, see Event Analysis.

9.2.7 Tagging Assets

By tagging assets across different asset groups, you can manage assets from an additional perspective.

There are two methods for manually tagging assets:

- When creating a new asset. For details, see Creating Asset.

- Choose **Asset Management > Asset Overview**, select multiple assets in the asset list, and click the icon at the upper-left of the list to batch add tags to the selected assets.

9.2.8 Exporting Assets

Choose **Asset Management > Asset Overview**, select the assets to be exported in the asset list, and click **Export Asset**.

9.2.9 Importing Assets

Note	LAS can batch import up to 10,000 assets. The rules for importing assets are as follows: • If an asset with the same IP already exists in the asset list, it will be automatically skipped; existing asset information and attributes remain unaffected. • If the asset/attribute does not exist, it will be automatically created after import. • Assets not present in the asset file but already existing in the asset list will not be deleted.

In addition to manually adding assets, LAS also supports batch importing asset information. Perform the following steps to import asset information:

Step 1 Choose **Asset Management > Asset Overview**, and click **Import Asset**.

Step 2 Click **Download Import Template**.

Step 3 Open the downloaded template on your local disk, enter asset information following the template prompts, and save it as an XLSX file.

Use Office 2019, Office 365, or WPS 2016 or later to edit the template file.

Step 4 Return to the **Asset Import** page, click **Select File** or drag the file to the designated area, and wait for the import to complete.

----End

9.3 Asset Discovery

LAS can perform automatic asset discovery by analyzing reported log information, eliminating the need for manual asset storage, and greatly reducing user workload.

The rules for asset discovery are as follows:

- If the asset is not found in either the formal assets or pending list, perform a discovery on the asset.
- If the asset does not exist in formal assets but exists in pending list, update the discovery time of that asset in the pending list.
- If the asset exists in formal assets but not in pending list, discard this discovery log entry.

When LAS discovers an asset, the asset information is stored in the pending list and categorized based on their attributes. Only after it becomes a formal asset, you can manage it in LAS.

9.3.1 Discovering Assets

Choose **Asset Management** > **Asset Discovery** and click **Configure Log Analysis**. LAS will discover qualified assets from received logs only when both the conditions of "IP range to be discovered" and "log types to be discovered" are met. The condition parameters are described in Table 9-7.

Table 9-7 Log Analysis Parameters

Parameter	Description
IP Ranges	Select the target IP range for asset discovery. Multiple selection is allowed.
Log Types	Select the log types for asset discovery. Multiple selection is allowed.
Whether to Enable	Whether to enable the function of asset discovery via log analysis.

9.3.2 Onboarding Assets

Asset onboarding refers to move assets from the pending list to the asset list in the **Asset Overview** page.

Choose **Asset Management > Asset Discovery**, select the assets and click the icon at the upper-left corner of the list.

Note	Batch onboarding assets across pages is allowed.

Asset onboarding principles are as follows:

- During asset onboarding LAS evaluates the binding relationship between the current asset attributes and the collector. If the collector reporting the asset matches the collector bound to the asset attribute, assign the asset to that asset attribute.
- If it matches the "asset scope" of a sub-asset attribute, assign it to the sub-asset attribute; otherwise, assign it to the parent asset attribute.
- Assets that cannot be matched to specific asset attributes are assigned to "unclassified assets".

10 System Management

Click the  icon on the quick access toolbar to enter the system management page, where you can perform configuration and management operations for security devices, collectors, LAS, etc.

This chapter contains the following sections:

Function	Description
Data Collection	Describes how to integrate and manage log information from various sources, including NSFOCUS security devices, third-party security devices, network devices, databases, Windows hosts, Linux hosts, web servers, and others.
Data Management	Describes how to configure backup restore, threshold management, Syslog forwarding, storage expansion, data migration, archive restore and high availability.
System Components	Describes how to configure system services and port rules.
Cluster Management	Describes how to manage clusters.
System Configuration	Describes how to configure network parameters, event notification parameters, system monitoring parameters, time synchronization parameters, and report template parameters.
Troubleshooting	Describes how to troubleshoot through network diagnosis, packet capture, remote assistance, and inspection.
License Management	Describes how to view certificate status and upload certificates.
Upgrade	Describes how to upgrade LAS manually or online, as well as how to manually upgrade the knowledge base.

10.1 Data Collection

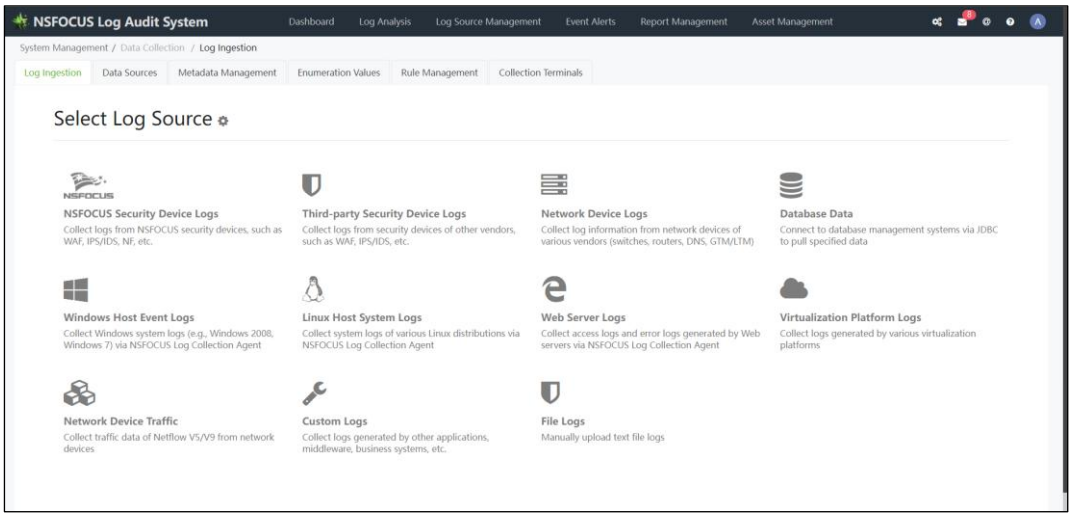
Data collection includes log ingestion, data sources, metadata management, collection terminals, rule management, and enumeration values. You can configure it to ingest logs and data information into LAS from various log sources, including NSFOCUS security devices and third-party security devices.

10.1.1 Log Ingestion

Log ingestion refers to collecting various logs classified by their sources.

Hover over the icon and choose **Data Collection > Log Ingestion**, as shown in Figure 10-1.

Figure 10-1 Log Ingestion



10.1.1.1 Log Types

Different log types differ in their built-in log parsing rules and coarse-grained extraction. For details, see Table 10-1.

- Built-in parsing rules: log types with built-in parsing rules do not require Configuring Field Extraction Rules to extract logs.
- One-click coarse-grained extraction: for log types without built-in parsing rules or using derived parsing rules, you can use the coarse-grained extraction to quickly parse and extract logs.

Table 10-1 Log Type Description

Log Type	Whether Built-in Parsing Rules are Included	Whether Coarse-grained Extraction is Supported
NSFOCUS Security Device Logs	√	×
Third-Party Security Device Logs	√ Note Partially available. Please refer to the actual product.	√ Note Only third-party security device logs without built-in parsing rules or using derived parsing rules support this function.

Log Type	Whether Built-in Parsing Rules are Included	Whether Coarse-grained Extraction is Supported
Network Device Logs	√ Note Partially available. Please refer to the actual product.	√ Note Only network device logs without built-in parsing rules or using derived parsing rules support this function.
Database Data	√ Note Partially available. Please refer to the actual product.	×
Windows Host Event Log	√	×
Linux Host System Logs	√	×
Web Server Logs	√	×
Virtualization Platform Logs	√ Note Partially available. Please refer to the actual product.	√ Note Only virtualization platform logs without built-in parsing rules or using derived parsing rules support this function.
Network Device Traffic	√	×
Custom Logs	√ Note Partially available. Please refer to the actual product.	√ Note Only custom logs without built-in parsing rules or using derived parsing rules support this function.
File Logs	√ Note Partially available. Please refer to the actual product.	×

Note	• For log categories that require field extraction rules, if you do not configure field extraction rules, LAS places the raw log text into unrecognized logs. • For database logs, if the data extraction rule is configured incorrectly, the log source file will be placed in unrecognized logs; otherwise, all will be placed in database logs.

10.1.1.2 Configuring Access

Access configuration includes auto-access configuration and FTP allowlist configuration.

Configuring Auto-access

Hover over the icon, choose **Data Collection** > **Log Ingestion**, click the icon to set the IP range for blocked access. Logs from log sources within the specified IP range will not be automatically accessed by LAS.

Configuring FTP Allowlist

When using an FTP server to store uploaded log files, configure an FTP allowlist and set the IP addresses allowed to access the FTP server to prevent unauthorized access and data leakage.

Hover over the icon, choose **Data Collection > Log Ingestion**, click the icon to configure the FTP allowlist list and enter IP addresses allowed to access the FTP service.

Note	This allowlist only applies to port 50071 of the FTP service.

10.1.1.3 Configuring Log Collection

Different types of log data sources have different configurations for connecting to LAS collectors.

Collecting NSFOCUS Security Device Logs

The steps for collecting NSFOCUS security device logs are as follows:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

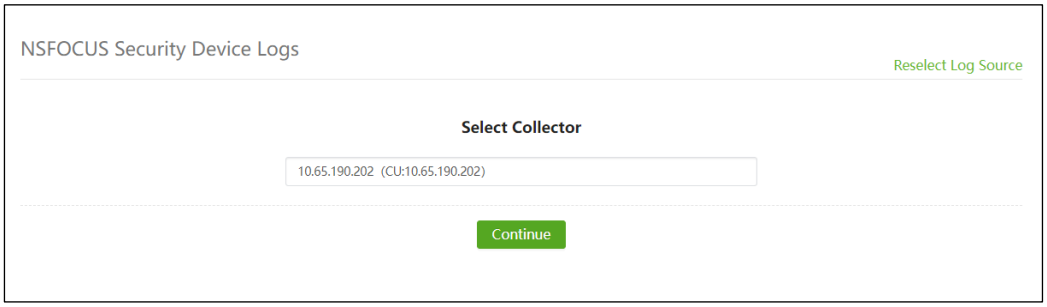
Step 2 Hover over **NSFOCUS Security Device Logs**, and a switch for auto-access appears at the upper-right corner.

a. After the switch is turned on, whenever an NSFOCUS security device connects, LAS can automatically configure the corresponding log source device for that NSFOCUS security device, eliminating the need to manually configure it following the steps below.

b. After the switch is turned off, follow the steps below to configure.

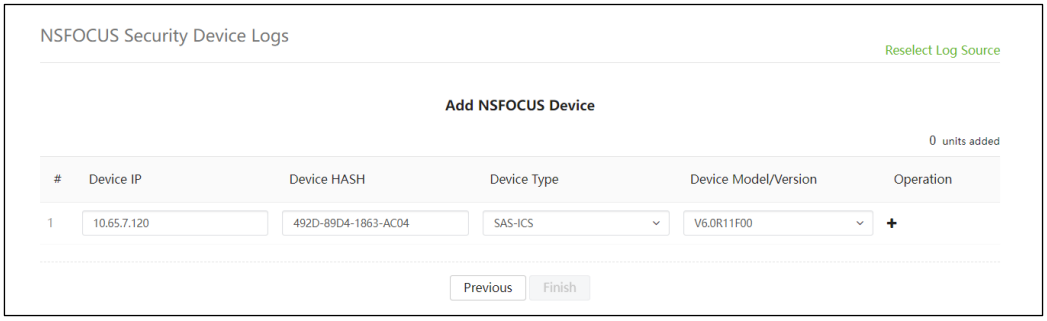
Step 3 Click **NSFOCUS Security Device Logs** to enter the page as shown in Figure 10-2.

Figure 10-2 NSFOCUS Security Device Logs



Step 4 Select a collector, click **Continue** to enter the page as shown in Figure 10-3.

Figure 10-3 Adding NSFOCUS Devices for Log Integration



Step 5 Configure the device IP, device HASH, device type, and device model/version of the NSFOCUS security device, click the + icon in the **Operation** column.

Step 6 Click **Finish**.

----End

Collecting Third-Party Security Device Logs

The steps for collecting third-party security device logs are as follows:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 Hover over **Third-Party Security Device Logs**. A switch for auto-access appears at the upper-right corner. LAS disables the auto-access function for third-party security devices by default.

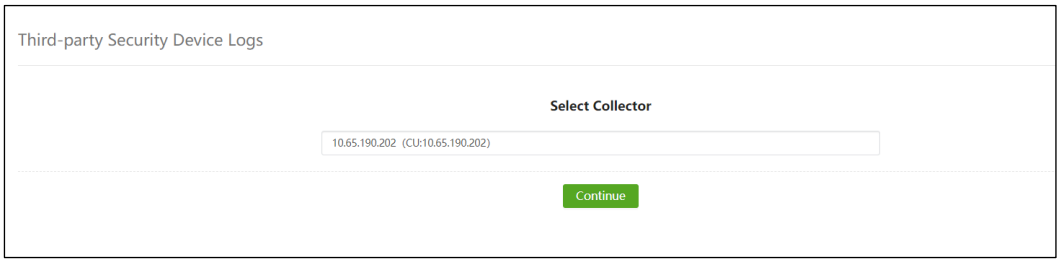
a. After the switch is turned on, configure the port numbers for auto-access (up to 3 ports supported) and enable the ports. Whenever log data is sent from third-party security device through the configured port, LAS automatically matches the newly ingested logs with the system built-in parsing rules, and associates the rule with the ingested logs of the highest match rate. When the port switch is disabled, the auto-access function for the corresponding port does not take effect.

b. After the switch is turned off, follow the steps below to configure.

Tip	If the IP address of a third-party security device is within the blocked IP range, automatic log ingestion will not be performed.

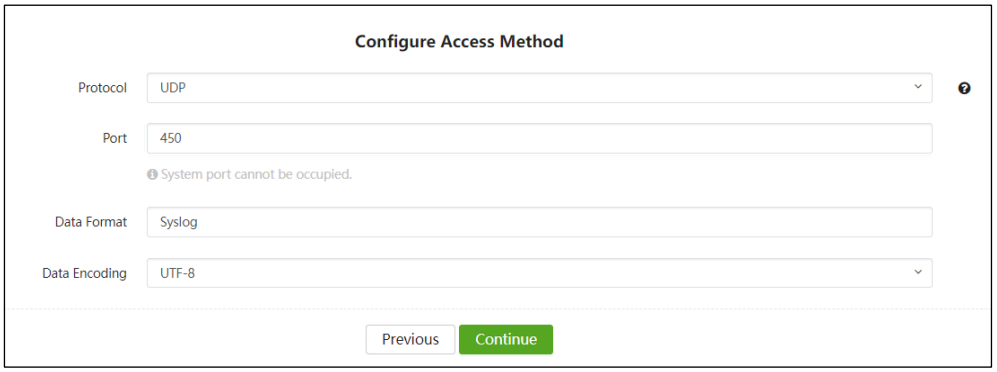
Step 3 Click **Third-Party Security Device Logs** to enter the page shown in Figure 10-4.

Figure 10-4 Selecting Collector for Third-Party Security Device Logs



Step 4 Select the collector, click **Continue**, and enter the page shown in Figure 10-5.

Figure 10-5 Configuring Access Method



Step 5 Configure the access method for third-party security devices. See Table 10-2 for parameter descriptions.

Table 10-2 Third-Party Security Device Integration Parameters

Parameter	Description
Protocol	Options include **UDP**, **FTP**, and **SNMP**.
Port	One port can only receive data of a single format via a single protocol. The system port must not be occupied. For FTP connections, only port 50071 is supported and cannot be modified.

Parameter	Description
Data Format	Supported data formats vary depending on the selected access protocol. • UDP: only supports Syslog format. • FTP: supports JSON, XML, and TEXT formats. • SNMP: only supports TEXT format.
Data Encoding	Encoding formats for ingested log data. Available options are **UTF-8**, **GBK**, and **US-ASCII**.

Step 6 Click **Continue** to enter the page as shown in Figure 10-6.

Figure 10-6 Adding Third-Party Security Devices for Log Ingestion

Step 7 Configure the device IP, vendor, type, and model/version for the third-party security device. Click the ✚ icon in the **Operation** column.

Step 8 (Optional) Repeat step 8 to continue adding third-party security devices.

a. If you need to add multiple third-party security devices, click **Batch Add**.

b. Configure the parameters shown in Table 10-3.

Table 10-3 Batch Add Third-Party Security Devices

Parameter	Description
Device IP	Enter the IP address or IP range of third-party devices.
Vendor	Select the manufacturer of third-party security devices.
Type	Select the type of third-party security devices.
Model/Version	Select the model/version of third-party security devices.

Step 9 Click **Finish** if the collected data does not require field extraction and can be directly stored in the database.

To extract log fields before ingesting log data. Click **Continue Rule**. For details, see Configuring Field Extraction Rules.

----End

Note	If using FTP to connect to third-party security devices, you need to log in to the FTP server using the generated account/password, and upload the log files to the root directory. Click **View FTP Details** to view the FTP server-related parameters.

Collecting Network Device Logs

The procedure for collecting network device logs is similar to that for Collecting Third-Party Security Device Logs.

Collecting Database Data

To collect database data, follow these steps:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 Select **Database Data**.

Step 3 Select the collector, click **Continue**.

Step 4 Configure database information.

a. Configure the database IP, database type, database version, and database port.

b. If the database already exists in LAS, you can click **Select from Existing Databases** to select an existing database as needed, and click the icon in the **Operation** column.

Step 5 Click **Continue** to configure database access parameters.

a. Select a database name from a drop-down list or click the icon to add a new one.

b. Enter the database login account/password.

c. Click **Add Data Table** to configure data tables for the database.

d. Select the data table type, and configure the data table and data table alias.

Step 6 (Optional) Configure data extraction rules.

a. Click **Finish** to save the integration without configuring field extraction fields.

b. Click **Configure Rule**. In the pop-up dialog, click the icon in the **Operation** column to extract log fields before ingesting database data. For extraction details, see Configuring Field Extraction Rules.

----End

Collecting Windows Host Event Logs

LAS can collect Windows host event logs via the NSFOCUS log collection agent. For supported Windows versions, see Operating Systems Supported by Agent.

The steps for collecting Windows host event logs are as follows:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 Hover over **Windows Host Event Logs**, and both the agent and a switch for auto-access appears at the upper-right corner. LAS enables the log auto-access function for Windows host by default.

a. If the switch is turned on, whenever Windows host event logs are ingested, LAS can automatically configure the log source device corresponding to those Windows host event logs, without the need to manually configure it as the steps below.

b. If the switch is turned off, follow the steps below to configure.

Step 3 (Optional) Download and install an agent. See Installing on Windows.

If the agent has already been installed on your Windows host, you can skip this step.

Step 4 Click **Windows Host Event Logs**.

Step 5 Select the collector, and click **Continue**.

Step 6 Configure the access method. For parameter descriptions, see Table 10-4.

Table 10-4 Windows Host Access Method

Parameter	Description
Access Method	Options include **Agent** and **WMI**.
Protocol	When the access method is **Agent**, this parameter is required. Currently, only **UDP** is supported.
Port	When the access method is **Agent**, this parameter is required. Each port can only ingest data of one format using one protocol.
Data Format	When the access method is **Agent**, this parameter is required. UDP only supports the Syslog format.
Data Encoding	When the access method is **Agent**, this parameter is required. Available options are **UTF-8**, **GBK**, and **US-ASCII**.

Step 7 Click **Continue** to enter the page for agent/WMI log collection, as shown in Figure 10-7 or Figure 10-8.

Figure 10-7 Add Windows Hosts for Log Collection (Agent)

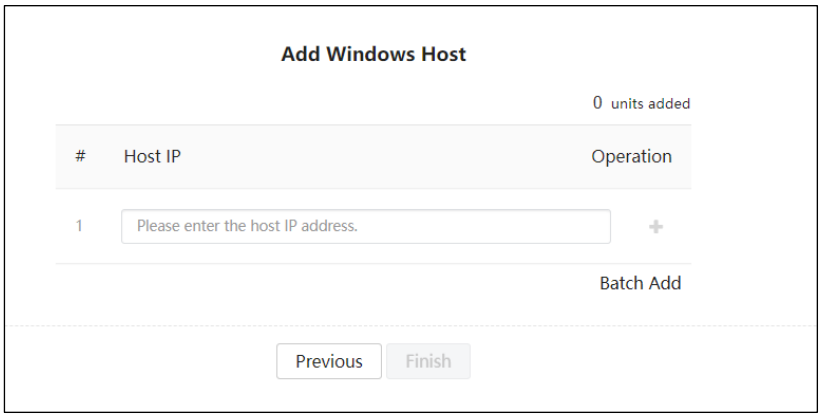
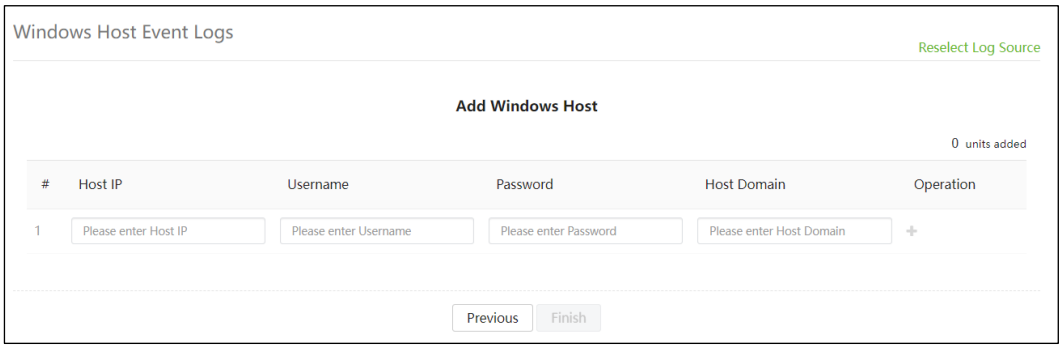


Figure 10-8 Add Windows Hosts for Log Collection (WMI)



Step 8 Configure the Windows host.

a. Agent integration method

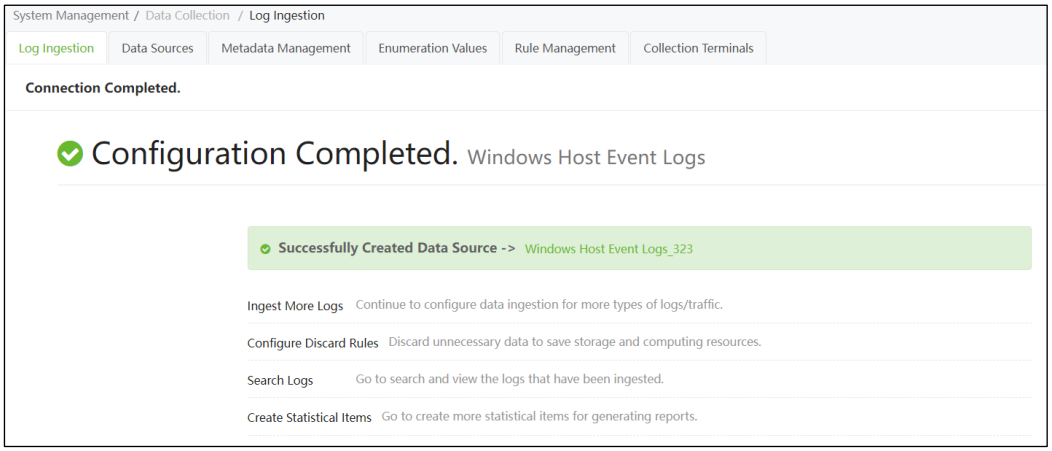
- Single add (default): fill in a single host IP address and click the + icon.
- Batch add: click **Batch Add**, and enter the host's IP address or IP range.

b. WMI access method

Configure the host IP address, username, password, and host domain, and then click the + icon.

Step 9 Click **Finish** to save the configuration, as shown in Figure 10-9.

Figure 10-9 Configuration Completed (Windows Host Event Log)



----End

Collecting Linux Host System Logs

LAS can collect Linux host system logs via the NSFOCUS log collection agent. For supported Linux versions, see Operating Systems Supported by Agent.

The steps for collecting Linux host system logs are as follows:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 Hover over **Linux Host System Logs**, and both the agent and a switch for auto-access appear at the upper-right corner. LAS enables the auto-access function for Linux hosts by default.

a. After the switch is turned on, whenever Linux host system logs are ingested, LAS can automatically configure the log source device corresponding to those Linux host system logs, eliminating the need to manually configure the steps below.

b. After the switch is turned off, follow the steps below to configure.

Step 3 (Optional) Download and install an agent. See Installing on Linux.

If the agent has already been installed on your Linux host, you can skip this step.

Step 4 Click **Linux Host System Logs**.

Step 5 Select the collector, and click **Continue**.

Step 6 Configure the access method for Linux hosts. For parameter descriptions, see Table 10-5.

Table 10-5 Linux Host Access Parameters

Parameter	Description
Access Method	Available options are **Agent** and **Rsyslog**.
Protocol	Currently, only **UDP** is supported.
Port	One port can only accept data in one format using one protocol.
Data Format	UDP only supports collecting data in Syslog format.
Data Encoding	Encoding formats for ingested data. Available options are **UTF-8**, **GBK**, and **US-ASCII**.

Step 7 Click **Continue** to configure the Linux host.

a. Agent method

- Single add (default): configure a host IP address and click the + icon.
- Batch add: click **Batch Add**, enter the host's IP address or IP range, and click **OK**.

b. Rsyslog method

- Single add (default): configure host IP, operating system, and version, and click the + icon.
- Batch add: click **Batch Add**, enter the operating system, version, and device IP address, and click **OK**.

Step 8 Click **Finish**.

----End

Collecting Web Server Logs

The steps for collecting web server logs are as follows:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 (Optional) Hover over **Web Server Logs**, click **Agent** to download and install agents. For details, see Installing Agent.

If agent has already been installed on your web server, skip this step.

Step 3 Click **Web Server Logs**.

Step 4 Select the collector, and click **Continue**.

Step 5 Configure the web server access method. For parameter descriptions, see Table 10-6.

Table 10-6 Web Server Access Parameters

Parameter	Description
Protocol	Currently, only **UDP** protocol is supported.
Port	One port can only accept data in one format using one protocol.
Data Format	UDP only supports log ingestion in Syslog format.
Data Encoding	Encoding formats for log ingestion. Available options are **UTF-8**, **GBK**, and **US-ASCII**.

Step 6 Click **Continue** to add the configurations of web servers.

a. Click **Add Web Server** to configure the server IP, server type, and log format for the web server, click **Confirm**.

b. Among them, the log format must be consistent with that configured in the web server.

Step 7 Click **Finish**.

----End

Collecting Virtualization Platform Logs

The procedure for collecting virtualization platform logs is as follows:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 (Optional) Hover over **Virtualization Platform Logs**, click **Agent** to download and install an agent. For details, see Installing Agent.

If the agent has already been installed on your virtualization platform, skip this step.

Step 3 Click **Virtualization Platform Logs**.

Step 4 Select the collector, and click **Continue**.

Step 5 Configure the ingestion method for the virtualization platform. For parameter descriptions, see Table 10-7.

Table 10-7 Virtualization Platform Access Parameters

Parameter	Description
Protocol	Currently, only **UDP** is supported.
Port	One port can only ingest data in one format using one protocol. The system port must not be occupied.
Data Format	UDP only supports data ingestion in Syslog format.
Data Encoding	Encoding formats for data ingestion. Available options are **UTF-8**, **GBK**, and **US-ASCII**.

Step 6 Click **Continue** to add the virtualization platform.

a. Click the + icon, configure the IP and name.

b. To add multiple virtualization platforms, click **Batch Add** at the bottom of the page and configure the platform parameters. The parameter descriptions are shown in Table 10-8.

Table 10-8 Batch Add Platform Parameters

Parameter	Description
Platform Name	Select the name of the virtualization platform. Options include **ESXi 6.7 GA** and **vSphere**.
Device IP	Enter the IP addresses or IP ranges of the virtualization platform.

Step 7 Click **Finish** if the collected data does not require field extraction and can be directly stored in the database.

To extract log fields before ingesting log data. Click **Continue Rule**. For details, see Configuring Field Extraction Rules.

----End

Collecting Network Device Traffic

The procedure for collecting network device traffic is as follows:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 Click **Network Device Traffic**.

Step 3 Select the collector, and click **Continue**.

Step 4 Configure the protocol, port, and data format for the access, and click **Continue**.

Step 5 Configure network devices.

a. Configure the device IP, vendor, type, and model/version, then click the + icon.

b. To add multiple network devices, click **Batch Add** at the bottom of the page, and configure the parameters. The parameter description is shown in Table 10-3.

Step 6 Click **Finish**.

----End

Collecting Custom Logs

LAS can collect logs via UDP, FTP, and Kafka protocols. The procedure for UDP and FTP protocols are similar to that for third-party security device logs. For details, see Collecting Third-Party Security Device Logs.

This section only describes the procedure for collecting logs via the Kafka protocol.

Note	Kafka log ingestion requires LAS to proactively pull data from the remote Kafka environment, so make sure the Kafka environment can be successfully accessed by LAS.

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 Click **Custom Logs**.

Step 3 Select the collector, and click **Continue**.

Step 4 Select **Kafka** as the protocol, configure the access parameters, and click **Continue**. Parameter descriptions are shown in Table 10-9.

Table 10-9 Access Parameters for Custom Logs

Parameter	Description
Protocol	Currently supports **UDP**, **FTP**, and **Kafka** protocols.
Port	A port can only ingest data in one format using one protocol. The system port must not be occupied.
Data Format	The supported data formats vary depending on the selected protocol. • **UDP**: only supports Syslog format. • **FTP**: supports JSON, XML, and TEXT formats. • **Kafka**: only JSON format is supported; the format cannot be modified.
Data Encoding	Encoding formats for ingested data. Available options are **UTF-8**, **GBK**, and **US-ASCII**.

Step 5 Enter the log source IP address and click **Continue**.

Step 6 Configure Kafka access parameters. Parameter descriptions are as shown in Table 10-10.

Table 10-10 Kafka Access Parameters Description

Parameter	Description
Immediate Pull	• **Yes**: pull new log data immediately. • **No**: selecting **No** for the first time means pulling all historical data + subsequent new data; selecting **No** for the next n time means pulling all historical data + subsequent new data starting from the time point of the last pull (incremental changes).
Ingestion Rate Limit (entries/second)	The maximum log ingestion rate, defaulting to **0** (no limit).
Connected Nodes	The list displays connected secondary nodes for LAS cluster. • If the list is empty, click **Add Node**, and enter the secondary node IP address and port number. • For existing nodes, click the icon in the **Operation** column to delete the current entry from the list. Click **Test** to test whether LAS can successfully connect to the secondary node.
Connected Topics	The list displays all connected topics. • If the list is empty, you can click **Add Topic**. Select a topic from the drop-down list and enter a topic alias. Click the icon to add multiple topics. • For existing topics, click the icon in the **Operation** column to delete the current entry from the list. Note that topics can only be added when the connection is successful.

Step 7 Click **Finish** if the collected data does not require field extraction and can be directly stored in the database.

To extract log fields before ingesting log data. Click **Continue Rule**. For details, see Configuring Field Extraction Rules.

----End

Collecting File Logs

The procedure for collecting file logs is as follows:

Step 1 Hover over the icon and choose **Data Collection** > **Log Ingestion**, as shown in Figure 10-1.

Step 2 Select **File Logs**.

Step 3 Select the collector, and click **Continue**.

Step 4 Configure the access parameters, and click **Continue**. Parameter description is as shown in Table 10-11.

Table 10-11 File Log Access Parameters

Parameter	Description
Protocol	Currently, only **UDP** is supported.

Parameter	Description
Port	A port can only ingest data in one format using one protocol. The system port must not be occupied.
Data Format	**UDP** only supports data ingestion in Syslog format.
Data Encoding	Encoding formats for data ingestion. Available options are **UTF-8**, **GBK**, and **US-ASCII**.

Step 5 Configure the log sources.

a. Configure the device IP, vendor, type, and model/version, and click the ✚ icon.

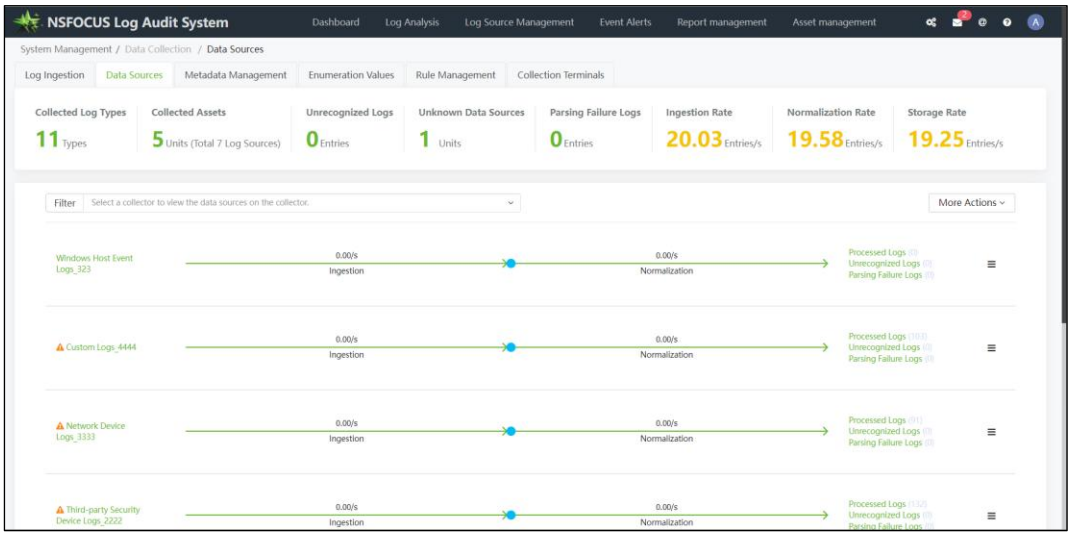
b. To add multiple file log sources, click **Batch Add** at the bottom of the page and configure the parameters. The parameter description is shown in Table 10-3.

Step 6 Click **Finish**.

Step 7 Add file log.

a. Hover over the ⚙ icon and choose **Data Collection > Data Sources**, as shown in Figure 10-10.

Figure 10-10 Data Sources



b. Click the newly added file log data source to enter the page shown in Figure 10-11.

Figure 10-11 File Log Data Source Details

c. Click the icon in the **Operation** column.

d. Click **Select File** / **Select Folder** or drag log files to the designated area, and click **Import**.

----End

Follow-up Operations

After configuring log collection, you can perform the following follow-up operations:

- Click **Collect More Logs**: configure log collection for more log types.
- Click **Configure Discard Rules**: discard unnecessary data to reduce waste of storage and computer resources. For details, see Configuring Discard Rules.
- Click **Search Logs**: search and view ingested logs.
- Click **Create Statistical Items**: create more statistic items for reporting. For details, see Statistics Management.
- Click **Configure Coarse-grained Parsing**: configure log data parsing rules before log ingestion. Only partial log types support coarse-grained parsing. For details, see Log Types.

10.1.1.4 Configuring Field Extraction Rules

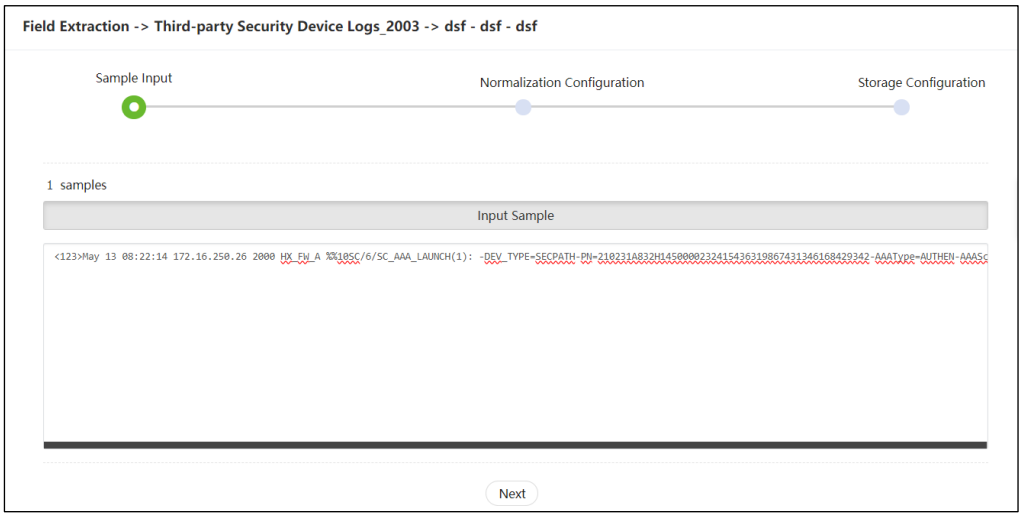
As shown in Table 10-1, LAS doesn't provide built-in log parsing rules for third-party security device logs, network device logs, virtualization platform logs, and custom logs. Manual configuration of field extraction rules is required to extract valid data from logs for normalization.

The procedure for configuring field extraction rules is as follows:

Step 1 Finish the configuration of log ingestion. For details, see Configuring Log.

Step 2 In the **Configuration Completed** page, click **Extract Field** in the **Operation** column to enter the page shown in Figure 10-12.

Figure 10-12 Sample Input



Step 3 Enter sample data in the text box, click **Next**, and by default you will enter the **Field Extraction** page of the normalized configuration, as shown in Figure 10-13.

a. If Syslog is selected as the data format, configure a sample in Syslog format.

b. If JSON is selected as the data format, configure a sample in JSON format.

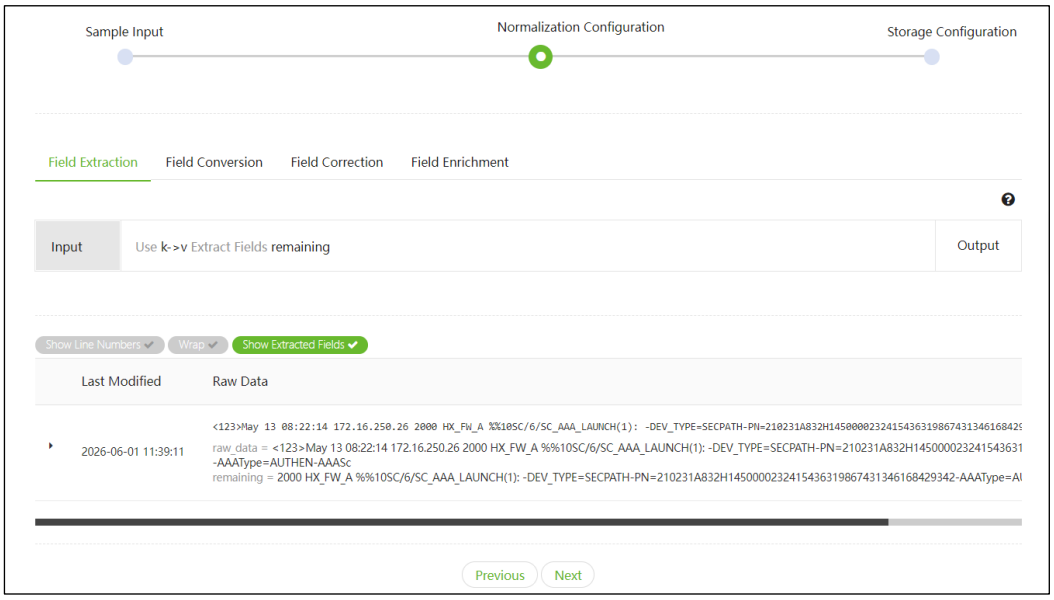
c. If XML is selected as the data format, the sample needs to meet the following format, and LAS currently only supports extracting attributes.

```
<rootelementname><elementname attribute1="value1" attribute
2="value2" ……>content</elementname></rootelementname>
```

d. If TEXT is selected as the data format, configure a sample in text character format.

Note	The bottom of the page displays the pre-parsed results; different data formats yield different numbers of pre-parsed result fields; if the sample is not in standard format, the pre-parsed results will return the original sample text.

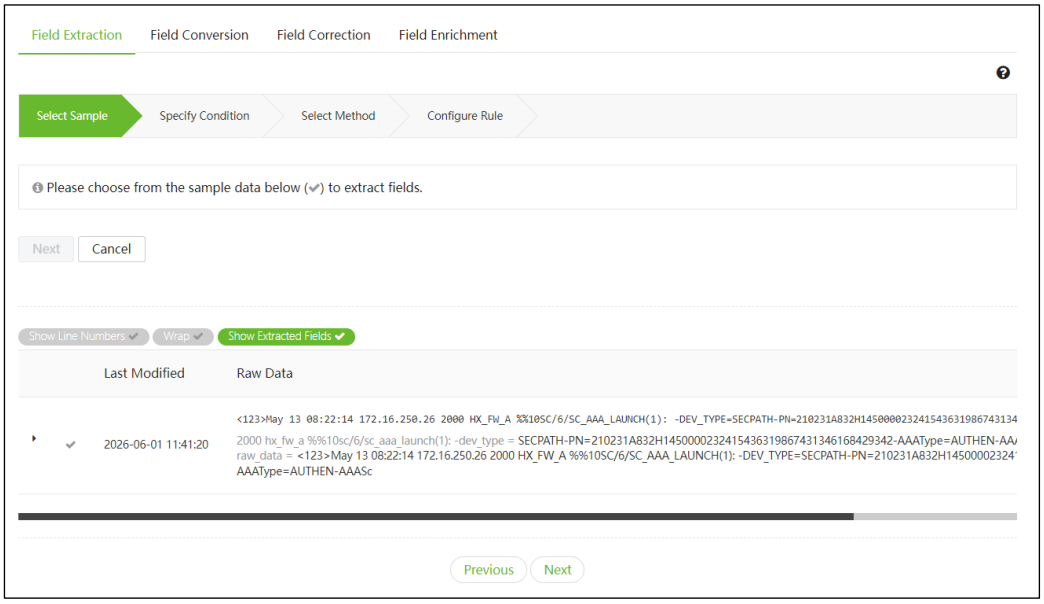
Figure 10-13 Normalization Configuration



Step 4 Configure field extraction rules.

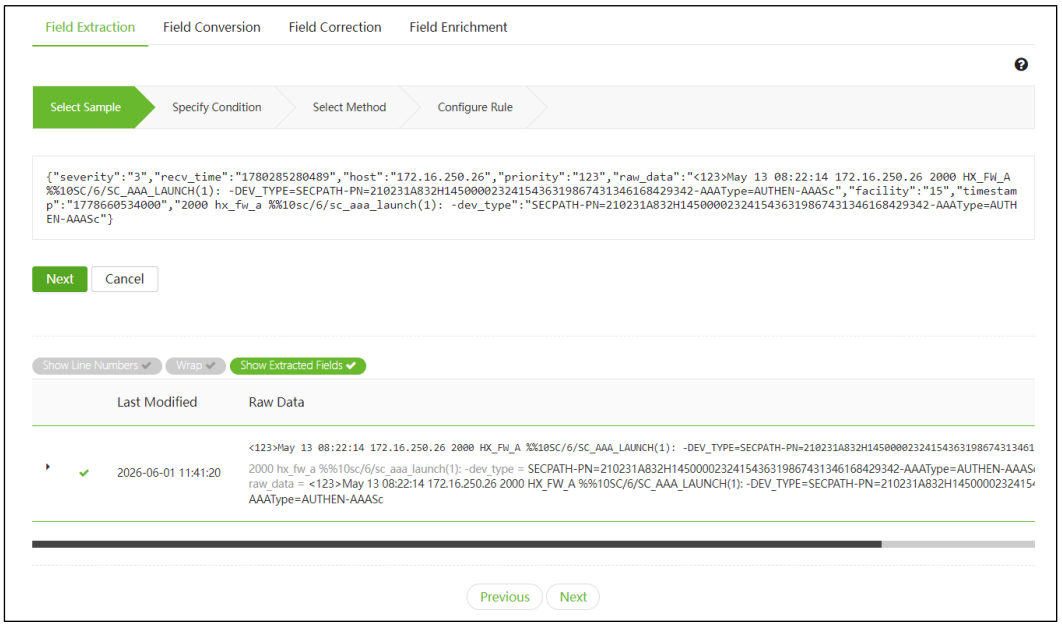
a. Click the ✚ icon to go to the **Select Sample** tab, as shown in Figure 10-14.

Figure 10-14 Selecting Sample



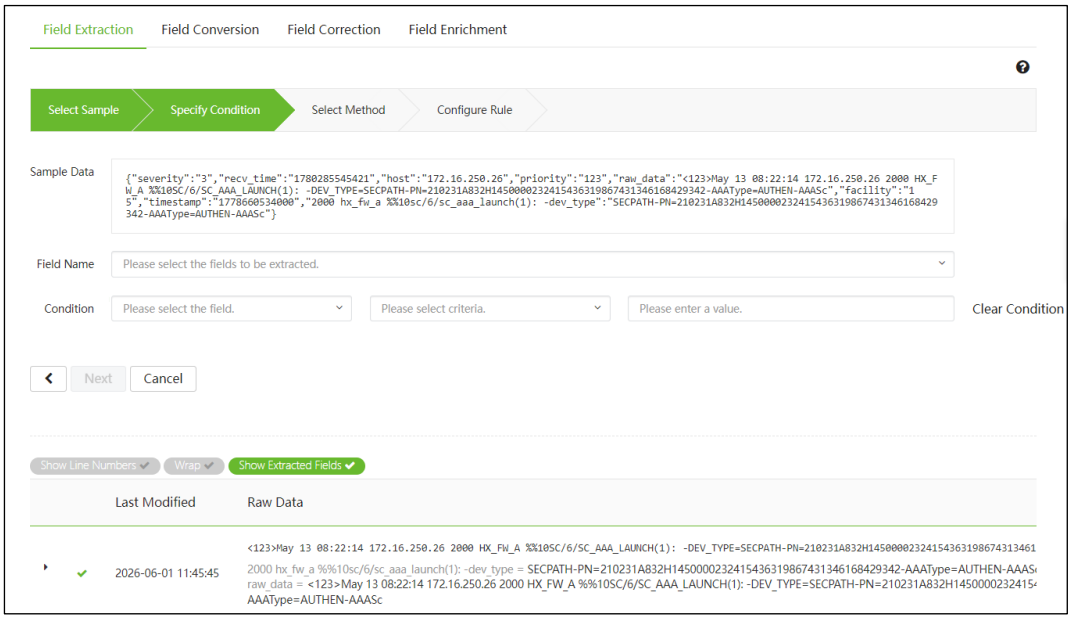
b. Select samples for normalization by clicking the ✔ icon, as shown in Figure 10-15.

Figure 10-15 Selecting Sample



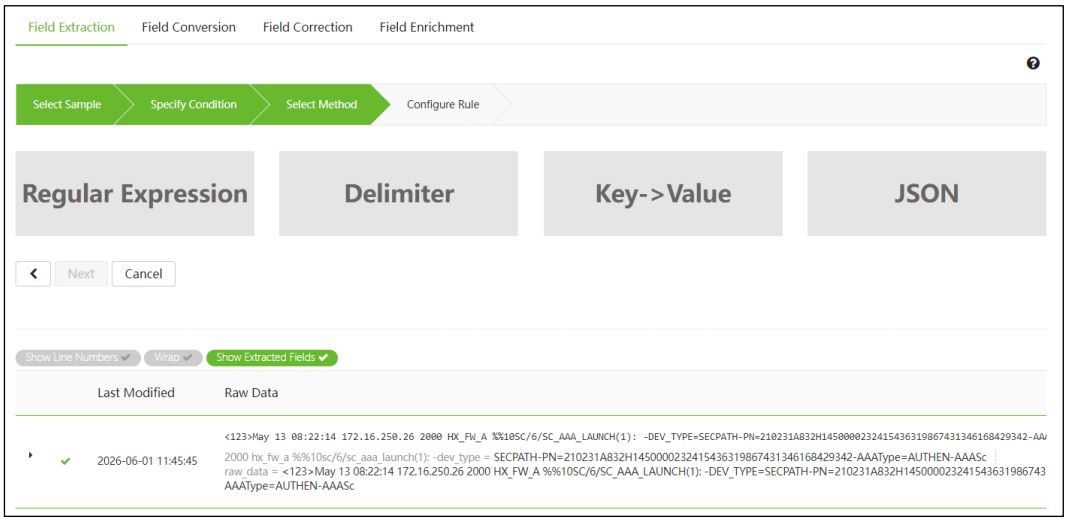
c. Click **Next** above the sample list to enter the **Specify Condition** page, as shown in Figure 10-16.

Figure 10-16 Configuring Specified Conditions



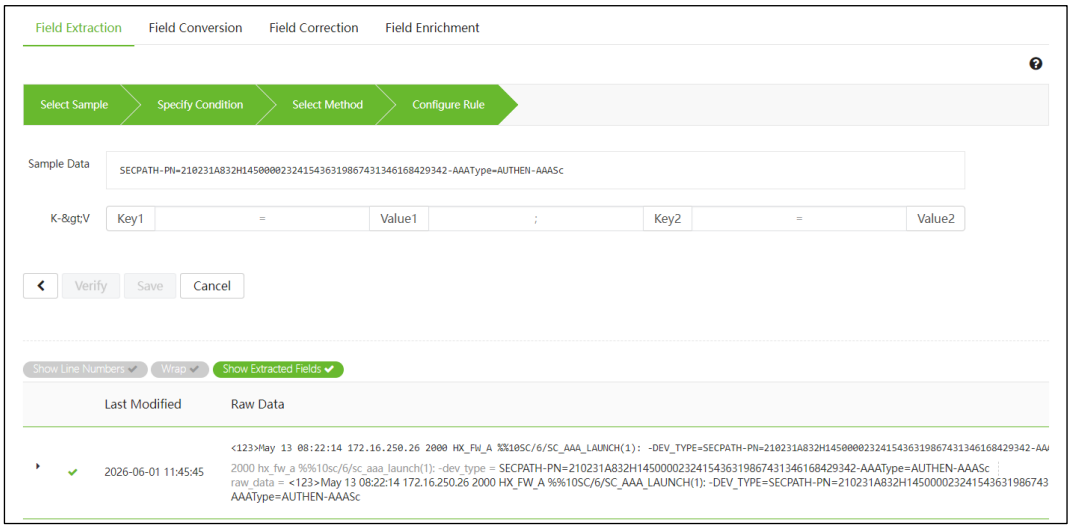
d. Configure field names and conditions to specify under what conditions to parse and extract which fields, and click **Next** above the sample list to enter the **Select Method** page, as shown in Figure 10-17.

Figure 10-17 Selecting Method



e. Choose **Regular Expression/Delimiter/Key->Value/JSON** to extract fields (using regular expression as an example), click **Next** above the sample list to enter the **Configure Rule** page, as shown in Figure 10-18.

Figure 10-18 Configuring Rules

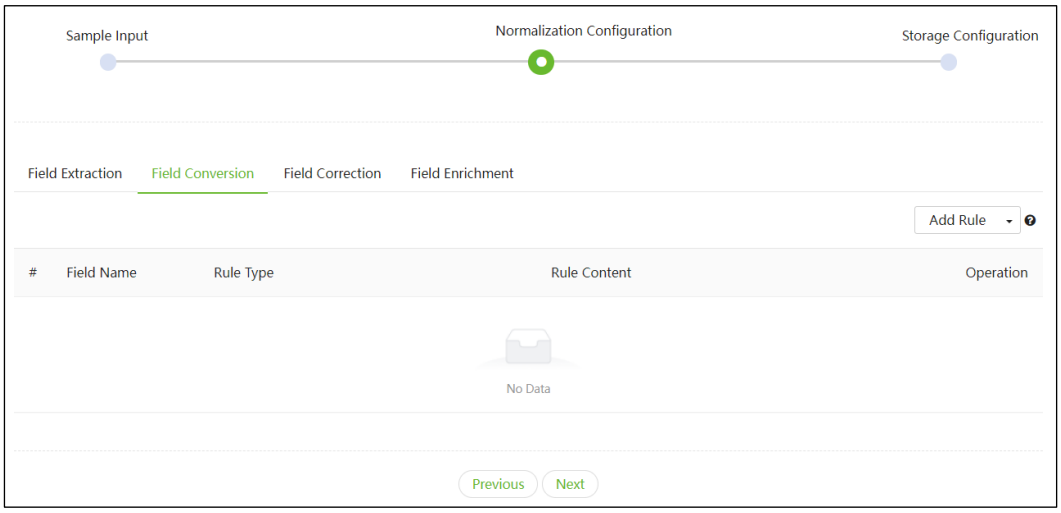


f. Configure specific rules (used for normalizing extracted fields, renaming them to new fields, and writing to the database).
   - Configure extraction specifications. For details, refer to the web interface.
   - Click **Verify** to review the extraction results.
   - Click **Save** to save the field extraction rules.

Step 5 Configure field conversion rules (used to normalize extracted fields to a specified format).

a. Select the **Field Conversion** tab, as shown in Figure 10-19.

Figure 10-19 Field Conversion



b. Click **Add Rule** to configure conversion rules. For parameter descriptions, see Table 10-12.

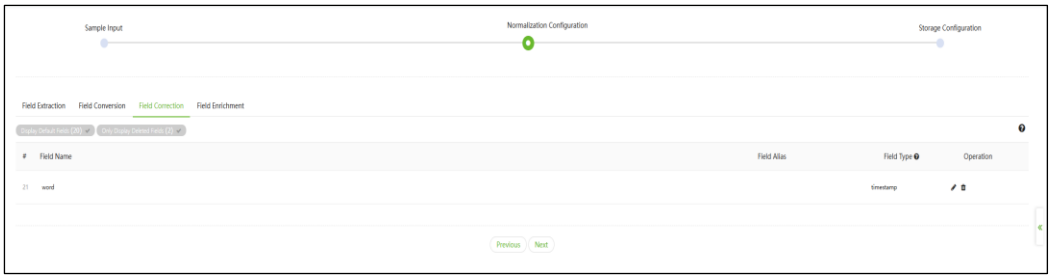
Table 10-12 Conversion Rules

Parameter	Description
Field Name	Name of the field to be converted.
Rule Type	Type of the field rule. • **Timestamp Conversion**: converts the specified time format to a standard timestamp. • **Field Value Mapping**: normalizes the original value in the field to the specified value.

c. Click **Confirm**.

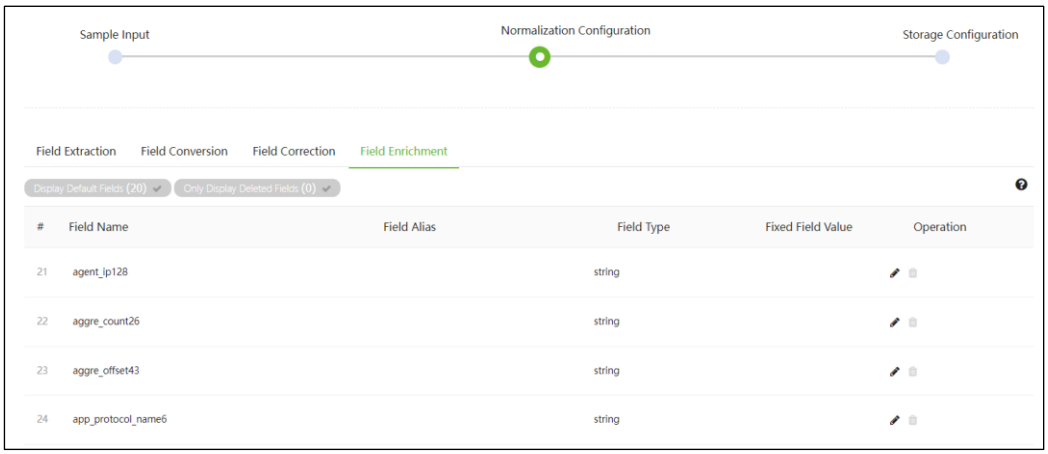
Step 6 Select the **Field Correction** tab to configure field names and types, as shown in Figure 10-20, and click the icon in the **Operation** column to edit the field.

Figure 10-20 Field Correction



Step 7 (Optional) Select the **Field Enrichment** tab to configure field enrichment rules as shown in Figure 10-21. Note that it only is available for third-party security device logs, network device logs, virtualization platform logs, custom logs, and file logs.

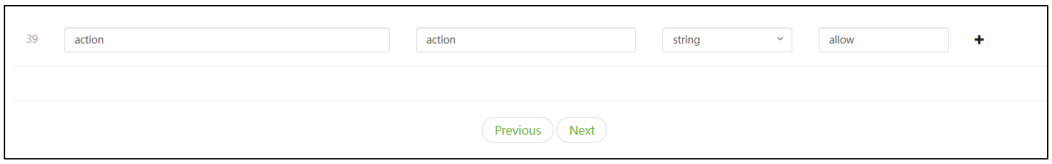
Figure 10-21 Field Enrichment



a. Click the icon to edit a field.

b. Click the icon to add a custom field enrichment, as shown in Figure 10-22.

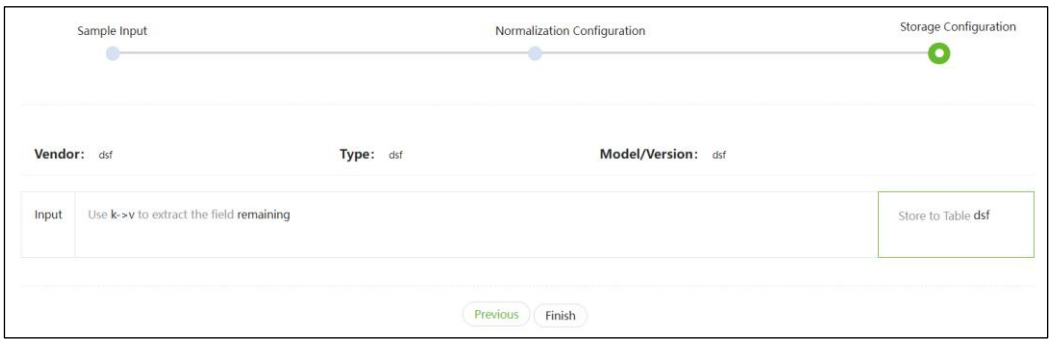
Figure 10-22 Adding Field Enrichment



Step 8 Save rules.

a. Click **Next** to enter the **Storage Configuration** tab, as shown in Figure 10-23.

Figure 10-23 Storage Configuration



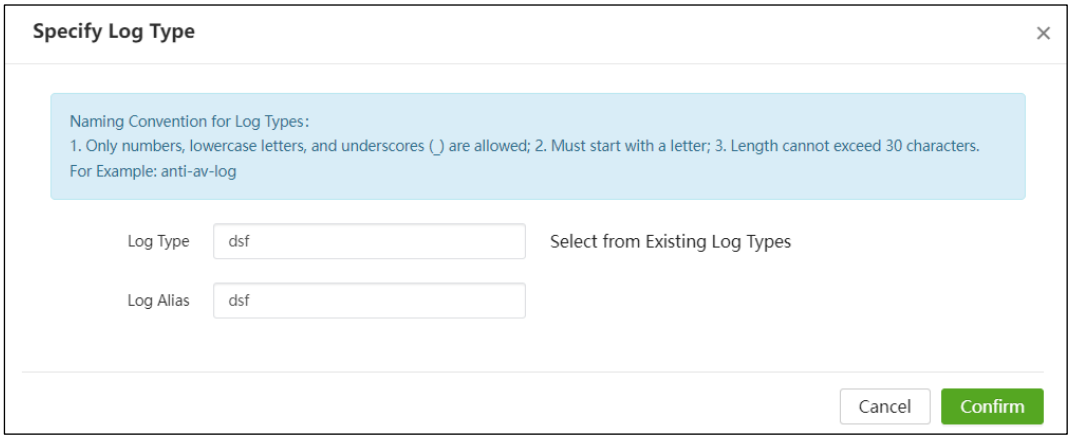
b. Select the field storage mode.

By default, all extracted fields are stored in a data table.

c. Specify the log type.

Click the icon to specify the log type, as shown in Figure 10-24. Click **OK**.

Figure 10-24 Specifying Log Type



Note	The log tables displayed here originate from the custom log tables configured in the Metadata Management module and the built-in log tables of LAS. For details, see Creating a Custom Log Table.

d. View the fields to be extracted.

Click the icon to check whether the fields to be extracted are correct.

e. Click **Finish**.

----End

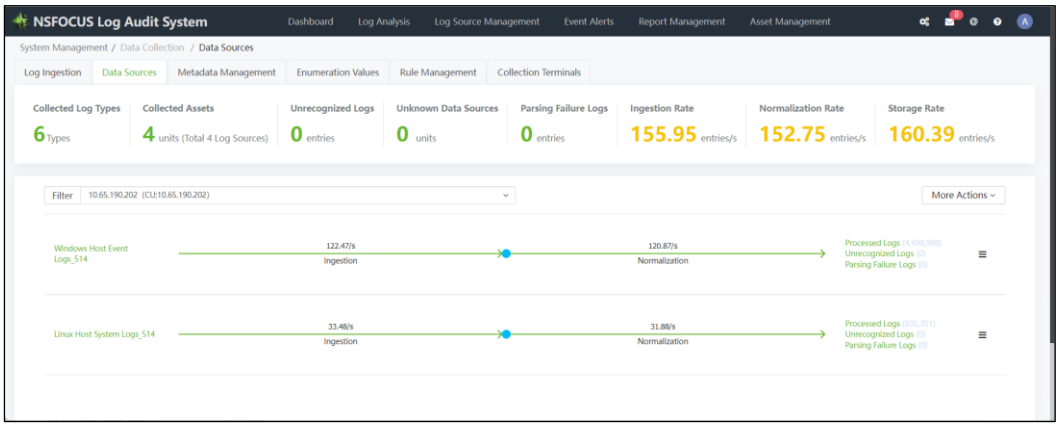
After you finish log object integration and field extraction rule configure, the configured rules will be displayed as custom rules in the Rule Management page.

10.1.2 Data Sources

Integrated log objects are displayed as data sources in the **Data Sources** page. LAS collector extracts their output logs based on corresponding field extraction rules. After extraction, you can manage and configure all stages of log data for each data source in LAS.

Hover over the icon, choose **Data Collection > Data Sources**, where you can view overall statistics of all data sources and manage each data source, as shown in Figure 10-25.

Figure 10-25 Data Sources



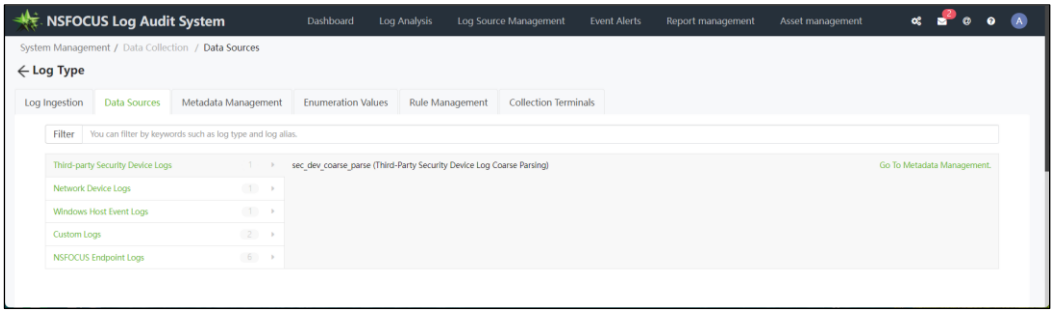
10.1.2.1 Viewing Statistics

As shown in Figure 10-25, the top of the page displays statistics cards for all data sources. Click a statistics card to choose the corresponding log type list to view more details.

Viewing Collected Log Types

Click on the number of the **Collected Log Types** card. The left side of the page displays all log types ingested into LAS. Hover over a log type to view its sub-log types on the right side of the page, as shown in Figure 10-26.

Figure 10-26 Connected Log Types



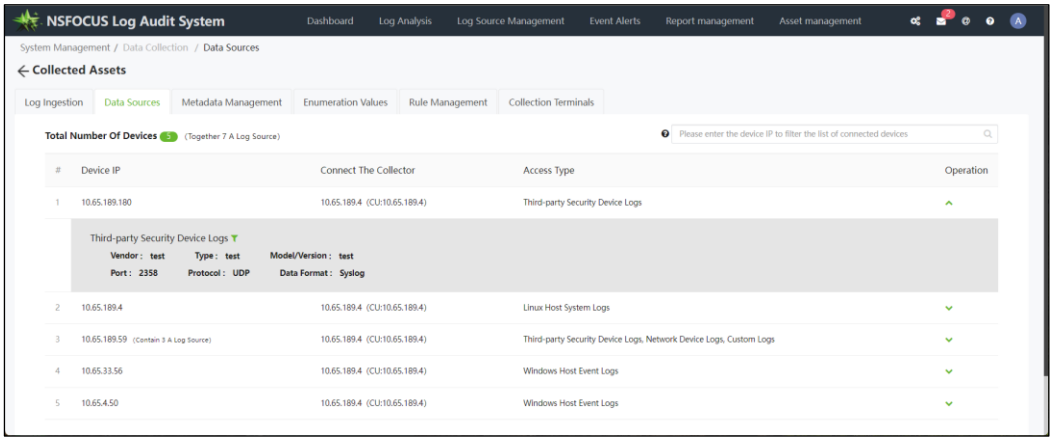
Click a sub-log type to view field details contained in that type of log, as shown in Figure 10-27.

Figure 10-27 Field Details for Sub-log Types

Viewing Collected Assets

Click on the number of the **Collected Assets** card to view the collected devices. Click the icon in the **Operation** column to view the details of the corresponding device, as shown in Figure 10-28.

Figure 10-28 Connected Assets (Log Sources) Details

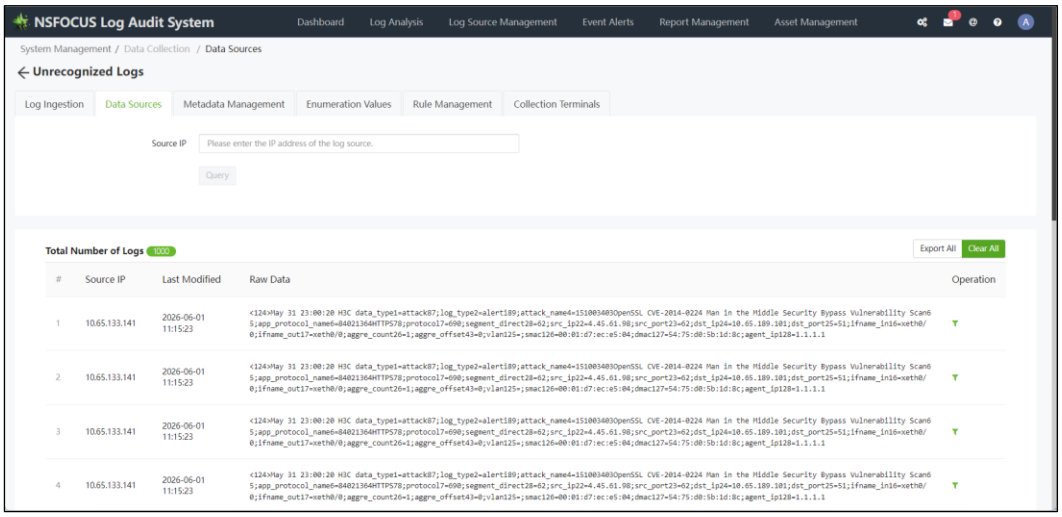


Viewing Unrecognized Logs

Click on the number of the **Unrecognized Logs** card to view log information that does not match existing rules and has not yet configured field extraction rules. Only the latest 1,000 records are displayed, as shown in Figure 10-29.

Click the icon in the **Operation** column, execute the Configuring Field Extraction Rules operation, which will automatically use the original log text as a sample.

Figure 10-29 Unrecognized Logs

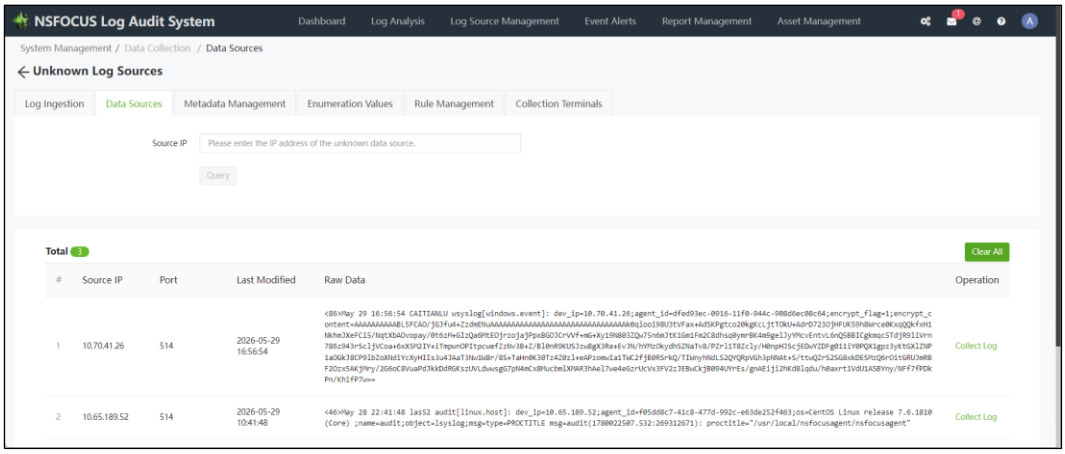


Viewing Unknown Data Sources

If a device IP that has not been configured for log ingestion sends log data to LAS, LAS will classify the device as an unknown data source.

Click on the number of the **Unknown Data Sources** card to view detailed information about unknown data sources, including source IP, port, reception time, and raw data, as shown in Figure 10-30.

Figure 10-30 Unknown Data Sources



It also supports the following operations on unknown data sources:

- Query a specified unknown data source by source IP address.
- Retain only the latest log entry for each unknown source IP.
- Click **Collect Log** in the **Operation** column to configure log collection for the unknown data sources. You can configure the ingestion using existing rules or through custom configurations. The configuration parameters are described in Table 10-13.

Table 10-13 Unknown Data Source - Configuration Parameters for Log Collection

Parameter		Description
Select Log Type	Log Type	Select a log type from the drop-down menu. Available options include: **Third-Party Security Device Logs**, **Network Device Logs**, **Virtualization Platform Logs**, and **Custom Logs**.
Select Collector	Collector	Select a log collector from the drop-down menu.
Configure Access Method	Protocol	Protocol used for log ingestion.
	Port	Port number used for log ingestion.
	Data Format	Log data format.
	Data Encoding	Data encoding method. Available options include: **UTF-8**, **GBK**, and **US-ASCII**.
Add Devices	Device IP	IP address of the log source device.
	Vendor	Vendor of the log source device.
	Type	Log source device type.
	Model/Version	Log source device model or version.

Viewing Parsing Failure Logs

Click on the number of the **Parsing Failure Logs** card to view log messages that match existing field extraction rules but failed to parse, as shown in Figure 10-31.

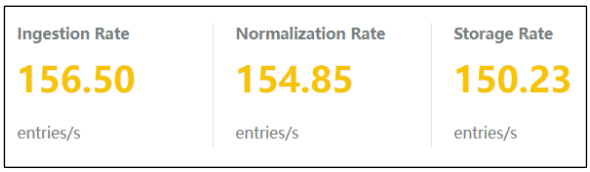
View parsing failure logs to verify whether the configured field extraction rules cover all uploaded logs. If not fully covered, click the icon in the **Operation** column to execute the Configuring Field Extraction Rules operation and modify the field extraction rules.

Figure 10-31 Parsing Failure Logs

Viewing Log Rates

The top of the **Data Sources** page also displays the rate of log ingestion, the rate of field normalization, and the rate of writing fields to the database in real-time, as shown in Figure 10-32.

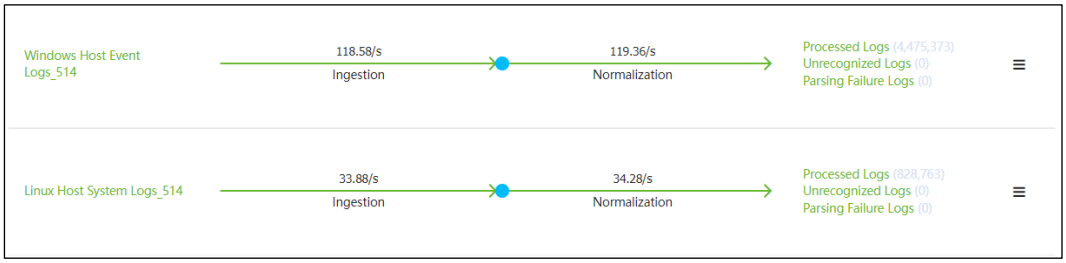
Figure 10-32 Viewing Log Processing Rates



Viewing Processing Information

The **Data Sources** page displays the ingestion rate of corresponding logs, the rate of normalized fields, and the number of processed/unrecognized/parsing failure logs for collected data sources, as shown in Figure 10-33.

Figure 10-33 Viewing Data Source Processing Information



More Operations

In the area shown in Figure 10-33, you can perform the following operations on data sources:

Querying Data Sources

Select a collector in the **Filter** area, and the list will only display data sources belonging to that collector.

Editing Data Sources

Choose ☰ > **Edit** to edit the name of the corresponding data source.

Deleting Data Sources

Choose ☰ > **Delete** to delete the corresponding data source. After deletion, the collector will no longer ingest and parse the corresponding log information.

Enabling/Disabling Data Sources

Choose ☰ > **Enable/Disable** to enable or disable the corresponding data source. After disabling a data source, the collector will no longer ingest and parse the corresponding log information.

Backing Up Data Sources

Choose **More Actions > Back Up Data Source**. After selecting the data source and collector to be backed up, you can export the specified data locally.

Restoring Data Sources

You can import a backup data source back to LAS for restore.

Choose **More Actions > Restore Data Source**, select the data under the collector to be restored, and import the specified data to LAS.

Configuring NAT

When a data source device connected to LAS uses NAT (Network Address Translation) to translate its real IP address, you can configure NAT in LAS to record the data source's real IP address, NAT forwarding server IP address, and data source device tag as the unique identifier of the data source device.

To configure NAT, follow the following steps:

Step 1 Choose **More Actions > Configure NAT**.

Step 2 Select the collector, and click **Continue** to configure the NAT access port.

Note	NAT access configuration cannot be modified. Among devices that underwent NAT before integrating with LAS, only those meeting one of the following conditions can configure NAT: • UDP is used. • Port number is consistent with that of the data source. • Data format is Syslog.

Step 3 Click **Continue** to configure NAT parameters and add data source devices that access LAS through NAT. Parameter descriptions are shown in Table 10-14.

Table 10-14 NAT Data Source Parameters

Parameter	Description
NAT IP	NAT server IP address used by the data source.
Device IP	Real IP address of the data source.
Device Tag	Select a string from the device logs that uniquely identifies the device type as the

Parameter	Description
	device tag.

Step 4 Click the + icon to add the data source device.

Step 5 Click **Finish** to save the NAT configuration.

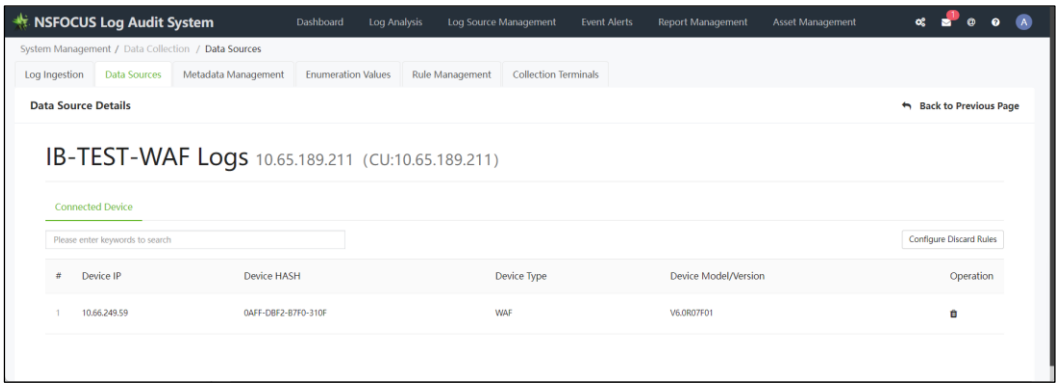
----End

10.1.2.2 Managing Data Sources

In the area shown in Figure 10-33, click the data source name to view and manage the data source configuration.

The management for each type of data source is similar. The following section uses third-party security device logs as an example, as shown in Figure 10-34.

Figure 10-34 Data Source Details



- In the **Connected Device** tab, you can view/delete connected devices, configure field extraction rules, and then configure discard rules. For file logs, uploading logs in file or folder format is supported. Some types of logs also support configuring log aggregation rules. For details, see Managing Connected Device.
- In the **Configuration** page, you can modify the access parameters for this data source. For details, see Managing Access Configuration.

Managing Connected Devices

In the data source module, you can configure and manage the connected devices.

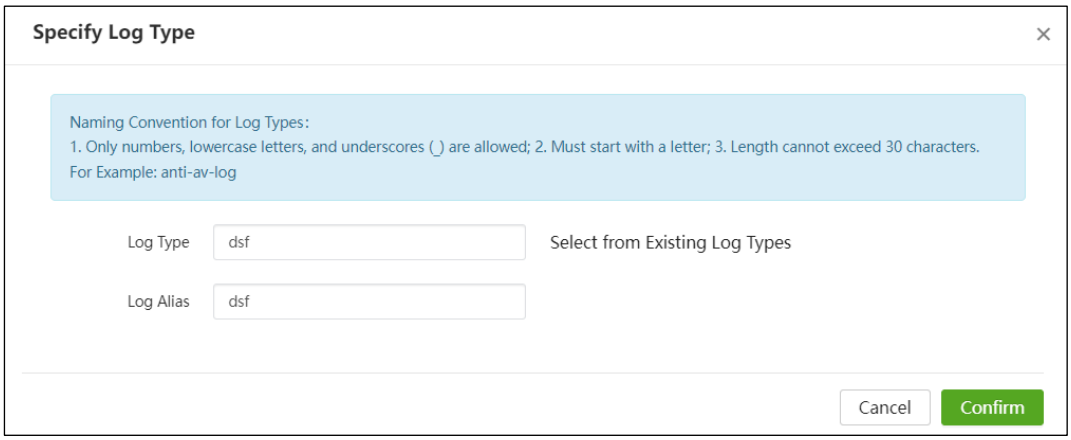
Deleting Connected Devices

Click the 🗑 icon in the **Operation** column to delete the corresponding connected device.

Configuring Coarse-grained Extraction

Click the icon in the **Operation** column, configure the log type and log alias in the popup dialog, then click **Confirm** to configure coarse-grained parsing rules, as shown in Figure 10-35.

Figure 10-35 Coarse-grained Extraction



Note	• Not all log types support coarse-grained extraction. See Log Type Description. • After configuring coarse-grained parsing rules, the configured coarse-grained parsing rules will be automatically applied to extract logs when collecting logs from the same vendor, type, and model/version.

Configuring Field Extraction Rules

Click the icon in the **Operation** column to configure the field extraction rules for data reported by the corresponding device. For details, see Configuring Field Extraction Rules.

Configuring Discard Rules

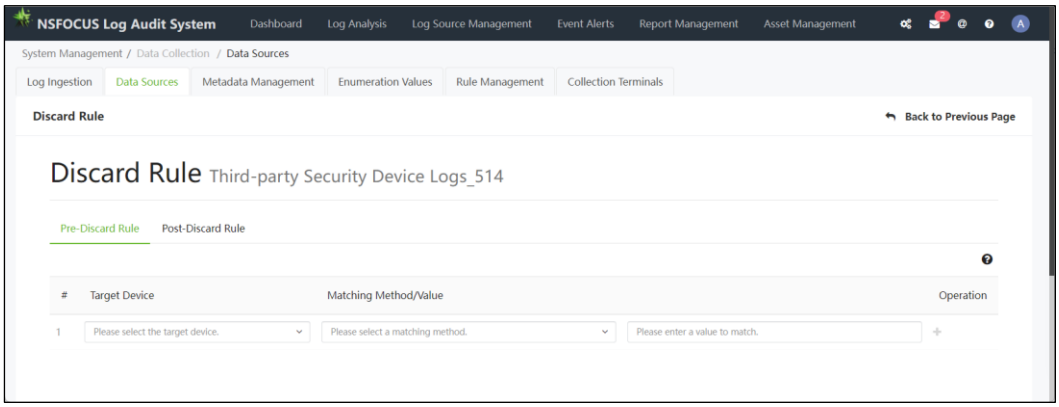
By configuring discard rules, you can discard unnecessary fields to save storage and computing resources. Discard rules are divided into two types:

- Pre-discard rule: discards the entire log entry before the collector parses fields.
- Post-discard rule: discards a specific characteristic string in Syslog only after the collector parses fields.

The procedure for configuring discard rules after configuring log collection is as follows:

Step 1 Click **Configure Discard Rules** to enter the page shown in Figure 10-36.

Figure 10-36 Discard Rules (Pre-discard Rules)



Step 2 Configure pre-discard rules.

Configure target devices and matching rules (click the + icon to add more rules).

Step 3 Configure POST-discard rules.

Configure target devices and matching rules (click the + icon to add more rules).

----End

Configuring Log Merge Rules

The following log types support configuring log merge rules, including:

- Third-party security device logs with UDP access
- Network device logs with UDP access
- Linux host system logs
- Windows host event logs

Click **Configure Merge Rules** to configure the target device, merge fields, and merge time window.

Managing Access Configuration

Access configuration refers to configuring the access parameters for the connected data source.

Choose the **Configuration** tab, and then click **Edit** to configure the parameters described in Table 10-15, and click **Apply**.

Table 10-15 Data Source Access Parameters

Parameter	Description
Protocol	Currently, only **UDP** is supported.
Port	A port can only accept data in one format using one protocol. The system port must not be occupied.

Parameter	Description
Data Format	• When the access protocol is **UDP**, only Syslog is supported. • When the access protocol is **FTP**, JSON and XML are supported.
Data Encoding	Encoding formats for ingested data. Available options are **UTF-8**, **GBK**, and **US-ASCII**.

10.1.3 Metadata Management

For different connected log sources, LAS creates log tables in the Clickhouse database according to specific metadata fields for storing parsed logs. LAS provides built-in log tables and supports custom log tables.

Hover over the icon and choose **Data Collection** > **Metadata Management**. By default, the page displays various types of built-in log tables.

Creating a Custom Log Table

In the **Metadata Management** page, click **Create Log Table** and configure parameters to customize a log table. Parameter descriptions are shown in Table 10-16.

Table 10-16 Log Table Parameters

Parameter	Description
Log Type	Select the log type group for the log object. Available options include: **Third-Party Security Device Logs**, **Network Device Logs**, **Virtualization Platform Logs**, **Custom Logs**, and **File Logs**.
Table Name	Name of the log table. Only numbers, lowercase letters, and underscores (_) are allowed; it must start with letters and its length cannot exceed 30 characters.
Table Alias	Alias of the log table name.
New Field	Add a field to the log table. Only numbers, lowercase letters, and underscores (_) are allowed; it must start with letters and its length cannot exceed 30 characters.
Field Name	Name of the field.
Field Alias	Alias of the field name.
Exact Search	Whether exact search is enabled for this field or not.
Field Type	Type of the field. Available options include: **float**, **int**, **string**, and **timestamp**.

Filtering Log Table

The log table list in the **Metadata Management** page supports fuzzy search and supports the following filters:

- Click the icon in the **Built-in** column, select the log table type, and filter matched log tables.

- Click the icon in the **Log Source** column, select the log type to filter matched log tables.

Viewing Log Table Details

In the **Metadata Management** page, click **View More** in the **Operation** column to view details of log tables.

Editing Log Table

In the **Metadata Management** page, select **View More > Edit** in the **Operation** column to edit the log table.

Both built-in log tables and custom log tables support editing the log table alias, but do not support editing the log type group and table name. The other editable content for both is slightly different:

- For built-in log tables: in the list, select **View More > Edit** in the **Operation** column to enable exact search for the selected fields. Adding fields is not supported.
- For custom log tables: in the list, select **View More > Edit** in the **Operation** column to edit the alias, types, and enable exact search for the selected fields. Adding fields and deleting individual fields are supported.

Copying Log Table

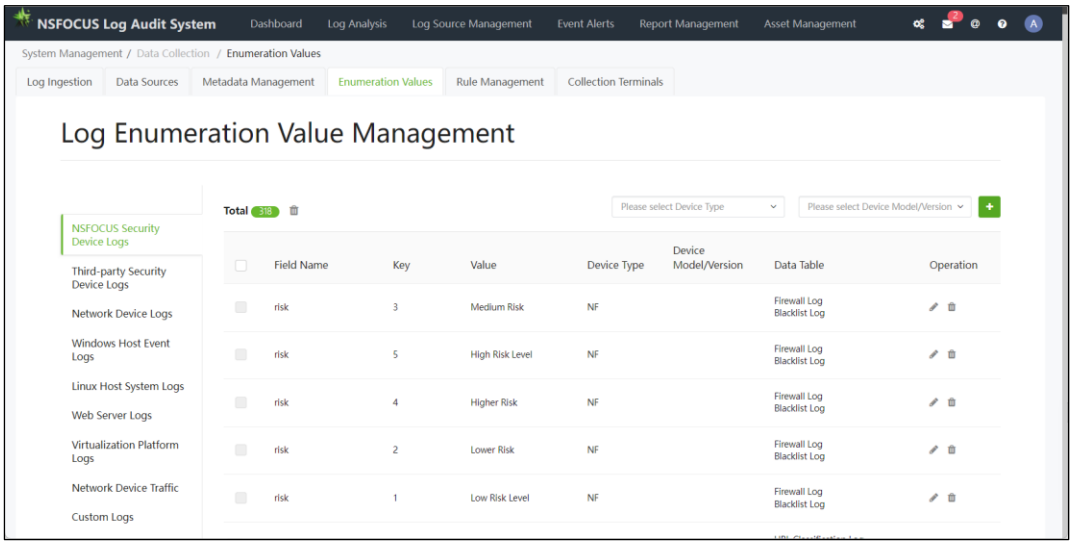
In the **Metadata Management** page, select **View More > Copy** in the **Operation** column to copy a built-in or custom log table for quickly creating a custom log table.

10.1.4 Enumeration Values

Enumeration values are used to map field names and key values of various data sources in output logs to easy-to-understand values.

Hover over the icon and choose **Data Collection > Enumeration Values**. The left side of the page displays log type categories, while the list on the right side shows the existing enumeration values for the corresponding log type category, as shown in Figure 10-37.

Figure 10-37 Enumeration Value



The management operations for enumeration values of various log types are basically identical. The following uses NSFOCUS security device logs as an example.

Click the icon to configure the enumeration values for NSFOCUS security device logs. The enumeration value parameter description is shown in Table 10-17.

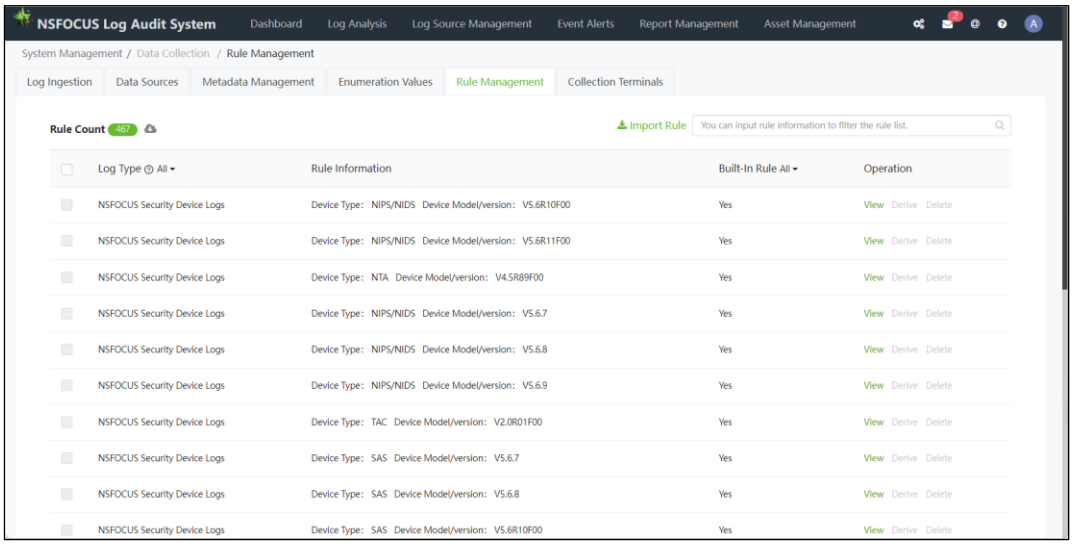
Table 10-17 Enumeration Value Parameters (NSFOCUS Security Device Logs)

Parameter	Description
Device Type	Type of NSFOCUS security device.
Device Model/Version	Model/Version of the selected device type.
Field Name	Field name in the log that needs to be mapped. Up to 30 characters are allowed.
Key	Value of the field name to be mapped in the log. Up to 64 characters are allowed.
Value	Content after mapping field names in logs to corresponding keys. Up to 16 characters are allowed.

10.1.5 **Rule Management**

Hover over the icon and choose **Data Collection > Rule Management**. By default, built-in log rules are displayed, as shown in Figure 10-38. In the **Rule Management** page, you can view, import, and export log parsing rules.

Figure 10-38 Rule Management



Note	• Built-in log parsing rules cannot be deleted or exported. • Built-in log parsing rules for NSFOCUS security device logs, database data, Linux host systems, and web server logs cannot be derived.

Importing Rules

Click **Import Rule**, and then click **Select File** or drag the log rule file (.dat) to the specified area, click **Import**.

Exporting Rules

Click the icon above the rule list to batch export selected rules.

Viewing Rules

In the rule list, click **View** in the **Operation** column to view the corresponding rule details.

Deriving Rules

In the rule list, click **Derive** in the **Operation** column to make modifications based on the selected rule and generate a custom log rule.

Deleting Rules

In the rule list, click **Delete** in the **Operation** column to delete the corresponding custom log parsing rule.

10.1.6 Collection Terminals

Collection terminals include collectors, devices, and agents.

10.1.6.1 Collector

Collector is a data acquisition component used to receive and parse data (for example: logs, traffic, etc.), normalize it in a unified format, and send it to LAS.

Hover over the icon, and choose **Data Collection > Collection Terminals > Collector**. In the collector list, you can click the icon in the **Operation** column to edit the collector's alias.

10.1.6.2 Device List

Devices refer to NSFOCUS security devices, for example, NIPS and NIDS. Only after a device is connected to LAS, it can report logs/data to the collector.

Different versions of NSFOCUS security devices vary slightly for accessing to LAS on the device side, as shown in Table 10-18.

Table 10-18 Device Access Method

Device Version Status	Device and Version	Registering via Device
New Device	NF v6.0R01F05	Configure on the device's Web-based Manager. For details, see Registering via New Device.
	NF v6.0R03F00	
	NF v6.0.1	
	NIDS/NIPS v5.6R10F00	
	NIDS/NIPS v5.6R10F01	
	NIDS/NIPS v5.6R10F02	
	NIDS/NIPS v5.6R11F00	
	TAC v2.0R01F00	
	TAC v2.0R01F01	
	TAC v2.0R02F00	
	TAC v2.0R02F01	
	SAS v5.6R10F00	
	WAF v6.0R06F00	
	WAF v6.0R06F01	
	WAF v6.0R07F00	
	WAF v6.0R07F01	
	SAS-H v5.6R10F00	
Legacy Device	NIDS v5.6.7~ v5.6.9	Configure on the device's Web-based Manager. For details, see Registering via Legacy Device.
	NIPS v5.6.7~ v5.6.9	
	SAS v5.6.7~ v5.6.8	
	WAF v6.0R05F01	

Note	Device management varies across different devices and versions. Refer to the web interface for details. This section only covers how to manage devices on LAS.

Hover over the icon and choose **Data Collection** > **Collection Terminal** > **Device**. When a NSFOCUS device connects to LAS via a non-management interface, click the icon at the upper-right corner of the device list to configure NAT-specific parameters for NSFOCUS devices. Click **Configure** to add a device or go to the device side to integrate with LAS. The NAT-specific parameters for NSFOCUS devices are described in Table 10-19.

Table 10-19 NSFOCUS Device NAT Scenario-specific Parameters

Parameter	Description
IP Address of Access Point	IP address of LAS non-management interface or the NAT-mapped IP of LAS. Both IPv4 and IPv6 is allowed.
Device HASH	HASH value of the NSFOCUS device to be connected.

10.1.6.3 Agent

Agents can be installed on Windows/Linux hosts, web servers, virtualization platforms, or custom log sources.

Downloading Agent

LAS supports the following two methods of downloading agent:

Method 1

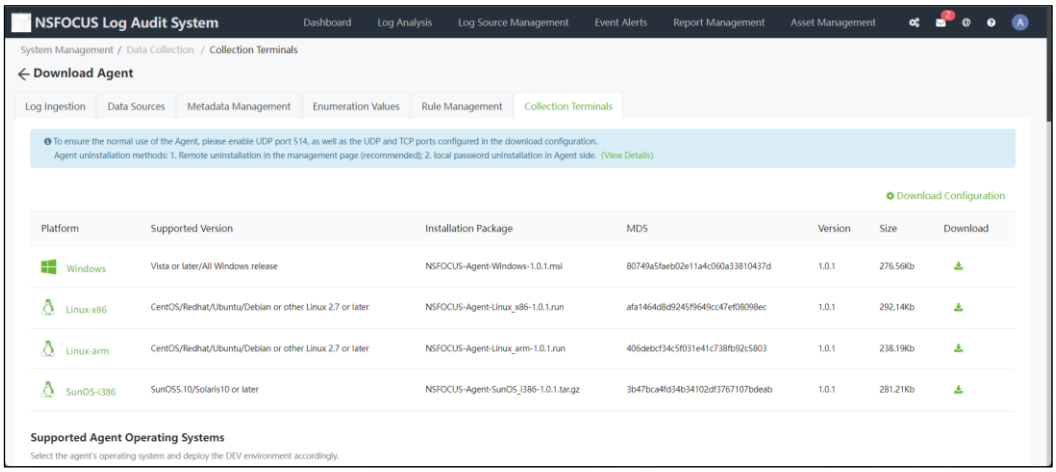
Step 1 Hover over the icon and choose **Data Collection > Log Ingestion**.

Step 2 Hover over **Windows Host Event Logs** or **Linux Host System Logs**, and the agent with a switch for auto-access appear at the upper-right corner.

LAS can ingest Windows/Linux host logs via the NSFOCUS log collection agent. For details, see Operating Systems Supported by Agent.

Step 3 Click **Agent** to enter the agent download page, as shown in Figure 10-39.

Figure 10-39 Agent Download Page



Step 4 Configure the parameters for downloading agents.

Click **Download Configuration** at the upper-right corner of the page to configure the parameters for agent communication with LAS. The parameter description is shown in Table 10-20.

Table 10-20 Agent Download Parameters

Parameter	Description
Management Center IP	IP address of LAS. If left blank, the platform's agent is downloaded by default; if an IP address is configured, the agent for the configured IP is downloaded.
UDP Port	UDP port number used for communication between the agent and LAS, defaulting to **17046**.
TCP Port	TCP port number used for communication between the agent and LAS, defaulting to **17047**.
Service Working Group	Name of service working group displayed for the agent in the client service. Defaults to **nsfocus** and cannot be modified.
Service Name	Service name displayed for the agent in the client service. Defaults to **nsfocusagent** and cannot be modified.
Product Identifier	Flag for determining agent coexistence, defaulting to **No**. **Yes** indicates that the agent can coexist with scanners, UES, and other agents.

Step 5 Download agent.

Return to the agent list, click the icon in the **Download** column, and download the corresponding agent based on the installation platform to your local machine.

----End

Method 2

Step 1 Hover over the icon and choose **Data Collection > Collection Terminals > Agent**.

Step 2 Click **Download Agent**.

Step 3 In the agent list, click the icon in the **Download** column to download the corresponding agent based on the installation platform to the local device.

----End

Installing Agent

Agent can be installed on Windows, Linux, and Unix systems. For details, see Operating Systems Supported by Agent.

Installing on Windows

Double-click or right-click the installation package **NSFOCUS-Agent-Windows-1.0.1.msi**, select **Install**, and after confirming the installation, the environment check is required; once the environment requirements are met, the configuration and installation are automatically completed.

Installing on Linux

Step 1 Log in to the Linux host with root privileges.

Step 2 Execute the **chmod 755 NSFOCUS-Agent-Linux_x86-1.0.1.run** command to grant 755 permissions on the Linux system, as shown in Figure 10-40.

Figure 10-40 Installing Agent on Linux - Granting Permissions

```
[root@lasdot101 opt]#
[root@lasdot101 opt]#
[root@lasdot101 opt]# chmod 755 NSFOCUS-Agent-Linux_x86-1.0.1.run
[root@lasdot101 opt]#
[root@lasdot101 opt]# ll | grep Agent
-rwxr-xr-x  1 root root 289161 Nov 19 17:40 NSFOCUS-Agent-Linux_x86-1.0.1.run
[root@lasdot101 opt]#
```

Step 3 Execute the **./NSFOCUS-Agent-Linux_x86-1.0.1.run** command to install the agent, as shown in Figure 10-41.

Figure 10-41 Installing Agent on Linux: Executing Installation

```
[root@lasdot101 opt]#
[root@lasdot101 opt]#
[root@lasdot101 opt]# ./NSFOCUS-Agent-Linux_x86-1.0.1.run
current machine x64
[ ok ] nsfocusagent.service start
agent install successfully in /usr/local/nsfocusagent/nsfocusagent
[root@lasdot101 opt]#
```

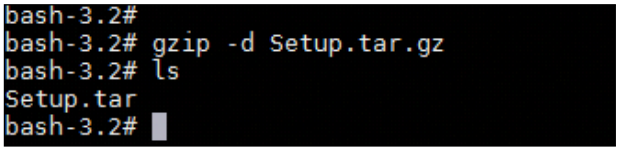
----End

Installing on Unix

Step 1 Log in to the Solaris 10 host.

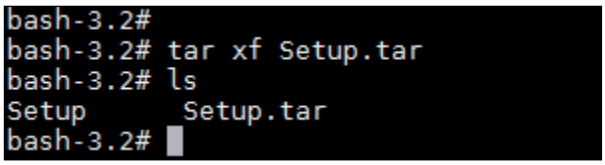
Step 2 Execute the **gzip -d Setup.tar.gz** command to decompress the setup.tar.gz file and obtain the setup.tar archive, as shown in Figure 10-42.

Figure 10-42 Installing Agent on Unix: Decompressing Setup File



Step 3 Execute the **tar xf Setup.tar** command to extract the setup.tar file, as shown in Figure 10-43.

Figure 10-43 Installing Agent on Unix: Extracting Setup File



Step 4 Execute the **cd setup** command to enter the setup folder.

Step 5 Execute the **./install.sh** command to install the agent.

----End

Viewing Agents

Hover over the icon and choose **Data Collection > Collection Terminals > Agent**, which displays information of installed agents. Select an agent in the list to expand and view its configurations.

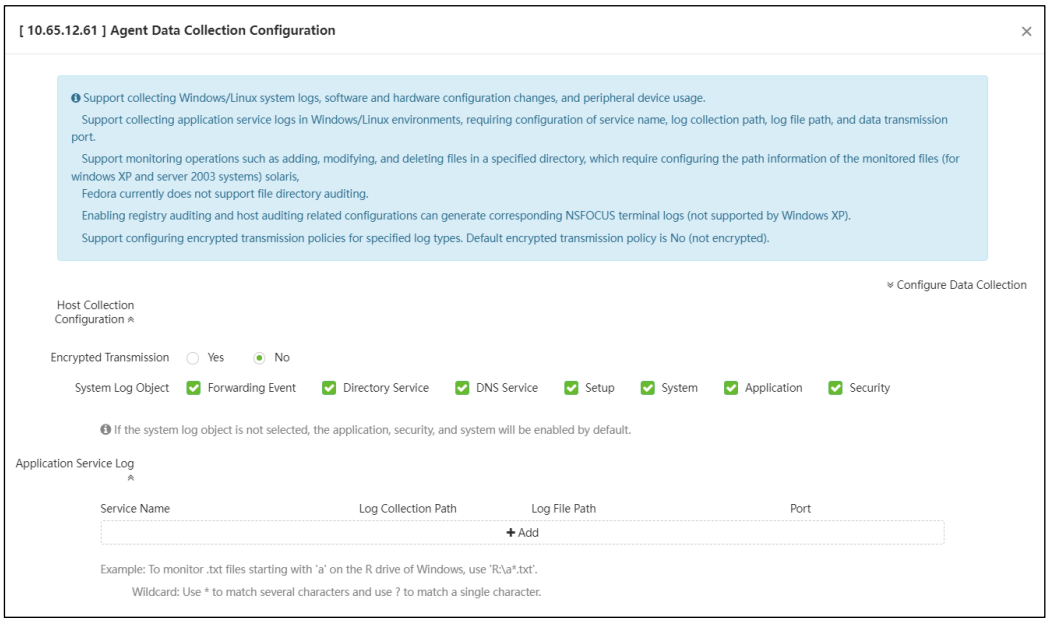
Configuring Agents

After installing an agent, you must also configure data collection for the agent to send log data to LAS.

Using Windows agent as an example, the procedure of configuring data collection is as follows:

Step 1 In the agent list, click the icon in the **Operation** column, and the agent data collection configuration is shown in Figure 10-44.

Figure 10-44 Configuring Agent Data Collection on Windows



Step 2 Configure host collection parameters. Parameter descriptions are shown in Table 10-21.

Table 10-21 Host Collection Parameters

Parameter	Description
Encrypted Transmission	Whether an encrypted transmission strategy is used during data transmission.
System Log	By default, it collects logs for application, security, and system when disabled. You can also select to collect forwarding event, directory service, DNS service, and setup.

Step 3 Configure application service logs.

Click **Add** to configure application service log parameters. Parameter description is shown in Table 10-22. Adding multiple application service logs is allowed.

Table 10-22 Application Service Log Parameters

Parameter	Description
Service Name	Built-in services include the following types: • **Nginx Server Log**: corresponds to the web server's Nginx access format. • **Linux Host User Activity Log**: the system log corresponding to the Linux host. • **Apache Access Log**: corresponds to the common log format of the Apache service type for web server access. • **Apache Error Log**: corresponds to the error log of the Apache service type for web server access. • **WebLogic Server Log**: corresponds to the custom log format for the WebLogic service type connected to the web server.

Parameter	Description
	• **IIS Server Log**: corresponds to the custom log format for the IIS service type of web server access. In addition to the above built-in services, you can customize application services. The recommended format is "application type"."log type". For example, "apache.access" refers to Apache access logs.
Log Collection Path	Parent folder path of the service log file.
Log File Path	Path of the service log file.
Port	Port number used for sending log collection data. Value range is 1~65535.

Step 4 Configure the file directory. Parameter description as shown in Table 10-23.

LAS allows monitoring operations such as adding, modifying, and deleting files in a specified directory.

Table 10-23 File Directory Parameters

Parameter	Description
Encrypted Transmission	Whether an encrypted transmission strategy is used during data transmission.
File Path	Path information for monitored files. Multiple paths are allowed, separated by line breaks.

Step 5 Configure the registry. For parameter descriptions, see Table 10-24.

Table 10-24 Registry Parameters

Parameter	Description
Encrypted Transmission	Whether an encrypted transmission strategy is used during data transmission.
Registry Review	Disabled by default. If it is enabled, the registry method is required. Options include: **Global** or **Customize**. When **Customize** is selected, the registry monitoring path is required.

Step 6 Configure the host audit parameters. For parameter descriptions, see Table 10-25.

Table 10-25 Host Audit Parameters

Parameter	Description
Encrypted Transmission	Whether an encrypted transmission strategy is used during data transmission.
Configuration Item	Select audit items for each host. Available options include **Mobile Storage Audit**, **Hardware Change Audit**, **Software Change Audit**, **Account Change Audit**,

Parameter	Description
	Password Change Audit, **User Login Audit**, **Process Creation Audit**, **Network Connection Audit**, and **User Permission Audit**. Multiple selection is allowed.

Step 7 Click **Confirm** to save the configuration.

----End

Associating Agents with Logs

Through agent association, you can view log information by specifying agents.

In the agent list, click the icon in the **Operation** column, select **View Log** to go to the log retrieval page, which displays log information related to that agent. For subsequent operations, see Log .

Enabling/Disabling Agents

In the agent list, click the icon in the **Operation** column, select **Enable**/**Disable**.

Once disabled, **Offline** is displayed in the **Online** column. Offline agents cannot be disabled.

Upgrading Agents

Offline agents cannot be upgraded.

In the agent list, click the icon in the **Status** column to start agent version synchronization. If a new version is available, it updates automatically. After the update is complete, the status column displays **Up to Date**.

Force-Updating Agents

Offline agents cannot be force-updated.

In the agent list, click the icon in the **Status** column or select **Force Update** in the **Operation** column. The **Status** column displays real-time update progress, as shown in Table 10-26.

Table 10-26 Agent Update Status

Updating Status	Description
Checking	Indicates that the system is checking whether the agent has an updated version.
Updating	Indicates that the agent is being upgraded with the update progress displayed.
Update Failed	Indicates that this update failed.
Updated	Indicates the agent has been updated to the latest version.

Uninstalling Agents

Offline agents cannot be uninstalled.

Uninstalling Online Agents

In the agent list, click the ☰ icon in the **Operation** column, select **Uninstall**; after uninstallation completes, the status column displays **Uninstalled**.

Caution	• After the agent is uninstalled, it cannot be recovered. • The operations for uninstalling online agent on Windows/Linux systems is similar.

Uninstalling Offline Agents

Uninstalling offline agent on Windows and Linux differs.

To uninstall offline agents on Windows, follow the steps below:

Step 1 Contact NSFOCUS technical support to obtain the offline uninstallation package.

Step 2 Launch **cmd.exe** with administrator privileges.

Step 3 Enter the following command in the command prompt and press **Enter**.

```
rundll32.exe c:\windows\system32\servicename.dll,u[uninstallpassword]
```

For example: if the service name is **nsfagent**, enter **rundll32.exe c:\windows\system32\nsfagent.dll,u5ba010200b3dd72b7ca33c9102eccd38** in CLI.

Step 4 After uninstallation is complete, the **Status** column for the corresponding agent in the agent list displays **Uninstalled**.

----End

To uninstall offline agents on Linux, follow the steps below:

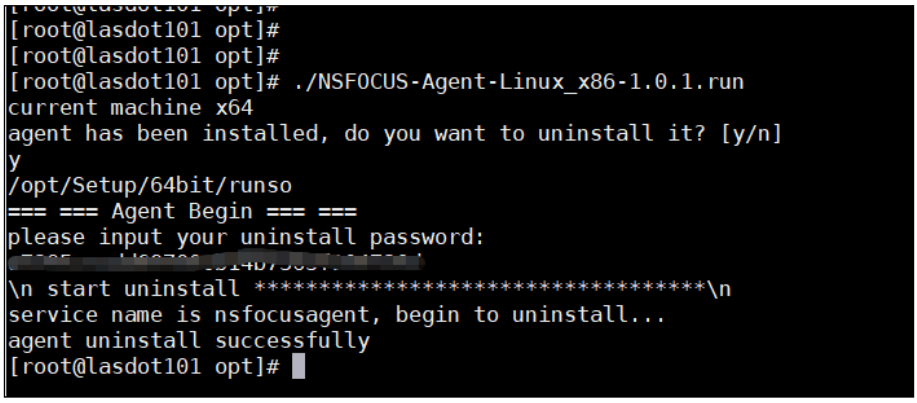
Step 1 Log in to the Linux host.

Step 2 Uninstall the agent, as shown in Figure 10-45.

a. Execute the **./NSFOCUS-Agent-Linux_x86-1.0.1.run** command to locate the agent installation package.

b. Enter **Y** as prompted, enter the uninstallation password, and select to uninstall the agent.

Figure 10-45 Execute Uninstallation



----End

Deleting Agents

In the agent list, click the ☰ icon in the **Operation** column, and select **Delete**.

Caution	• After an online agent is deleted, refreshing the agent list will display it again. • Only offline agents can be permanently deleted.

10.2 Data Management

Data management includes backup restore, threshold management, syslog forwarding, data migration, storage expansion, high availability, and archive restore.

10.2.1 Backup Restore

LAS supports log/file backup restore.

Log Backup

Hover over the ⚙ icon and choose **Data Management** > **Backup Restore** > **Log** to view backup and restore history records. Both manual backup and auto backup are displayed.

For both manual and auto backup, LAS uploads log files to the specified SFTP/FTP server. For details, see Configuring SFTP Server.

Manual Backup

In the **Manual Backup** area, configure manual log backup parameters and click **Start Backup**. Manual log backup parameter descriptions are shown in Table 10-27.

Table 10-27 Manual Backup Parameters

Parameter	Description
Time Duration	Select the time frame of logs to be backed up.
Log Type	Select the type of logs to be backed up. Multiple selection is allowed.
SFTP/FTP Server	Select the destination SFTP or FTP server for backup logs. Note The NIC of either the LAS device or the destination SFTP server must have an MTU (Maximum Transmission Unit) of 1500 bytes

Auto Backup

In the **Auto Backup** area, configure the log backup parameters, and click **Confirm**. The parameters are described in Table 10-28.

Table 10-28 Auto Backup Log Parameters

Parameter	Description
Time Duration	Select the backup frequency (options include: **Daily**, **Weekly**, and **Monthly**) and set the corresponding backup time.
Log Type	Select the type of logs to be backed up. Multiple selection is allowed.
SFTP/FTP Server	Select the destination SFTP or FTP server for backup logs. Note The NIC of either the LAS device or the destination SFTP/FTP server must have an MTU (Maximum Transmission Unit) of 1500 bytes.
Enable Auto Backup	Whether to enable auto backup for logs.

Log Restore

Hover over the icon, choose **Data Management > Backup Restore > Log > Log Restore**, and choose the destination SFTP/FTP server. After the connection status displays as normal:

- In the pending restore list, click **Restore** in the **Operation** column to start restoring the corresponding log packages. Multiple selection is allowed.
- Or click **Get Real-time Data**, select a log package in the preceding check box, set a password, and then click **Confirm** to directly restore the log package.

The restore results of the log package are displayed in the backup restore history list.

File Backup

Hover over the icon, choose **Data Management > Backup Restore > File**. In the **File Backup** area, choose the backup objects, click **Start Backup**.

When backing up a log source, go to the Asset Management module and synchronize the backup log source assets (that is, perform asset export and asset import), which is used to provide monitoring data for Monitoring Collected Asset.

File Restore

Executing the file restore operations will overwrite the current system configurations.

- To restore log sources: first go to the asset management module to import log source asset data; after finishing data restore, go to the data collection module to enable data sources. For details, see Importing Asset.
- If restoring event rules, after finishing data restore, you need to enable the event rules. For details, see Enabling/Disabling Event Rules.

Hover over the icon, choose **Data Management > Backup Restore > File**; in the **File Restore** area, choose **Select File (*.dat)** to select the configuration file downloaded via File Backup from the local system to restore.

Note	If the imported configuration file contains data sources or event rules, you need to manually re-enable them for the configuration to take effect. For details, see More Operations.

10.2.2 Threshold Management

Threshold management allows you to configure system disk overload policies, including disk usage rate and data retention days.

Hover over the icon, choose **Data Management** > **Threshold Management**, configure policy parameters, and click **Apply**. The description of parameters is shown in Table 10-29.

Table 10-29 Threshold Management Parameters

Parameter		Description
Over-limit Deletion (Access Log)	Disk Usage Limit	When the system disk usage rate reaches the limit, the oldest log data will be deleted. Value range is 50%~90%, defaulting to 90%.
Overdue Deletion (Access Log)	Auto-delete	Disabled by default.
	Retention Period	After enabling, when the log storage time exceeds the value, the system automatically deletes the logs that exceed the specified number of days. Value range is 180~1000 days, defaulting to 180.
Overdue Deletion	Auto-delete	Disabled by default.

Parameter		Description
(Audit Log)	Retention Period	After enabling, when the audit log storage time exceeds the value, the system automatically deletes audit logs that exceed the specified number of days. Value range is 180~1000 days, defaulting to 180 days.

10.2.3 Syslog Forwarding

LAS supports sending events, messages, and specified log types in Syslog format to a specified port on a designated server according to predefined forwarding rules (up to 3 rules).

Hover over the icon, choose **Data Management > Syslog Forwarding**, select **Add Configuration**, and configure the forwarding rule parameters. The parameters are as shown in Table 10-30.

Table 10-30 Syslog Forwarding Rule Parameters

Parameter	Description
Target IP Address	The IP address of the server storing Syslog.
Target Port	The server port for receiving Syslog from LAS.
Sending Port	The port for sending Syslog. If not configured, the system automatically selects a port.
Forwarding Type	Select the data content to forward. Available options are **Event**, **Message**, and **Log**. When **Log** is selected, you need to configure the forwarding log type.
Data Format	Select the data format. Available options are **Key->Value** and **JSON**.
Log Type	When **Log** is selected as the forwarding type, select the log types to be forwarded.
Compact Mode	When **Log** is selected as the forwarding type, enable the compact mode as needed. • **Disabled** (default): outbound logs include the original text and all parsed fields. • **Enabled**: outbound logs include only the original text (raw_data) and the device IP (dev_ip).

10.2.4 Storage Expansion

LAS supports NFS (Network File System) and S3 (Simple Storage Service) to expand log storage when storage space is insufficient.

- NFS is a network file system used for sharing files across a network, suitable for scenarios that require expanded storage space. The specified server must have the NFS service installed and must have granted access permissions to LAS.
- S3 is an object storage service suitable for scenarios requiring highly scalable, highly available, and secure storage solutions. It provides a cost-effective and easy-to-use Cloud storage solution.

Hover over the icon, choose the **Data Management** > **Storage Expansion**, select **NFS/S3 Service** and configure parameters; click **Save** to enable the NFS/S3 service.

The descriptions of NFS and S3 service parameters are shown in Table 10-31 and Table 10-32 respectively.

Note	• NFS and S3 services cannot be enabled at the same time. • NFS does not support IPv6. • NFS is not supported in cluster deployment and VM LAS.

Table 10-31 NFS Service Parameters

Parameter	Description
Server IP Address	IP address of the NFS server.
Storage Path	The storage path used for log storage.

Table 10-32 S3 Service Parameters

Parameter	Description
Access Key ID	Enter the credentials used for authentication and authorization when connecting to the S3 service.
Secret Access Key	Works with access key ID together as credentials for AWS accounts.
Region Name	Specifies the geographic location of the S3 bucket, which affects data access performance, availability, fault tolerance, and compliance.
Service Address	Server address where the S3 bucket is located, through which clients communicate and interact with the S3 service to enable functions such as data access, network configuration, and secure transmission.
Bucket Name	Unique identifier of the S3 bucket, used for identification in data storage and organization, access control, and uniqueness constraints.
State	Whether to perform data transferring.

NFS Configuration Preparation

Before configuring the NFS server, ensure that the NFS service is installed on the server and permissions have been granted to LAS. The detailed steps are as follows:

Step 1 Create a new shared storage directory, and ensure it has read/write permissions (**chmod go+w**).

Step 2 Configure client permissions as **rw,sync,no_root_squash** in the **/etc/exports** file.

Format: mount path client IP (permission)

Example: /data 10.65.1.1 (rw,sync,no_root_squash)

Step 3 Reload the NFS configuration and execute the **exportfs -rv** command.

----End

Local Disk Expansion

This function is only available for VM LAS.

You can expand the system space capacity by mounting one disk at one time. Multiple disks can be loaded through multiple operations.

The procedure for mounting disks is as follows:

Step 1 Hover over the icon and choose **Data Management** > **Storage Expansion > Local Disk Expansion**. LAS automatically detects if there are any mountable disks. When mountable disks are detected, disk information will be displayed.

Step 2 Choose **Mount Disk > Confirm**.

Step 3 Hover over the icon, choose **Components** > **System Services**, and restart the storage service to make the mounted disk take effect.

Step 4 (Optional) Unmount the existing disks.

a. Click **Unmount Disk** under the mounted disk, then confirm to unmount the corresponding disk.

b. After the disk is unmounted, choose **Components** > **System Services** and restart the storage service to make the disk unmount take effect.

----End

10.2.5 Data Migration

This function is not available for VM LAS or when LAS is deployed in cluster mode.

One-click data migration allows a configured backup machine to receive and synchronize pending backup data from the working machine when the working machine becomes unavailable due to hard disk drive failure or other issues.

The procedure for how to configure data migration is as follows.

Step 1 Hover over the icon, then choose **Data Management > Data Migration**.

Step 2 Click **Working Machine** to configure the parameters as shown in Table 10-33.

Table 10-33 Working Machine Data Migration Parameters

Parameter	Description
Data for Backup	Select the data types for data migration when a fault occurs. Available options include **Log Data**, **Event Alert**, **Report Management**, **Data Collection** (mandatory), and **Asset Management**. Multiple selection is allowed.
Backup Machine IP Address	Enter the backup machine IP address. It supports both IPv4 and IPv6.

Step 3 Configure the backup machine.

a. Log in to the web-based manager of the backup machine.

b. Hover over the icon, and choose **Data Management > Data Migration**.

c. Select **Backup Machine**.

d. Click **Confirm**.

Note	After the data migration starts, all previous data on the backup machine will be cleared.

----End

10.2.6 High Availability

LAS supports high availability. When the primary node is performing log collection, storage, and parsing operations, the secondary node simultaneously performs data synchronization and monitors the primary node's working status in real time. When the primary node fails, the secondary node takes over all operations of the primary node. This effectively reduces log data loss caused by system incidents and maintains the high availability of LAS.

The procedure of configuring high availability for LAS is as follows:

Step 1 Log in to the secondary node to obtain the verification code.

a. Hover over the icon, then choose **Data Management** > **High Availability**.

b. Click **Secondary** to set the current node as the secondary node.

c. Click **Get Verification Code**, and the page displays the verification code; click the icon to copy the verification code.

Step 2 Log in to the primary node for configurations.

a. Hover over the icon, then choose **Data Management** > **High Availability**.

b. Click **Primary** to set the current node as the primary node.

c. Configure parameters as shown in Table 10-34.

Table 10-34 Primary Node Parameters

Parameter	Description
Verification Code	Enter the verification code obtained in step 1.
Secondary Node IP Address	Enter the IP address of the secondary server.
Virtual IP	Enter the virtual IP address used by all nodes. Note After configuring high availability, all data must be sent to the virtual IP instead of the host IP; otherwise, after a switchover, the new primary server will not receive data.

d. Click **Test** to verify the connectivity between all nodes.

e. Click **Confirm** to finish configuration.

Tip	After the node is successfully configured, its system can be accessed normally.

Step 3 Log in to the secondary LAS for configuration.

a. Hover over the icon, then choose **Data Management** > **High Availability**.

b. Click **Secondary** to set the current host as the secondary node.

c. Configure parameters as shown in Table 10-35.

Table 10-35 Secondary Node Parameters

Parameter	Description
Primary IP Address	Enter the IP address of the primary node.
Virtual IP	Enter the virtual IP address shared by the primary node and secondary node. It must be consistent with that of the primary node configuration.

d. Click **Test** to test the connectivity among all nodes.

e. Click **Confirm** to finish configuration.

Tip	After the secondary node is successfully configured, its system will exit and become inaccessible.

----End

10.2.7 Archive Restore

When the local storage space of LAS is insufficient and reaches the configured threshold conditions (see Threshold Management), it triggers the remote storage server to perform log archiving. After log archiving is complete, the corresponding log data on LAS will be deleted.

Hover over the icon, choose **Data Management** > **Archive Restore** to view the log archive records performed by the remote storage server. Querying by log date and type is allowed.

In the archive list, select an archive record and click **Restore** in the **Operation** column to download the archived log data from the remote storage server to your local storage. You can select up to 100 successfully archived records at one time for batch restore.

During the restore process, if the page prompts about insufficient disk capacity or excessive usage in the currently selected disk, you must first clean up the local disk of LAS, and then resume the restore.

10.3 System Components

System components include system services and port rules.

10.3.1 System Services

Hover over the  icon to choose **Components** > **System Services**, you can restart/shut down the system, view the status of the current node and other operations, and manage backend service processes of the node. The bottom of the page displays the serial number of the current device and contact information for the vendor.

Restarting System

Click **Restart System** to restart the current node, including the data ingestion service, advanced engine, and basic services within the node. Restarting the system will cause the system to be temporarily unavailable.

Shutting Down System

Click **Shut Down System** to shut down the current node, including the data ingestion service, advanced engine, and basic services within the node. Shutting down the system will make the system unavailable.

Viewing Service Details

Click + on the right of the current node name to view all the statistics of backend services, including data ingestion service, data storage service, advanced engine, and basic services. Click the  icon to restart services.

10.3.2 Port Rules

Hover over the  icon and choose **Components** > **Port Rules** to view the network firewall configuration policies for LAS ports, including inbound rules and outbound rules. When you hover over the icon in the **Port Status** column, the current status of the corresponding port is displayed; for non-system ports, you can click the icon to enable or disable the corresponding port.

10.4 Cluster Management

10.4.1 Adding Nodes

By default, each LAS node can function as a standalone node. For cluster deployment, you can add more nodes.

This section only covers the configuration of adding nodes in the web-based manager of LAS. For deployment of nodes, please refer to the *NSFOCUS Log Audit System installation and deployment guide*.

The procedure of adding a node is as follows:

Step 1 Hover over the icon and choose **Cluster** > **Cluster Overview**. By default, there are no nodes.

Step 2 Click **Add Node** in the **Cluster Overview** page, or select the **Cluster Management** tab.

Step 3 In the **Cluster Management** tab, click **Add Node** to configure the node IP and security code.

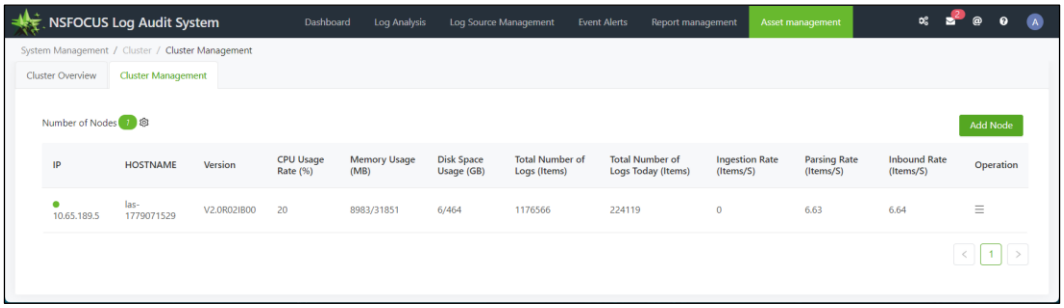
Obtain the security code from the node. For details, refer to the *NSFOCUS Log Audit System installation and deployment guide*.

Caution	• All nodes must be of the same version type: either hardware or virtualized LAS. • The major version (i.e., F version) of the nodes must be identical.

Step 4 Click **OK**.

After successfully adding the node, the **Cluster Management** tab page is shown in Figure 10-46.

Figure 10-46 Successfully Added a Node

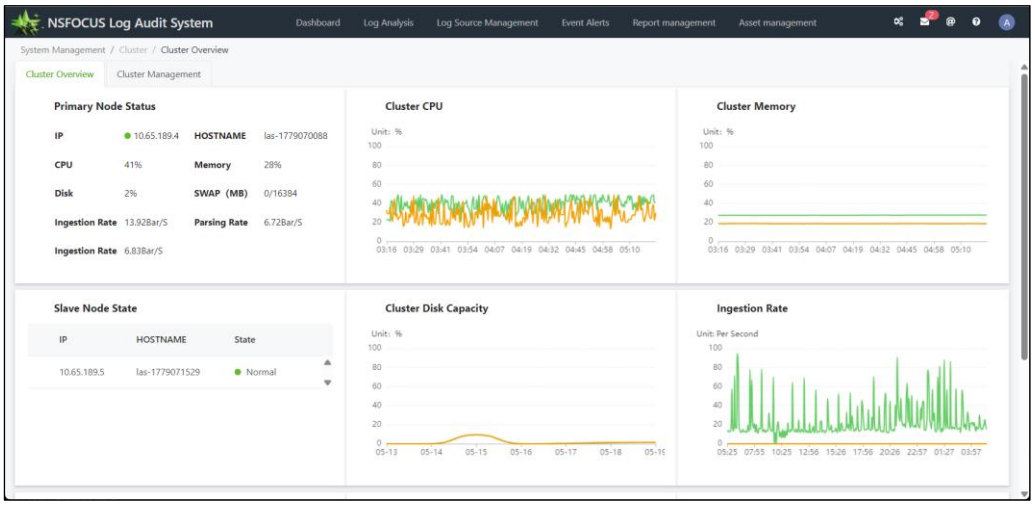


----End

10.4.2 Cluster Overview

After adding a node, hover over the icon and choose **Cluster Management** > **Cluster Overview** to view node status, service status, CPU trend chart, disk capacity trend chart, parsing rate trend chart, memory trend chart, ingestion rate trend chart, and last 7 days log count trend chart, as shown in Figure 10-47.

Figure 10-47 Cluster Overview



10.4.3 Cluster Management

Hover over the icon and choose **Cluster** > **Cluster Management** to add nodes and perform management operations, as shown in Figure 10-46.

Caution	If a node is offline, you can only view the node details but cannot delete or restart it.

Adding Node

For details, see Adding Node.

Viewing Node Details

In the node list shown in Figure 10-46, select **View Node Details** the **Operation** column to view detailed information of the corresponding node, including node basic information, node service information, and real-time status of system resources.

Restarting Node

In the node list shown in Figure 10-46, select **Restart Node** in the **Operation** column to restart the corresponding node.

10.5 System Configuration

System configuration includes basic configurations related to operations and management.

10.5.1 Theme Configuration

Through theme configuration, you can configure the system style, title, and text. You can also import theme packages to configure corresponding parameters.

Configuring System Display Name

System display name refers to the text displayed at the upper-left corner of the web-based manager of LAS.

Hover over the icon, choose **Configuration** > **Theme Configuration** > **System Display Name**, configure the system name, and click **Save**.

Configuring System Style

Hover over the icon and choose **Configuration > Theme Configuration > System Style Configuration** to configure or restore system styles. Parameter description is shown in Table 10-36.

- Click **Save** at the bottom of the page to make the system style changes take effect.
- Click **Restore** to restore the system style configuration to its default status.

Table 10-36 System Style Parameters

Parameter	Description
System Theme Color	Color of the system's theme and banner. Click the color block corresponding to "Theme color" or "Banner color", and customize the RGB values.
System Logo	• Click **Download Sample File** to download the corresponding default logo to your local machine. • Click **Replace** to customize the logo; click **Restore** to restore the default logo. Refer to the instructions in the web interface for supported image formats, size limits, and recommended dimensions for each logo type.
Login Background Image	• Click **Download Sample File** to download the default background image to the local machine. • Click **Replace** to change the background image; click **Restore** to restore the default background image. Refer to the instructions in the web interface for supported image formats, size limits, and recommended dimensions of the background image.

10.5.2 Network Configuration

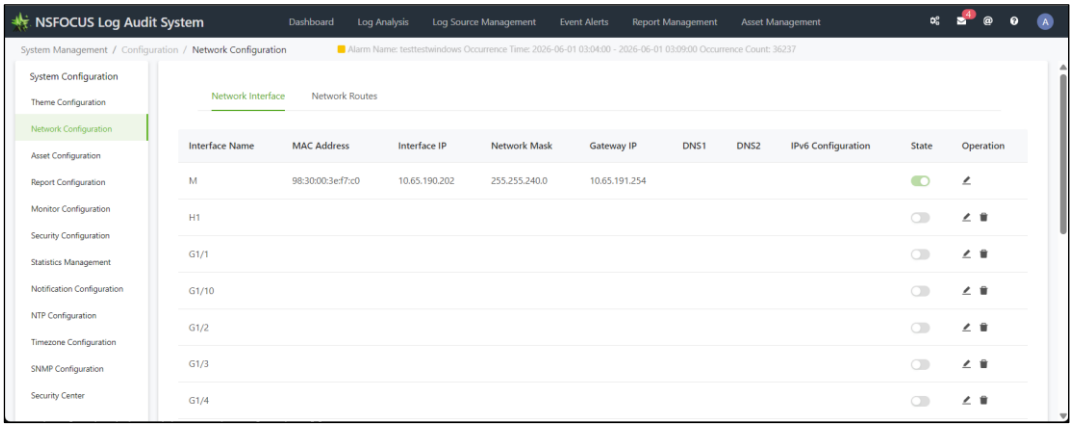
Only the system administrator has permission to configure network interfaces and network routes.

Configuring Network Interfaces

Hover over the icon and choose **Configuration** > **Network Configuration** > **Network Interface**, which lists the LAS management interface and other service interfaces, as shown

in Figure 10-48. Note that the H1 interface is configured as a service interface by default, but can be set as a management interface via Network Configuration.

Figure 10-48 Network Interface Configuration (Hardware Version)



Caution	The supported network interfaces depend on the device type. Some devices do not support the **H** interface.

Click the icon in the **Operation** column of the network interface list to edit the corresponding interface properties (supports IPv4 and IPv6) as shown in Table 10-37.

Table 10-37 Interface Attribute Parameters

Parameter		Description
Interface Name		Displays the current interface name. Modification is not allowed.
IPv4 Configuration	Interface IP	Enter the IPv4 address of the interface.
	Network Mask	Enter the network mask of the interface.
	Gateway IP	Enter the IPv4 gateway to enable network access to this interface.
	DNS1/DNS2	Enter the IP address of DNS servers. It supports both IPv4 and IPv6.
	MTU	Enter the maximum size (unit: bytes) of data packets transmitted during Syslog forwarding. Valid values are integers from 1500 to 9000. Note Modifying the MTU may result in unavailable functions of system configuration.
IPv6 Configuration	Interface IP	Enter the IPv6 address of the interface.
	IPv6 Prefix	Enter the prefix length of the IPv6 address. Valid values are integers from 0 to 128.
	IPv6	Enter the IPv6 gateway address for network access to this interface.

Parameter		Description
	Gateway IP	

Note	Modifying the IP of the management interface triggers the IP change immediately. You need to wait approximately for 5 minutes before you can log in to LAS using the new IP. When configuring interfaces other than the management interface, note the following: • Modifying the IP of management interface on the web page does not require system restart. • Modifying the IP of management interface on the console requires system restart.

Configuring Network Routes

You can configure static network routes for gateway addresses and interfaces.

Hover over the icon and choose **Configuration** > **Network Configuration** > **Network Route**. In the initial state, there is only a default route. Click **New Route** to configure static route parameters. For parameter descriptions, see Table 10-38.

Table 10-38 Network Route Parameters

Parameter	Description
Route Name	Enter the name of the static route. Value range: 1~20 characters. Special characters, such as \/ :* ?<>|=@#$%^&;()'[] and spaces, are not allowed.
Destination IP Address	The IP address of the destination host or destination network segment to which packets are delivered. It supports both IPv4 and IPv6.
Subnet/Prefix (IPv6)	• If the destination IP address is IPv4, fill in the netmask of the destination host or destination network segment to which the packet is delivered. • If the destination IP address is IPv6, enter the IPv6 prefix of the destination host or destination network segment to which the packet is delivered. IPv6 prefix is an integer ranging from 0 to 128.
Metric	Enter the metric value for the static route. The valid range is integers from 1 to 9999. The lower the metric value, the higher the priority. Routes with smaller metric values are used to forward data packets.
Route Type	• **Gateway:** enter the gateway address for the static route, typically the entry IP address of the next-hop device. It supports IPv4 and IPv6. • **Interface:** select the outbound interface for forwarding packets.

10.5.3 Asset Configuration

Through asset configuration, you can manage asset attributes and tags.

Adding Attributes

In addition to the basic information of assets, you can customize asset attributes for grouping and managing assets.

By default, LAS provides four asset attributes: asset groups, geographic locations, business systems, and organizational structures.

Hover over the icon and choose **Configuration > Asset Configuration > Attribute Management**. To create a new asset attribute, click **New Attribute**. For descriptions of asset attribute parameters, see Table 10-39.

Note	• System built-in attributes cannot be deleted. • Asset attributes of the "Text" type cannot be edited. • LAS allows you to maintain up to 15 asset attributes (including system built-in attributes), and management attributes cannot exceed 10.

Table 10-39 Asset Attribute Parameters

Parameter	Description
Attribute Name	Enter the attribute name. Up to 15 characters are allowed. It cannot contain special characters other than #-_.():\/+&@.
Attribute Value Type	• **Text:** displays as a text box in the page. • **Tree:** displays as a list in the page. - The depth of the tree hierarchy is up to 6. - Add child node: select the first-level node, click **Add Child Node**, configure the attribute values in the pop-up dialog, and click **Create**.
Attribute Type	When the attribute value type is **Text**, set the following categories of attribute values: • **Integer:** indicates positive integer, 0, or negative integer. • **Character:** includes characters, numeric characters, and other ASCII characters, with a value range of 0~254 characters. • **Boolean:** either true or false. • **Floating Point:** a number with a decimal part.
Set as Management Attribute	When the attribute value type is **Tree**, this parameter is required, which will only be displayed in the asset management page.

Managing Tags

Asset tags are used to quickly identify assets when editing asset information.

Hover over the icon and choose **Configuration > Asset Configuration > Tag Management**. By default, the system displays built-in asset tags.

Note	• In the Tag Management page, creating asset tags is not allowed. Tags can only be added when creating an asset. For details, see Creating Asset. • System built-in tags cannot be deleted.

10.5.4 Report Configuration

Hover over the icon, choose **System Configuration** > **Report Configuration**, configure the report template parameters, and click **Save**. Parameter description is shown in Table 10-40.

Table 10-40 Report Logo Parameters

Parameter	Description
Configuration Method	• **Default**: use the system built-in logo in reports. • **Customize**: upload custom images.
Logo	When the configuration method is **Customize**, click **Upload Logo**. Only JPG, PNG, and BMP files are supported. Recommended size is 171x98 pixels.

10.5.5 Monitoring Configuration

Hover over the icon, choose the **Configuration** > **Monitor Configuration**, and configure system asset monitoring parameters. Click **Save** respectively, and the corresponding alert settings take effect. LAS starts monitoring the CPU, memory, and disk usage of the current host.

When the system detects that CPU, memory, or disk reaches the threshold, a notification appears in the Message Center. For disk alerts, in addition to the notification in the Message Center, email notification is also generated. Parameters are described in Table 10-41.

Table 10-41 System Monitoring Parameters

Parameter	Description
CPU Alert Settings	If the current host's CPU utilization continuously exceeds the specified threshold within the specified duration, an alert is triggered through the Message Center. • **CPU Alert Threshold**: value range is 10%~95%. • **Duration**: valid range is 10~600 seconds.
Memory Alert Settings	If the current host's memory usage rate continuously exceeds the specified threshold within the specified duration, an alert is triggered through the Message Center. • **Memory Alert Threshold**: value range is 10%~95%. • **Duration**: valid range is 10~600 seconds.
Disk Alert Settings	If the disk space usage in the current host is greater than or equal to the threshold, an alert is triggered through the Message Center and an email will be sent to the admin account. Valid range:10%~95%.

10.5.6 Security Configuration

Security configuration includes login configuration and password reset.

Login Configuration

Login configuration includes managing login failures, password policies, and system automatic logout time of the web-based manager.

Hover over the icon, and choose **Configuration** > **Security Configuration** > **Login Configuration** to configure login parameters as shown in Table 10-42.

Table 10-42 Login Configuration

Parameter		Description
Login Failure Configuration	Max Retries	If the number of failed login attempts for an account exceeds the value, the account will be locked. Valid range: 3~10.
	Lockout Duration	Duration for account lockout. Unit: minutes.
Password Policy Configuration	Password Length	Length range of user password for login. Valid range: 6~20 characters.
	Password Strength	User password strength for login. Available options are level 2, level 3, and level 4; the page displays the corresponding password strength requirements.
	Password Change Cycle	Validity period for user passwords. When it exceeds the value, the system forces a password change. Valid range: 1~90 days.
	Password Expiration Reminder	Advance notification period for user password expiration. When the value is reached, the system sends a password update notification to the Message Center. Valid range is 1~7 days.
System Configuration	Auto-logout	When the system inactive duration reaches the value, it will automatically log out. Valid range: 1~60 minutes.

Resetting Console Password

If you forget the console password, you can reset it to the initial password.

Hover over the icon, choose **Configuration** > **Security Configuration** > **Console Management**, and click **Reset Password** to reset the console administrator's password. For details, see Initial User Account.

10.5.7 Statistics Management

Through statistical management, you can provide content and methods for data display for Report Management.

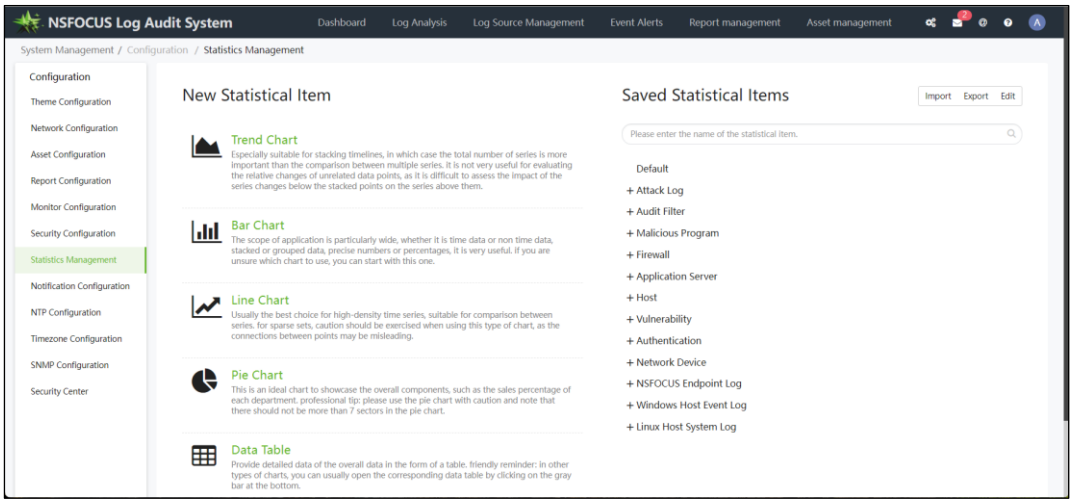
Creating Statistics Item

Each statistical item can have multiple forms, including trend charts, column charts, line charts, pie charts, and data tables. Additionally, LAS supports statistical item plugin functionality. For details, see Custom Statistics Plugin.

The following takes trend chart as an example to introduce the procedure for creating a new statistics item.

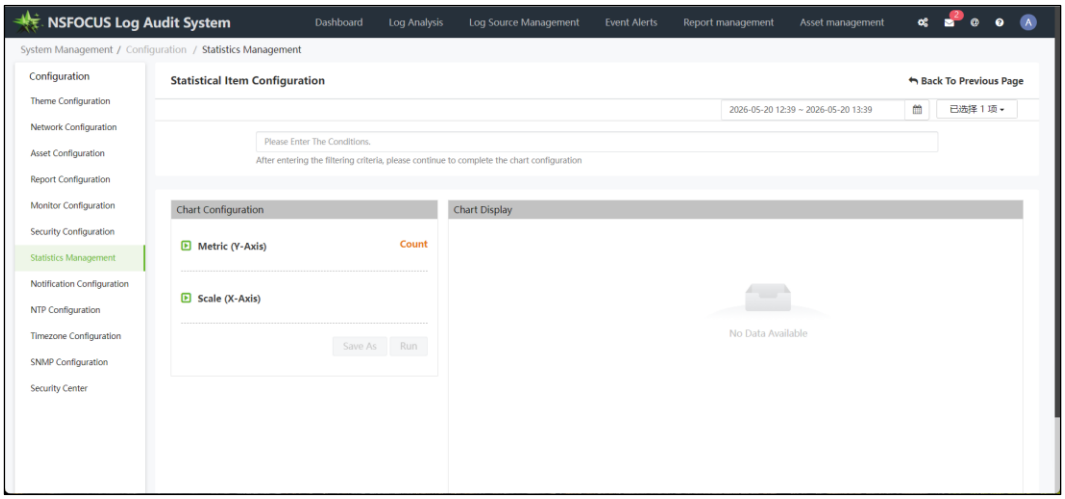
Step 1 Hover over the icon, and choose **Configuration** > **Statistics Management**. The left side of the page is the entry point for creating new statistical items, as shown in Figure 10-49.

Figure 10-49 Statistics Management



Step 2 Select **Trend Chart** on the left side of the page. The **Statistical Item Configuration** page is as shown in Figure 10-50.

Figure 10-50 Configuring Statistical Items of Trend Chart



Step 3 Select the time frame for log generation, and select the log type for the data to be counted.

Step 4 (Optional) Configure filter conditions to filter log fields for the data to be counted.

When certain fields of the logs to be viewed have specified values, you can perform this operation.

Step 5 Configure the metrics (Y-axis).

Click the icon to expand the Y-axis configuration items and configure relevant parameters.

Step 6 Configure the measurement scale (X-axis).

Click the icon to expand the X-axis configuration items and configure relevant parameters.

Step 7 (Optional) Click **Run** to preview the statistical chart.

Step 8 Click **Save as**, enter the name of the statistics item in the popup dialog, and select the group.

Step 9 Click **Save**. This statistic item will be displayed in the saved statistic items group as shown in Figure 10-49.

----End

Exporting Statistical Items

Navigate to the page shown in Figure 10-49, click **Export** on the right side of the page. The popup dialog provides two export methods:

- Expand the statistics items and make selections, click **Export Selected Items** to export the selected statistics items as a compressed package of JSON files.
- Click **Export All** to export all statistical items as a compressed package of JSON files.

Note	The exported statistical item file cannot be modified.

Importing Statistics Items

Navigate to the page shown in Figure 10-49. Click **Import** on the right side of the page. In the popup dialog, click **Select Plugin** or drag the statistical item file to the specified area, and then click **Import**.

Adding Statistics Item Group

LAS supports grouping saved statistical items for categorized management.

The procedure of adding a statistics item group is as follows:

Step 1 Navigate to the page shown in Figure 10-49, click **Edit** at the upper-right corner of the page.

Step 2 Add a statistical item group.

a. Click the icon in the group list.

b. Configure a unique group name (up to 30 characters and special characters are not allowed).

c. Click **Confirm**.

Step 3 (Optional) Add subgroups as needed.

a. In the group list, select a group.

b. Click the icon in the subgroup list to open the new group dialog box.

c. Configure a unique subgroup name (up to 30 characters and special characters are not allowed).

d. Click **Confirm**.

Step 4 Add statistics items.

Select a group/subgroup, then drag statistics items from the ungrouped area to that group.

Step 5 Click **Save**.

----End

Note	Built-in statistics items/statistics item groups cannot be deleted.

Saving as Statistics Item

When editing a statistical item, click **Save as** to re-edit the current statistical item and save it as a new statistical item.

Custom Statistics Plugin

Custom plugins only support .dat and .zip files.

Navigate to the page shown in Figure 10-49. Click **Custom Statistics Plugin** on the left side of the page. In the pop-up dialog, click **Select Plugin** or drag the plugin file to the designated area. After entering the name of the statistics plugin, click **Import**. The custom statistics plugin will be displayed.

10.5.8 Notification Configuration

Notification configuration includes email server configuration, SMS server configuration, and SFTP server configuration.

Configuring Mail Server

To enable email notifications in LAS, you must configure the relevant parameters for the SMTP server.

Hover over the icon, choose **Configuration** > **Notification Configuration** > **Mail Server**, and configure the SMTP server parameters. Parameter descriptions are shown in Table 10-43.

After configuring the SMTP server, click **Test** to configure verification parameters and verify whether the SMTP server configuration is correct. If the test mail is received normally, it indicates that the SMTP server configuration is correct. The SMTP server verification parameters are described in Table 10-44.

Table 10-43 SMTP Server Parameters

Parameter	Description
Server Address/Port	Enter the IP address or domain name and port of the SMTP server. Note • IP address supports IPv4 and IPv6. • Currently, three SMTP protocol authentication methods are supported: PLAIN, CRAM-MD5, and LOGIN. Make sure that the SMTP server to be configured uses one of these three authentication methods.
Email Address/Password	Enter the account/password for sending emails. You must enter a complete email address, for example: test@test.com. If **No password required** is selected, it indicates that sending emails can be performed without entering a password.
Login Verification	Whether to enable login verification.
SSL	Whether to enable SSL encryption. Note If the SMTP server does not support SSL encryption, select **No**; otherwise, emails cannot be sent.

Table 10-44 SMTP Server Verification Parameters

Parameter	Description
Recipient	The recipient email address for receiving test emails.
Title	The subject of the test mail.
Content	The body of the test mail.

Configuring SMS Server

To enable SMS notifications in LAS, you must configure the SMS server.

Hover over the icon, choose **Configuration** > **Notification Configuration** > **SMS Server**, select the device type, and configure the SMS server parameters. SMS device parameters are described in Table 10-45. For parameters about Jiaxun MAS and Tencent Cloud SMS platforms, see Table 10-46 and Table 10-47.

After configuring the SMS server, click **Test** and configure the verification parameters to verify whether the SMS server configuration is correct; if you can receive test SMS messages normally, it indicates that the SMS server configuration is correct.

Table 10-45 SMS Device Parameters

Parameter	Description
Device	The SMS server device used. Select **SMS**.
Username	The username for the SMS server. Up to 100 characters are allowed.
Password	The password for the username. Up to 100 characters are allowed.
Server Address	The IP address of the SMS server, supporting IPv4 and IPv6.
Database Name	The database name of the SMS server used for storing SMS notifications; it supports up to 100 characters.
Table Name	The table name for storing SMS notifications. It supports up to 100 characters.

Table 10-46 Jiaxun MAS SMS Platform Parameters

Parameter	Description
Device	Select **Jiaxun MAS SMS Platform**.
MAS Server IP Address	IP address of the MAS server. It supports IPv4 and IPv6.
API Listening Port	Port number on MAS for listening to clients. Value range: 1~65535.
API Identifier	Identifier of the API.
API Login Password	Login password of the API. Up to 100 characters are allowed.
SMS Extension Code	Extension code of the SMS. Up to 100 characters are allowed.
Maximum Messaging Times per Minute	Maximum frequency for sending SMS per minute. Value range: 1~20.
SMS Suffix	Suffix of the SMS. Up to 100 characters are allowed.

Table 10-47 Tencent Cloud SMS Platform Parameters

Parameter	Description
Device	Select **Tencent Cloud SMS Platform**.
API Secret Key ID	API key is an important credential for building API requests. Through the Tencent Cloud API, you can operate all tencent Cloud resources using the specified user account.
API Secret Key	
SMS Server URL	URL of API request, defaulting to **sms.tencentcloudapi.com**.
Tencent Cloud APP ID	The sdkappid generated after adding an application in SMS console.
Template and Signature	• **Function Module**: the name of functional modules where LAS needs to use SMS services. Currently, only event alerts use SMS services. • **Signature Content**: SMS signature content, using UTF-8 encoding. You must fill in an approved signature.

Parameter	Description
	• **SMS Template ID**: ID of an approved template. For sending SMS to overseas phone numbers, use international/Hong Kong, Macao, and Taiwan SMS templates. • **Template Content**: content of the SMS template.
More Configuration	• **SMS Code Extension Number**: SMS code extension, disabled by default. Please contact SMS helper if you need to enable it. • **Phone Number Prefix**: prefix for mobile phone numbers. For example: +86. • **Session Content**: content of the user session can carry context information such as user ID, and the server will return it as-is. • **Sender ID**: if you need to enable the sender ID for international/Hong Kong/Macau/Taiwan regions, contact SMS helper; SMS for Chinese Mainland doesn't require a sender ID.

Configuring SFTP Server

To upload files/data to an SFTP/FTP server for backup, you must configure the SFTP or FTP server in LAS.

Hover over the icon, choose **Configuration > Notification Configuration > SFTP Server**, click **New SFTP**, and configure the server parameters as shown in Table 10-48.

Table 10-48 SFTP/FTP Server Parameters

Parameter	Description
Connection Type	The protocol type used. Available options include **SFTP** and **FTP**.
Name	The name of the SFTP or FTP server. It supports up to 128 characters.
Host Address	The IP address of the SFTP or FTP server. It supports IPv4 and IPv6.
Service Port	The port number used for SFTP or FTP server communication.
Login Account/Password	Username/password for login to the SFTP or FTP server. The username supports up to 30 characters.
Upload Mode	The mode for data upload. Available options are **Passive Mode** and **Active Mode**.
Storage Path	The path for data backup to the SFTP or FTP server.
Remark	The description of the SFTP or FTP server. Up to 255 characters are allowed.

10.5.9 NTP Configuration

Hover over the icon, choose **Configuration** > **NTP Configuration**, and configure the time synchronization method for LAS. NTP parameter descriptions are shown in Table 10-49.

Table 10-49 NTP Parameters

Parameter	Description
Sync Mode	LAS supports the following synchronization modes: • **Periodic Sync**: LAS periodically synchronizes with the time server. • **Immediate Sync**: LAS immediately performs a one-time synchronization with the time server. • **Manual Calibration**: manually configure the time displayed in LAS.
Primary/Secondary NTP Server	The address of the NTP server. It supports IPv4, IPv6, and domain names. The parameter is only required when **Periodic Sync** or **Immediate Sync** is selected.
Calibration Time	Directly configure the system time displayed in LAS. The parameter is only required when **Manual Calibration** is selected.

10.5.10 Timezone Configuration

The system supports dynamic timezone switching to ensure time display conforms to the local time conventions. All business data is stored in UTC format. Switching timezones only affects the front-end display and does not affect underlying data or scheduled tasks.

Only administrators can configure the system timezone.

Hover over the icon, choose **Configuration** > **Timezone Configuration**, configure the time zone for LAS, and click **Save**.

10.5.11 SNMP Configuration

LAS supports SNMP (Simple Network Management Protocol) management and mainstream SNMP management tools, such as MIB Browser. LAS acts as an agent to respond to queries from SNMP management hosts and return corresponding status information to SNMP management hosts.

LAS supports SNMP v3. When querying LAS using SNMP v3, the transmitted information is not only encrypted using encryption algorithms (supporting DES and AES), but user keys must also be set for LAS to verify user identity.

Configuring SNMP

This section describes how to configure LAS to support SNMP management.

Hover over the icon, choose **System Configuration > SNMP Configuration**, and configure SNMP parameters. Parameter descriptions are shown in Table 10-50.

Table 10-50 SNMP System Parameters

Parameter	Description
System Location	The position of LAS in the network environment. Up to 30 characters are allowed.
Contact	Contact information for the system owner. Defaults to the email address of NSFOCUS technical support. You can enter a phone number or email address.
Description	Enter the description for LAS. Up to 250 characters are allowed.
SNMP Service	Whether to enable LAS to accept management from SNMP management hosts.
Security Level	After the SNMP service is enabled, configure the security level for SNMP v3 users to ensure access security. • **Without Authentication**: no authentication is required when an SNMP management host queries LAS. You only need to configure the MIB subtree and read/write permissions. • **Authentication Required**: when an SNMP management host queries LAS, authentication is required. You need to configure the MIB subtree, read/write permissions, username, authentication protocol, and authentication key. • **Authenticated and Encrypted**: when an SNMP management host queries LAS, authentication and encryption are required. You need to configure the MIB subtree, read/write permissions, username, authentication protocol, authentication key, encryption protocol, and encryption key.
MIB Subtree	Manage the host's access permissions to the management information base subtree in LAS. Access permissions are controlled through OID (Object Identifier). **1** indicates having access permissions for all nodes, for example: 1.3.6.1.4.1.19849.2.
Read/Write Permissions	Manage the read/write permissions of the management host for the management information base subtree in the LAS device. Available options are **rw** (read and write) and **r** (read).
Username	When the security level is **Authentication Required** or **Authenticated and Encrypted**, configure the SNMP v3 user name. Up to 30 characters are allowed.
Authentication Protocol	When the security level is set to **Authentication Required** or **Authenticated and Encrypted**, configure the authentication protocol used for authentication. Available options are **MD5** and **SHA**.
Authentication Key	When the security level is set to **Authentication Required** or **Authenticated and Encrypted**, configure the key used for authentication with a string of at least 8 characters. It is used by the authentication protocol for one-way hash calculation.
Encryption Protocol	When the security level is **Authenticated and Encrypted**, configure the encryption algorithm used for encrypted transmission. Available options are **DES** and **AES**.
Encryption Key	When the security level is **Authenticated and Encrypted**, configure the key used for information encryption. It must be a string of at least 8 characters.

Downloading MIB Library

In the **SNMP Configuration** page, click **Download MIB Library** to download the MIB library file to the local machine.

Viewing SNMP Configuration Guide

In the **SNMP Configuration** page, click **SNMP Configuration Guide** to browse the SNMP configuration file online, and you can also download it to the local machine.

10.5.12 Security Center

LAS supports integration with NSFOCUS devices and third-party devices.

NSFOCUS Devices

Hover over the icon, choose **Configuration > Security Center**, which by default displays the NSFOCUS devices tab.

- NSFOCUS Enterprise Security Center (ESPC)

  ESPC is a centralized management platform designed for NSFOCUS series products. It provides various management and monitoring functions including centralized system monitoring across multiple products, unified policy configuration, and comprehensive report management, significantly improving user efficiency in security management operations.

  After integrating with LAS, ESPC can centrally manage, authorize, and upgrade multiple LAS devices. Centralized authorization only supports VM LAS.

- NSFOCUS Intelligent Security Operation Platform (ISOP)

  After LAS enables the integrated log data synchronization with ISOP, it sends log data to a specified port on a specified platform via encrypted transmission. To improve data transmission efficiency, if the volume of a certain type of log data is large, configure a separate port for data transmission.

The parameters for configuring the connection between LAS and NSFOCUS devices are described in Table 10-51.

Table 10-51 LAS and NSFOCUS Device Connection Parameters

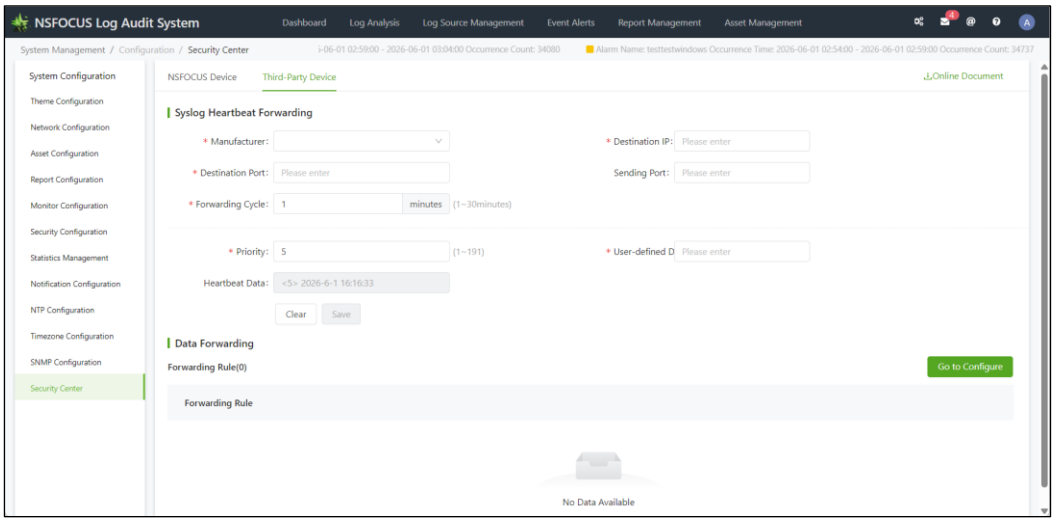
Parameter		Description
Enterprise Security Center (ESPC)	Server Address	Enter the IP address of the linked ESPC. Select **Enable** and click **Save** to start the connection between LAS and ESPC.
NSFOCUS Intelligent Security Operation Platform (ISOP)	Security Platform IP	The IP address of ISOP connected to LAS.
	Log Sync	After enabled, synchronize logs between LAS and ISOP. • **Log Type**: synchronizes all log types; modification is not allowed. • **Port**: enter the port number for ISOP to receive LAS logs. Defaults to **5010**.
	Event Sync	After enabled, synchronize security events in Event Analysis with ISOP. • **Event Type**: selected security event types will be sent to ISOP. Fuzzy search for event types is allowed. • **Port**: enter the port number for ISOP to receive security events from LAS. Defaults to **1**.
	Message Center Alert Sync	After enabled, send the real-time messages of Message Center to ISOP.

Parameter		Description
		• **Alert Type**: selected message types will be sent to ISOP. • **Port**: enter the port number for ISOP to receive messages from LAS. Defaults to **1**.

Third-Party Devices

Hover over the icon, and choose **Configuration** > **Security Center** > **Third-Party Device**, as shown in Figure 10-51.

Figure 10-51 Third-Party Device



- Syslog heartbeat outbound

  LAS sends heartbeat data to third-party devices in Syslog format. For details, click **Online Documentation** at the top of the page.

- Data forwarding

  Click **Go to Configure** to go to the Syslog Forwarding module, click **+ Add Configuration** to configure new forwarding rules, as shown in Figure 10-52.

  The parameters of data forwarding configuration are described in Table 10-52.

Figure 10-52 New Forwarding Configuration

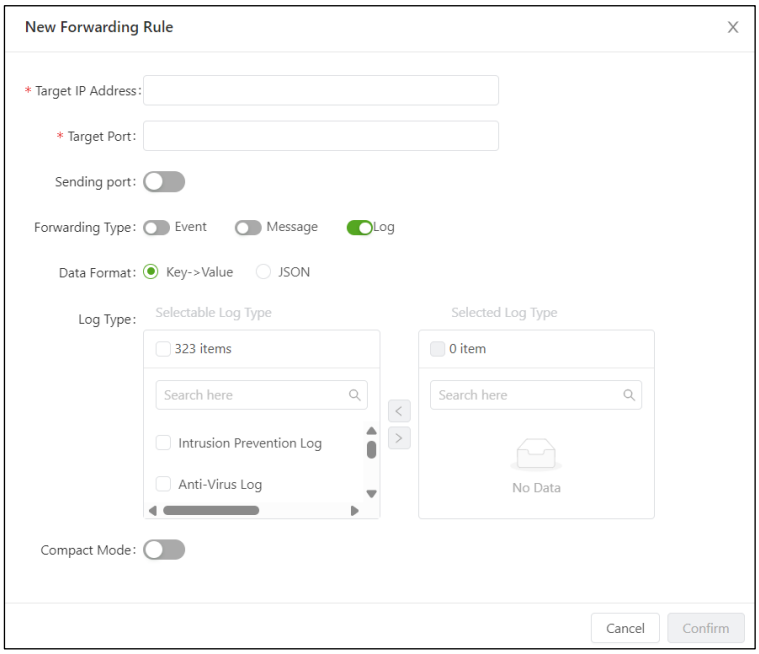


Table 10-52 LAS Data Forwarding Configuration Parameters

Parameter	Description
Target IP Address	IP address for receiving logs.
Target Port	Port for receiving logs.
Sending Port	Port for sending logs.
Forwarding Type	Content types for data forwarding. Options include **Event**, **Message**, and **Log**.
Data Format	Format for data forwarding. Options include **Key->Value** and **JSON**.
Log Type	When **Log** is selected in forwarding settings, you need to select the forwarding log type.

10.6 Troubleshooting

LAS supports four fault diagnosis methods: network diagnosis, remote assistance, network packet capture, and one-click inspection.

10.6.1 Network Diagnosis

Hover over the icon, choose **Fault Diagnosis > Network Diagnosis**, configure the network diagnosis parameters, and click **Diagnosis** to diagnose whether LAS is reachable to the target IP. The network diagnosis parameter descriptions are shown in Table 10-53.

Table 10-53 Network Diagnostic Parameters

Parameter	Description
Diagnostic Method	• **PING:** use PING to diagnose whether the target IP is reachable. • **TELNET**: use TELNET to diagnose whether the target IP is reachable. The target port is required.
IP Address	IP address of the connected target.

10.6.2 Remote Assistance

This function is intended only for NSFOCUS technical support during network diagnosis.

Hover over the icon and choose **Fault Diagnosis > Remote Assistance**. You can select to turn on or turn off the SSH service.

10.6.3 Packet Capture

The packet capture function captures packets passing through LAS to assist with troubleshooting.

The procedure for enabling packet capture is as follows:

Step 1 Hover over the icon and choose **Fault Diagnosis > Network Packet Capture**.

Step 2 Configure the parameters as shown in Table 10-54.

Table 10-54 Network Packet Capture Parameters

Parameter	Description
Interface	Select an interface to perform packet capture. **Any** means capturing packets on all logical interfaces.
Protocol	Select a protocol type for packet capture. **Any** indicates capturing packets of all protocols.
Source IP	Source IP address for packet capture. **0.0.0.0** indicates any IP.
Source Port	Source port for packet capture. **0** indicates any port.
Destination IP	Destination IP address for packet capture. **0.0.0.0** indicates any IP.
Destination Port	Destination port for packet capture. **0** indicates any port.
Duration (seconds)	The execution duration of the packet capture task. When the configured duration is reached, the packet capture task is stopped. Value range: 0~300 seconds; **0** is equivalent to 300.
Packet Count	The number of packets to capture. When the configured count is reached, the packet capture task is stopped. Value range: 0~1000; **0** is equivalent to 1000.

Step 3 Click **Start** to start packet capture.

The page displays captured data in real time. Click **View** to view the captured data.

During packet capture, you can click **Stop** to interrupt the packet capture.

Step 4 After the packet capture is successful, click **View** to display the most recently captured data packet.

Step 5 Click **Download** to download the most recently captured data packets to your local machine for analysis.

----End

10.6.4 One-click Inspection

One-click inspection checks the health and availability of LAS, including resources, processes, and key configurations.

Hover over the icon and choose **Fault Diagnosis** > **One-Click Inspection**. The page displays SSL certificate validity period information at the top. Select the inspection method, click **Start Inspection**. After the inspection is completed, the page displays the inspection result. The description of parameters is shown in Table 10-55.

Table 10-55 One-Click Inspection Method

Parameter	Description
All	Inspection scope covers all items for resource, process, and key configuration.
Resource Inspection	Inspects operating system, kernel version, product form, database type, database version, CPU usage, memory usage, SWAP usage, disk usage (including disk space used by secondary directories), and NIC information.
Process Inspection	Inspects the status and data backlog of log/event storage, Kafka service status, server / interface A status, status of services under supervisor, streamsets pipeline and status, and clickhouse service status.
Key Configuration Inspection	Inspects firewall rules, node configuration files, log/event storage configuration files, and kernel parameters.

10.7 License Management

When using the LAS hardware version or VM LAS for the first time, you must import correct certificates. For details, see First-time Login.

Note	The correct certificate file refers to: • The file extension is **.lic**. • The file must match the HASH value of LAS.

This section introduces certificate management methods during subsequent use.

10.7.1 Uploading Certificate

In the following situations, you can perform the operation of uploading and importing LAS certificates:

- When exceeding the certificate's validity period.
- During normal use of LAS.
- Switch authentication method (VM LAS only).

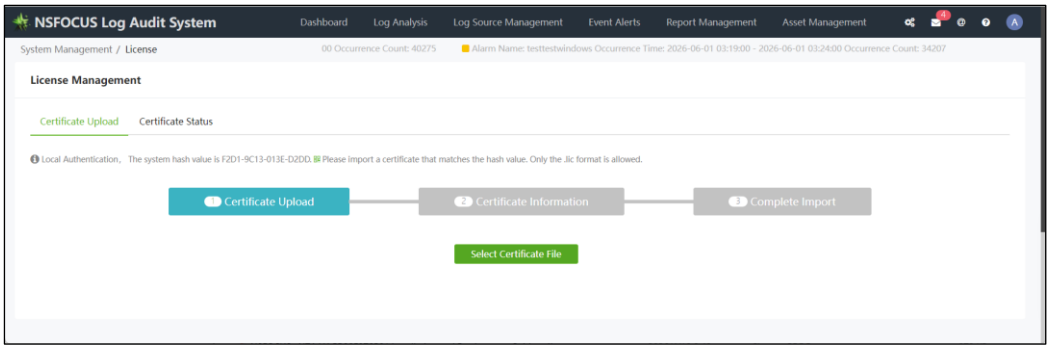
The certificate upload operations for the LAS hardware version and VM LAS are slightly different, as described separately below.

Uploading Certificate for Hardware Version

The procedure for importing certificates of LAS hardware version is as follows:

Step 1 Hover over the icon, choose **License > Certificate Upload**, as shown in Figure 10-53.

Figure 10-53 Certificate Upload (Hardware Version)



Step 2 Click **Select Certificate File** to select a local certificate file.

Step 3 Click **Confirm Import**.

After logging in to LAS again, hover over the icon, choose **License > Certificate Status**, and view certificate details. For details, see Certificate Status.

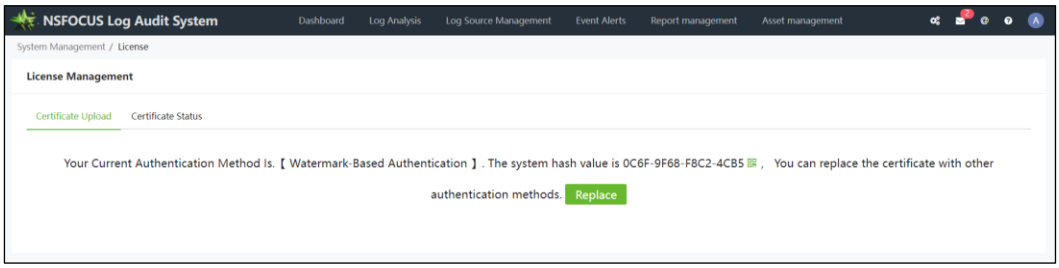
----End

Uploading Certificate for VM LAS

The operation method for importing VM LAS certificate is as follows:

Step 1 Hover over the icon, choose **License > Certificate Upload**, and confirm the current authentication method, as shown in Figure 10-54.

Figure 10-54 Authentication Method Confirmation (VM LAS)



Note	The default authentication method for VM LAS is watermark-based authentication.

Step 2 Click **Replace** to enter the certificate upload page, as shown in Figure 10-55.

Figure 10-55 Certificate Upload (VM LAS)

Step 3 Select an authentication method, click **Select Certificate File** to select a local certificate file.

Step 4 Click **Confirm Import**.

After logging in to LAS again, hover over the icon, choose **License > Certificate Status**, and view certificate details. For details, see Certificate Status.

----End

10.7.2 Switching Authentication Method

LAS supports switching to cloud authentication and watermark-based authentication methods.

Switching to Cloud Authentication Mode

To switch to Cloud authentication, follow these steps:

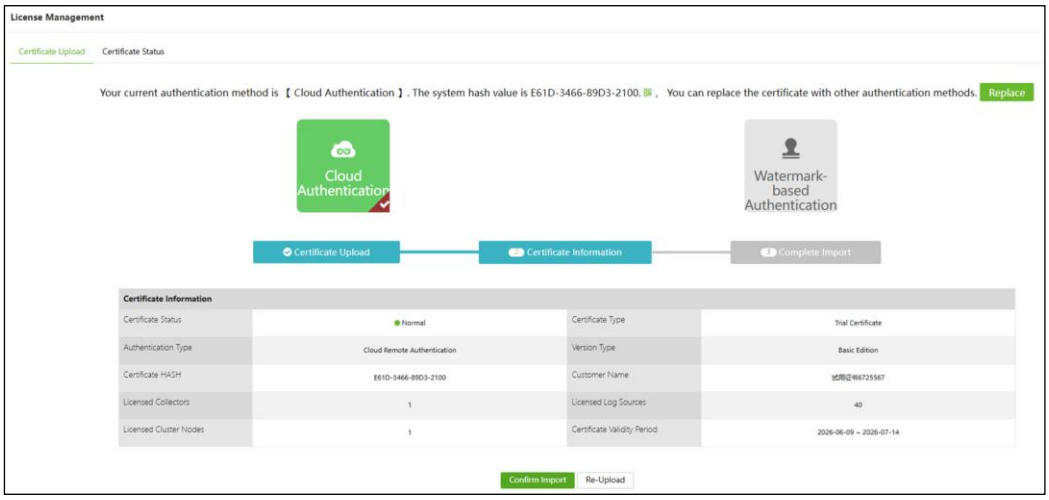
Step 1 Hover over the icon, choose **License > Certificate Upload**, and click **Replace** to change the authentication method.

Step 2 Select **Cloud Authentication**, as shown in Figure 10-56.

Figure 10-56 Uploading Certificate (Cloud Authentication)

Step 3 Click **Select Certificate File**, and select a local certificate file to go to the **Certificate Status** page, as shown in Figure 10-57.

Figure 10-57 Certificate Information (Cloud Authentication)



Step 4 Click **Confirm Import**. After successful activation, a prompt indicates that system-related services need to be restarted.

Step 5 Click **OK**. After the system logs out, log in again in 3~5 minutes to finish the authentication method switch.

----End

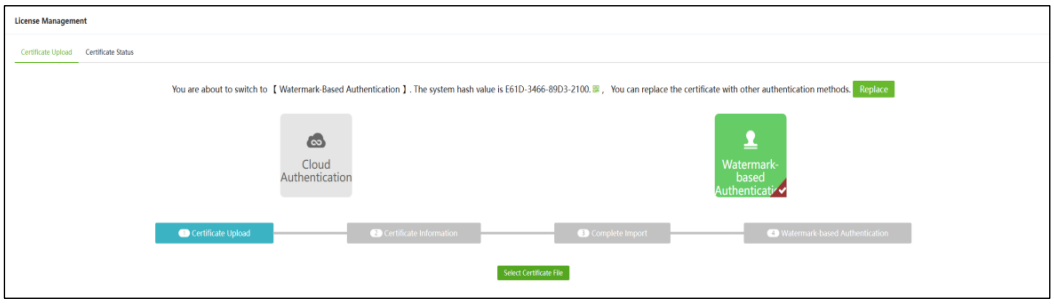
Switching to Watermark-based Authentication Mode

To switch to the watermark-based authentication method, follow the steps below:

Step 1 Hover over the icon, choose **License > Certificate Upload**, and click **Replace** to change the authorization method.

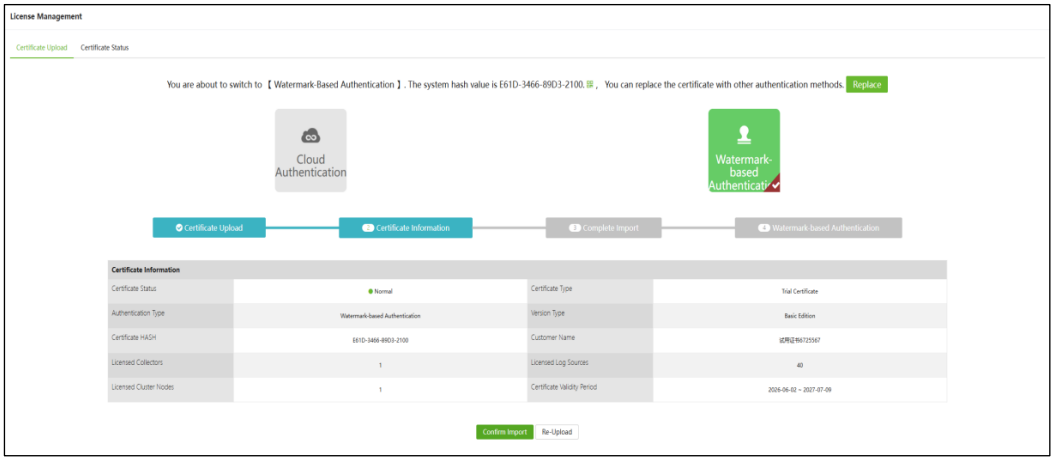
Step 2 Select **Watermark-based Authentication**, as shown in Figure 10-58.

Figure 10-58 Uploading Certificate (Watermark-based Authentication)



Step 3 Click **Select Certificate File**, select a local certificate file to go to the **Certificate Information** page, as shown in Figure 10-59.

Figure 10-59 Certificate Information (Watermark-based Authentication)



Step 4 Click **Import** to import the certificate, and copy the displayed device information and provide it to NSFOCUS technical support to obtain the watermark file.

Step 5 Click **Import Watermark File** to import the obtained watermark file. After successful authentication, a prompt appears indicating that system-related services need to be restarted.

Step 6 Click **OK**. After the system logs out, log in again in 3~5 minutes to finish the authentication method switch.

----End

10.7.3 Certificate Status

Before an LAS certificate is about to expire, the system sends a notification message; if the certificate has not been updated after expiration, a notification message will also be sent. For how to view messages, see Message Center.

Hover over the icon and choose **License** > **Certificate Status** to view certificate information and export certificate files, as shown in Table 10-56.

Table 10-56 Platform Certificate Information

Display Item	Description
Certificate Status	Status of the certificate.
Certificate Type	Type of the certificate, such as trial certificate and commercial certificate.
Authentication Type	Authentication methods, such as cloud authentication and watermark-based authentication. Note The hardware version of LAS supports only local authentication. VM LAS supports all the authentication methods.
Version Type	LAS version type, such as basic edition.
Certificate HASH	Certificate hash value.
Customer Name	Customer name authorized by the certificate.
Licensed Collectors	The maximum number of collectors authorized by the certificate.
Licensed Log Sources	The maximum number of log sources authorized by the certificate.
Licensed Cluster Nodes	The maximum number of cluster nodes authorized by the certificate.
Certificate Validity Period	Validity period of the certificate.
Database Type	Database type used by LAS, such as postgresql.

Caution

The validity period of a LAS certificate refers to the period from 0:00 on the start date to 24:00 on the end date.

Notes for commercial certificates are as follows:

- Commercial certificates can be updated within their validity period.
- The validity period of commercial certificates refers to the service period for authorized product upgrade.
- 3 months before the commercial certificate expiration date, the system reminds and prompts you to update the certificate.
- After the commercial certificate expires, LAS can still be used but cannot be upgraded. The system reminds you of the number of expired days.

Notes for trial certificates are as follows:

- Trial certificates can be upgraded within their validity period.
- The validity period of a trial certificate refers to the product trial date.
- 7 days before the trial certificate expires, the system reminds and prompts you to update the certificate.
- After the trial certificate expires, you cannot perform any other functional operations in LAS except importing certificates.

Viewing Certificate

In the certificate information table, click the icon next to the certificate HASH to view the QR code.

Exporting Certificate

At the upper-right corner of the **Certificate Status** page, click **Export Certificate** to back up the certificate locally.

10.8 Upgrade

The upgrade of LAS includes system upgrade and knowledge base upgrade.

10.8.1 System Upgrade

LAS supports both manual upgrade and online upgrade.

Manual Upgrade

Manual upgrade refers to downloading the upgrade package and then uploading the package to LAS to perform an upgrade.

The procedure for manually upgrading LAS is as follows:

Step 1 Hover over the icon and choose **Upgrade > System Upgrade > Manual Upgrade**.

Step 2 Click **Select Upgrade Package (*.dat)** to select a local upgrade package file.

Step 3 Verify that the upgrade package information is correct, and click **Confirm Upgrade**.

The page displays the upgrade status and progress of all nodes.

- Success: when all nodes have been successfully upgraded, the page displays the upgrade success message.
- Failure: LAS will be locked for upgrade. To avoid irreversible damage to the system, please contact NSFOCUS technical support.

----End

Online Upgrade

Online upgrade refers to the situation where LAS directly downloads the upgrade package and performs the upgrade. Online upgrade methods include auto upgrade and semi-auto upgrade.

Auto Upgrade

After auto-upgrade is enabled, LAS checks the upgrade site at the scheduled time for available upgrade packages. If a new package exists, LAS automatically downloads and installs it.

The procedure of configuring an auto-upgrade policy is as follows:

Step 1 Hover over the icon, and choose **Upgrade > System Upgrade > Online Upgrade**.

Step 2 Enable **Auto-Upgrade**, and set the upgrade method to **Check and Upgrade**.

Step 3 Configure the auto upgrade parameters, as shown in Table 10-57.

Step 4 Click **Confirm**.

----End

Table 10-57 Auto Upgrade Parameters

Parameter	Description
Upgrade Site	The upgrade site from which LAS obtains upgrade packages. Defaults to http://update.nsfocus.com.
Upgrade Time	The frequency and time for LAS to automatically check for upgrade packages.
Use Proxy	Whether an HTTP proxy is required to connect to the upgrade site. If set to **Yes**, you need to configure the proxy server's address, port, and login username with password.

Semi-auto Upgrade

After semi-auto upgrade is enabled, LAS will automatically check at the upgrade site at the update time for the existence of an upgrade package. If an upgrade package exists, LAS will record the upgrade package information in the upgrade information and prompt the user to perform the upgrade. The user can perform manual upgrade operation in the upgrade information list.

The procedure for configuring a semi-auto upgrade strategy is as follows:

Step 1 Hover over the icon, and choose **Upgrade** > **System Upgrade** > **Online Upgrade**.

Step 2 Enable **Auto-upgrade**, and set the upgrade method to **Check for Updates**.

Step 3 Configure parameters as shown in Table 10-57.

Step 4 Click **Confirm**.

LAS will periodically check for upgrade packages according to the settings. If upgrade packages are found, it will prompt you to perform a manual upgrade. LAS will sequentially download upgrade packages and perform upgrades from low to high based on version dependencies.

----End

10.8.2 Knowledge Base Upgrade

Knowledge base refers to the built-in content in LAS, such as log parsing rules and event rules. Knowledge base only supports manual upgrade. You must manually download the upgrade package and then upload the package to LAS for an upgrade.

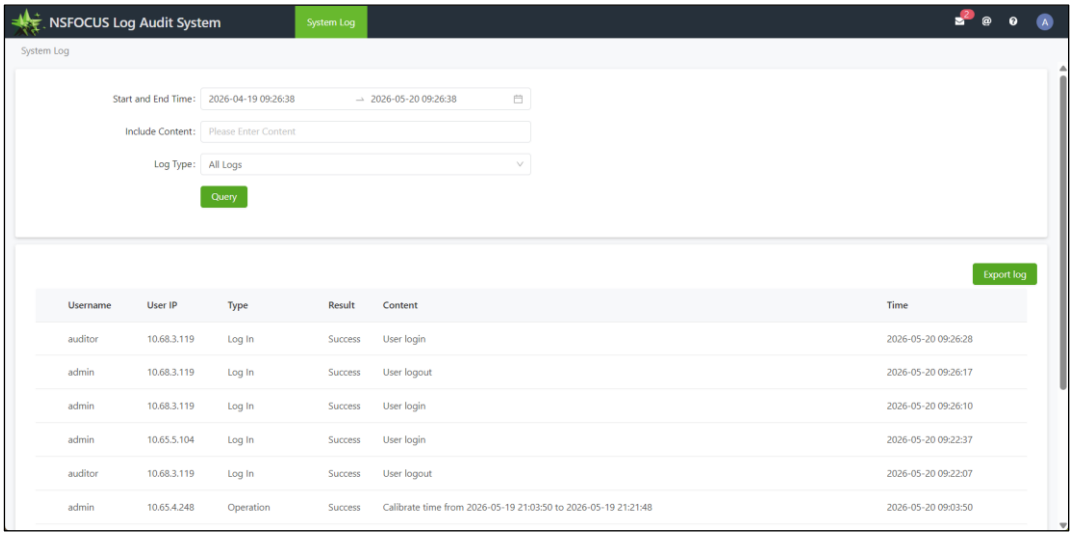
Hover over the icon, choose **Upgrade** > **Knowledge Base Upgrade**, and manually upgrade the knowledge base. The upgrade method is basically the same as manually upgrading the system. For details, see Manual Upgrade.

11 Audit Logs

Only users with the audit administrator role can view audit logs in LAS. The audit logs record login logs, operation logs, exception logs, and upgrade logs for all users.

In the **System Log** page, select the start and end time and log type, click **Query**, and the system audit logs meeting the conditions are displayed, as shown in Figure 11-1; click **Export Logs** to export the audit logs as a CSV file.

Figure 11-1 System Audit Log



A Console Management

By connecting to the serial port, the console administrator can access the management interface of LAS to perform functions such as system initial configuration, status detection, and restore initial configuration. When a fault occurs in the Web-based Manger and you cannot log in, or for management operations that cannot be performed through the Web-based Manger, you can manage LAS through the console.

This chapter covers the following topics:

Function	Description
Console Login	Introduces the login method for the console.
Keyboard Operations	Introduces the keyboard operation methods for the console.
Function Introduction	Introduces the function menu of the console.

A.1 Console Login

Before you log in to the console, the following preparations are required:

- 1 workstation.
- 1 serial cable (included in accessory kit).
- Terminal software capable of connecting to a serial port (such as the terminal included with Windows).
- Use a serial cable to connect the serial ports of LAS and the workstation.

The following takes PuTTY terminal as an example to describe the detailed steps for logging in to console with the default account.

Step 1 In file explorer of your computer, select **Computer/This PC**, right-click and select **Properties** > **Device Manager**, and view the serial port of your machine in device manager.

Step 2 Open PuTTY software, as shown in Figure A-1. Configure serial port connection properties according to Table A-1.

Figure A-1 Selecting Connection Port

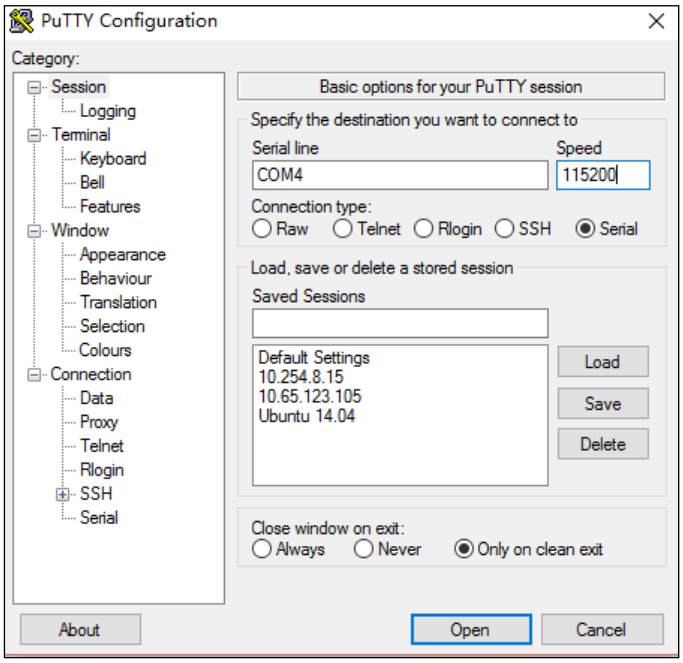


Table A-1 Serial Port Connection Properties

Parameters	Value
Serial Line	Comx (COM port, customized according to your system), obtained from step 1.
Speed	Set the connection speed. Enter **115200** (bits per second).
Connection Type	Select **Serial**.

Step 3 Click **Open** to successfully establish a connection with LAS.

Step 4 Enter the initial username and password of the console administrator (see Initial User Account) to log in to the console interface.

First, enter the language selection interface as shown in Figure A-2.

Figure A-2 Language Selection

Step 5 Select **English**, and press **Enter** to enter the main menu, as shown in Figure A-3.

Figure A-3 Console Main Menu

Step 6 Configure the IP address of the management interface.

Choose **Network Configuration > Set Management Interface**, and modify the IP address of the management interface, as shown in Figure A-4.

Figure A-4 Configure IP of Management Interface

Step 7 After the IP address of the management interface is modified, log in again using the newly configured IP: https://newIP.

----End

A.2 Keyboard Operations

In the console management interface, only keyboard operations are permitted. The descriptions are as shown in Table A-2.

Table A-2 Key Instructions

Keyboard	Description
↑	① Switch to input box ② Move up
↓	① Switch to **OK** ② Move down
←	① Switch to **OK** ② Move left
→	① Switch to **Cancel** ② Move right
Esc	Cancel

Keyboard	Description
Enter	Confirm
Tab	Switch between the input box, **OK**, and **Cancel**
Backspace	Deleting the character before the current cursor position

A.3 Function Introduction

After successfully logging in to the console, the console's main menu includes administration, network configuration, network diagnosis, system status, and user management.

A.3.1 Administration

Navigate to the **Administration** page, where you can manage and configure LAS as shown in Table A-3.

Table A-3 Console Administration Operation

Operation	Description
Restart System	Restarts LAS.
Shut Down System	Shuts down LAS.
Version Information	Displays the version information.
Shut Down/Start SSH Service	After enabling the SSH service, NSFOCUS technical support can remotely log in to LAS for troubleshooting. Note If the SSH service is shut down, you need to log in to the consoleto enable it.
Setting System Clock	Sets the date and time displayed in LAS.
Resetting Web Administrator Password	When system administrator forgets the login password, reset it to the initial password.
Resetting Web Audit Administrator	When the audit administrator forgets the login password, reset it to the initial password.
Resetting Web Operator	When the operator forgets the login password, reset it to the initial password.
Modifying Console Administrator Password	Modify the login password of the console administrator. Its length must be 9 to 20 characters and contains at least two of the following: letters, numbers, or special characters (@#$^_).
Set as Secondary Node	Configure this device as a secondary node via console.

A.3.2 Network Configuration

Go to **Network Configuration**, where you can view and configure the network settings of LAS, as shown in Table A-4.

Table A-4 Console Network Configurations

Operation	Description
Show Network Settings	Displays the configurations of the management interface.
Configuring Management Interface	Specifies the IP address, netmask, and gateway address of the management interface. It supports both IPv4 and IPv6. Note After the management interface IP is changed, the system will unavailable for 5~10 minutes. Please wait patiently.
Adding Management Interface Route	Specifies the path for network access.
Deleting Management Interface Route	If a static route is no longer needed, you can manually delete it.
Changing Management Interface	The default management interface is m interface. If the current LAS device has multiple nics in enabled status, after entering this menu, all enabled nics will be displayed, and you can select the desired NIC and set it as the management interface.

A.3.3 Network Diagnostics

Navigate to **Network Diagnosis**. You can diagnose the network of LAS using methods such as ping, traceroute, and dig. Operation instructions are shown in Table A-5.

Table A-5 Console Network Diagnostic Operation

Operation	Description
Ping (IPv4)	Check network connectivity for a host.
Ping (IPv6)	Check network connectivity for a host.
Route Tracing	Track the routing status between the system and the specified IP.
Network Status	Check the current network status.
Display Routing Information	Check routing information for the current network.
DNS Query	Query DNS information for a specific host.

A.3.4 System Status

Navigate to **System Status**, which displays information such as NIC configuration and routing for LAS. Operation instructions are shown in Table A-6.

Table A-6 Console System Status Operation

Operation		Description
Network Status Detection	Display Network Settings	Display the network configurations of the management interface.
	Display Routing Information	Display the system routing table.
NIC Status Detection		Display NIC status.

A.3.5 User Management

This function is only available in LAS hardware version, for managing console user accounts, specifically the engineer and product accounts.

Navigate to **User Management** to activate, disable, and view other console accounts as shown in Table A-7.

Table A-7 Console User Management Operation

Operation		Description
Engineer (engineering staff)	Display Engineer User Status	Display the status of the current engineer account.
	Configure Engineer User Status	Enable/Disable the engineer account, defaulting to disabled.
	Set Engineer User Password	Change the user password of the engineer account.
	Reset Engineer User Password	Set the password of the engineer account to the default one.
Product (production staff)	Display Product User Status	Display the status of the current product account.
	Set Product User Status	Enable/Disable the product account, defaulting to disabled.
	Set Product User Password	Change the password of the product account.
	Reset Product User Password	Set the password of the product account to the default one.

B Default Parameters

This section introduces the default parameters of LAS.

B.1 Initial User Accounts

Role	Username	Password
System Administrator	admin	admin@123456
Audit Administrator	auditor	auditor@123456
Console Administrator	conadmin	conadmin@123456

B.2 Console Communication Parameters

Baud Rate	Number of Transmission Bits
115200	8

C Device Access

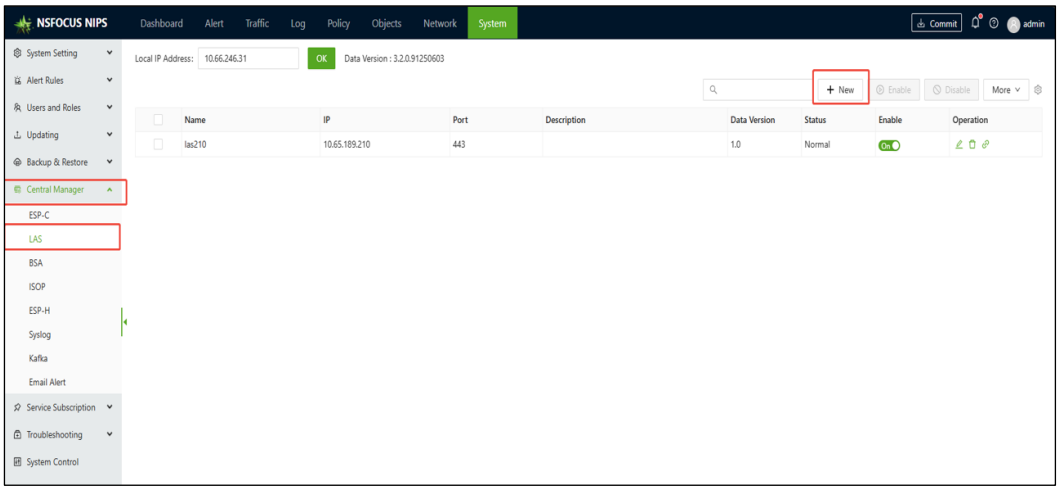
C.1 Registering via New Devices

This section uses NIPS v5.6R10F00 as an example to walk through how to configure new versions of security devices to enable their access to LAS.

Step 1 Log in to NIPS.

Step 2 Choose **System > Security Center**, and click **New**, as shown in Figure C-1.

Figure C-1 NIPS Configuration Page for LAS – New Devices



Step 3 Configure connection parameters as shown in Table C-1.

Table C-1 Connection Parameters

Parameter		Description
Local IP Address		Used to manage the IP address of NIPS.
Enterprise Security Center (ESPC)	Server Address	IP address of the collector. Connecting to multiple LAS systems is allowed.
	Port	Port number for communicating with LAS. Currently it supports 443 only.

Step 4 Select **Start**, and click **OK**.

After successful connection, the status displays as **Connected**.

----End

C.2 Registering via Legacy Devices

This section uses NIPS v5.6.9 as an example to walk through how to configure previous versions of security devices to enable their access to LAS.

Step 1 Log in to web-based manager of NIPS.

Step 2 Choose **System > Central Manager**.

Step 3 Configure basic configuration parameters as shown in Table C-2.

Table C-2 Basic Configuration Parameters

Parameter	Description
Local IP Address	Used to manage the IP addresses of NIPS.
NSFOCUS Enterprise Security Center Address 1/2/3/4	The collector's IP address. • For a single LAS, configure any address of NSFOCUS ESPC. • Connecting to multiple LAS systems is allowed.

Step 4 Select **Start**, and click **OK**.

Step 5 Restart the engine.

a. Choose **System > System Control**.

b. Click **Restart Engine**.

----End

D Communication Matrix

D.1 Supported Devices

This chapter describes the devices that LAS supported for onboarding. For onboarding procedures, refer to the corresponding operation guides for specific devices.

Supported Devices	Device Engine Version
NF	• V6.0.1 • V6.0R01F05 • V6.0R03F00
NIDS	• V5.6.7 • V5.6.8 • V5.6.9 • V5.6R10F00 • V5.6R10F01 • V5.6R10F02 • V5.6R11F00
NIPS	• V5.6.7 • V5.6.8 • V5.6.9 • V5.6R10F00 • V5.6R10F01 • V5.6R10F02 • V5.6R11F00
NTA	V4.5R89F00SP04 and later versions
SAS	• V5.6.7 • V5.6.8 • V5.6R10F00
SAS-ICS	V5.6.10
SAS-H	V5.6R10F00
TAC	• V2.0R01F00

Supported Devices	Device Engine Version
	• V2.0R01F01 • V2.0R02F00 • V2.0R02F01
OSMS	V5.6R10F00
FWCX	V6.0R70F30
WAF	• V6.0R05F01 • V6.0R06F00 • V6.0R06F01 • V6.0R07F00 • V6.0R07F01

D.2 Operating Systems Supported by Agent

The operating systems supported by agent are all 64-bit.

System		Version Information
Windows		Windows XP
		Windows Server 2003
		Windows Server 2008
		Windows Server 2012 Note Both standard and data center editions are supported.
		Windows Server 2016
		Windows Server 2019
		Windows 7
		Windows 8
		Windows 10
Linux	X86	CentOS 6.5
		CentOS 6.6
		CentOS 6.7
		CentOS 6.9
		CentOS 7.0/7.1/7.4/7.5/7.7/7.8/7.9
		CentOS 7.2
		CentOS 7.3

System		Version Information
		CentOS 7.6
		Debian 6.0.6
		Debian 8.7
		Debian 9.11
		Debian 10.2/10.7/10.9
		Red Hat 5.4
		Red Hat 5.9
		Red Hat 6.4
		Red Hat 6.5
		Red Hat 6.7
		Red Hat 7.3
		Red Hat 7.4
		Red Hat 7.2/7.5/7.6/7.7
		Red Hat 8.7
		SUSE 11 SP2/SP4
		SUSE 11 SP3/SP5
		SUSE 12 SP3/SP5
		SUSE 15
		Linx
		Linx 6.0.60/6.0.80
		Red Flag Asianux 7.6
		Anolis-OS 7.7/7.9/8.4/8.6
		Red Flag Asianux 3.0.4.1.2-44
		openEuler 20.03-LTS-SP3
	Arm	Kylin 4.0/4.0.2
		Kylin Linux Advanced Server V10
		Neokylin Linux Advanced Server V7Update6 (Chromium)
		Neokylin Linux Advanced Server V7.6Update6 (Chromium)
		Uniontech OS Server 20 enterprise --- Linux oa-sms01 4.19.0-arm64-server
Unix		Solaris 10 (sunos 5.10)
Ubuntu		Ubuntu16/16.04
		Ubuntu14.04

System	Version Information
	Ubuntu18.04
	Ubuntu20.04
	Ubuntu12
BC-Linux	7.1/7.4/7.5/7.6/7.7
	8.1/8.2
Opensuse	42.3
	15.2