NSFOCUS LAS
Syslog Data Forwarding Spec

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 the data format, configurations and descriptions of Syslog in NSFOCUS Log Audit System ("LAS" for short).

This document is provided for reference only.

Organization

Chapter	Description
1 Data Format	Introduces LAS syslog forwarding data format.
2 Functional Configurations	Introduces LAS syslog forwarding configuration details.
3 Data Description	Introduces log data, event data, and message center data.

Change History

Version	Description
V2.0R02IB00	Initial release.

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

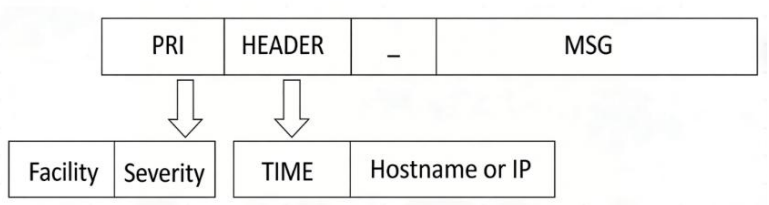
For any query regarding the usage of the documentation, you can contact us:

Email: info-support@nsfocus.com

1 Data Format

The forwarding data (over UDP) of LAS syslog uses the RFC 3164 data format protocol. Syslog messages consist of three parts: PRI, HEADER, and MSG, as shown in Figure 1-1.

Figure 1-1 Syslog Message Structure



- PRI indicates the priority. The default PRI value for LAS syslog forwarding is 11.
- HEADER indicates the header section, containing the hostname and timestamp of the machine running LAS. The timestamp format is MM DD HH:MM:SS. For example: Feb 24 15:52:41.
- MSG indicates the information section, containing forwarded data types and detailed data of various logs forwarded by LAS.

Example: <PRI>Time Hostname Data Type:Data Details

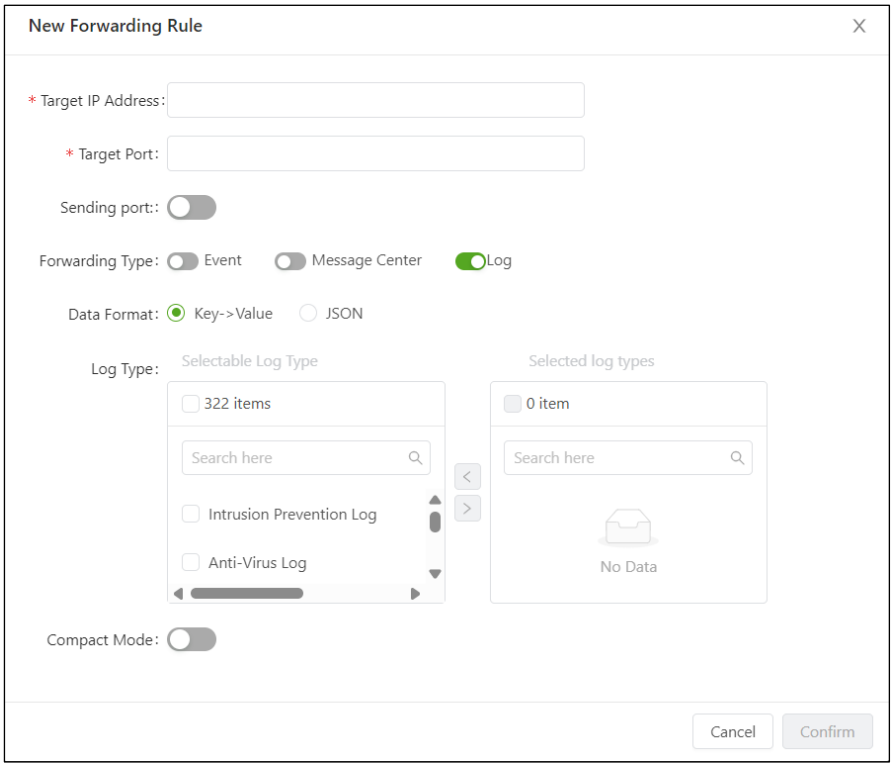
2 Functional Configurations in LAS

Step 1 Log in to the web-based manager of LAS.

Step 2 Hover the mouse over the icon, choose **Data Management > Syslog Forwarding**.

Step 3 Click **Add Configuration** to enter the page shown in Figure 2-1.

Figure 2-1 New Forwarding Rule Configuration for Syslog



Parameter Description

Target IP Address

Required. The device address for receiving syslog logs. Currently, only IPv4 addresses are supported.

Sending Port

Optional. If it is not set, LAS will use a random port to send data. Note that the specified sending port cannot be duplicate with the port in data ingestion; otherwise, the sending will fail.

Forwarding Type

Required. Log data forwarding is selected by default.

Currently, LAS supports three types of data forwarding: event data (identifier: `stream-event`), message data (identifier: `msg-center`), and log data (identifier: `sas-l`).

Specific examples are as follows:

- Event Example

<11>May 10 15:47:04 hostname stream-event: data

- Message Example

<11>May 10 15:47:04 hostname msg-center: data

- Log Example

<11>May 10 15:47:04 hostname sas-l: data

Data Format

Required, defaults to JSON.

Currently, LAS supports two data formats: Key->Value and JSON.

Specific examples are as follows:

- Key->Value Example

<11>May 10 15:47:04 hostname sas-l: param1=value1;param2=value2;

- JSON Example

<11>May 10 15:47:04 hostname sas-l: {"param1":"value1","param2":"value2"}

Log Type

Configure the corresponding forwarding data types. You can specify one or more log types.

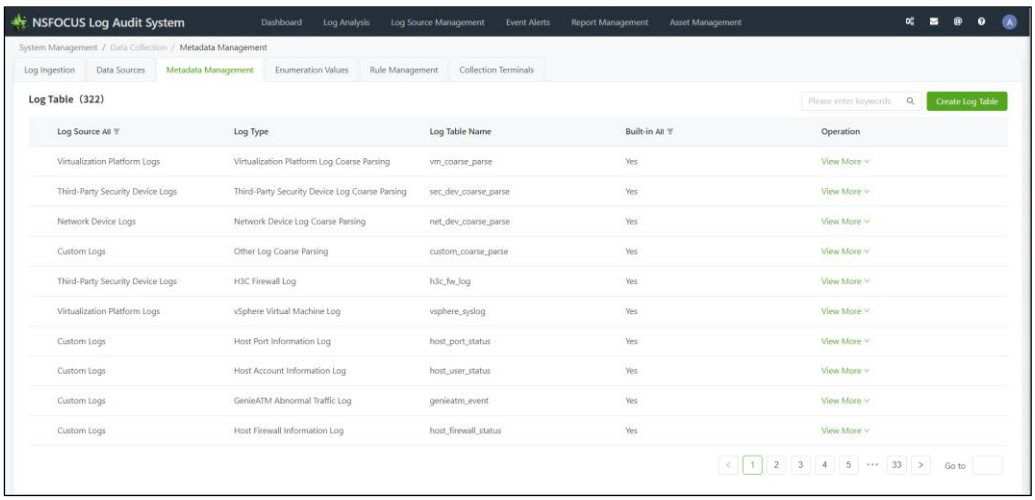
3 Data Description

3.1 Logs

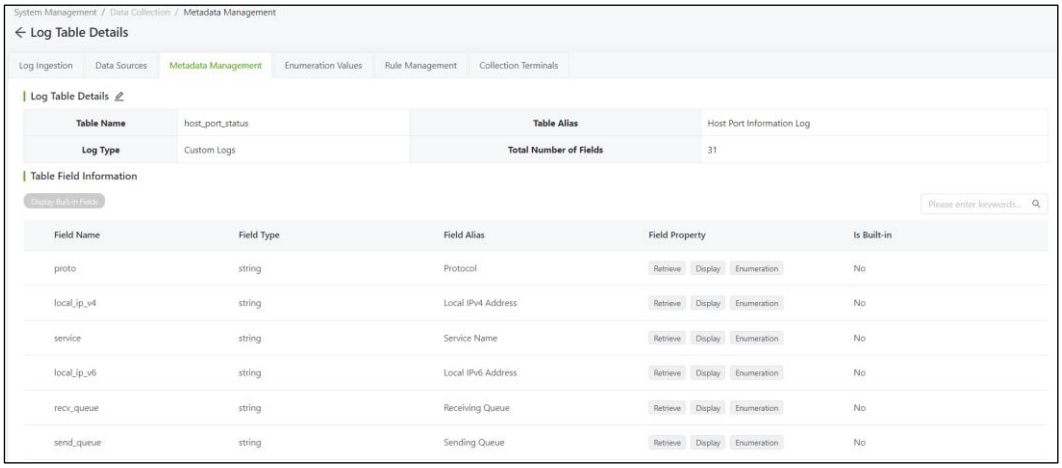
You can view the detailed logs in the web-based manager of LAS. For enumeration values of each field in the log data, refer to the definitions of security devices integrated with LAS.

Step 1 Log in to the web-based manager of LAS, hover the mouse over the icon, and choose **Data Collection > Metadata Management**.

Step 2 View all log types for the accessed objects, as shown in the following figure.



Step 3 Click **View More** in the **Operation** column to view the corresponding log type, as shown in the following figure.



----End

3.2 Events

Field Name	Field Type	Field Description	Remark
dasset_gr	string		
dst_organization	number	Target organization	
fall_host	string		
dst_business	number	Target company	
focus	string	Concerns	
dip	string	Target IP	
project_id	string		
sasset	string	Attacker’s asset information	
dst_city	string	Target city	
nta_src_sum_packets	number		
dst_province	string	Target province	
app_id	string		
category2	string	Level 2 event type	
info_hit	string		
tagid	number	Tag number	
category1	string	Level 1 event type	
src_occurrence	number	Number of attacks	
src_business	number		

Field Name	Field Type	Field Description	Remark
nsuid	string	Event ID	
src_country	string	Attacker's country	
domain	string	Domain name	
name	string	Event name	
alarm_id	string	Alert ID	
dasset	string	Target asset information	
dst_topology	number		
src_province	string	Attacker's province	
extension	string		
description	string	Event description	
src_organization	number	Attacker's organization	
collecter_id	string	Collector ID	
src_topology	number		
dport	number	Target port	
focus_content	string	Content of interest	
soc_id	string	Related log details collection	
sip	string	Source IP address	
src_city	string	Attacker's city	
dst_country	string	Target country	
nta_src_sum_bytes	number		
suggestion	string	Remediation recommendation	
url	string	URL path	
rule_id	string	Event rule ID	
sasset_gr	string		
dev_ip	string	Device IP address	
dst_occurrence	number	Number of attacks	
sport	number	Source port	
invalid_for_trap	string		
agent_id	string	ID of the data-collecting agent	
valid	boolean		
action	number		
alarm_no	number	Contains log user ID	

Field Name	Field Type	Field Description	Remark
alarm_rule_id	number	Alert rule ID	
nta_event_type	number	Alert event type	
alarm_state	number	Alert status	Pending: -1; Alerted: 1
nta_severity	number	Alert level	Low: 1; Medium: 3; High: 5
start_time	number	Start time	
times_for_trap	number		
end_time	number	End time	
stage	number	Attack phase	
risk	number	Risk level	Low: 1; Medium: 3; High: 5
nta_event_id	number		
sum_packets	number	Attack peak (packets)	
sum_bytes	number	Attack peak (bytes)	
nta_max_bytes	number	Total attacks (bytes)	
nta_max_packets	number	Total attacks (packets)	
nstimestamp	number	Event timestamp	

3.3 Messages

Field Name	Field Type	Field Description	Remark
id	number	Message ID	
uid	number	User ID	
type	string	Message type	See Message Type.
sub_type	string	Message subtype	See Message Type.
priority	number	Message priority	High: 3; Medium: 2; Low: 1.
params	string	Parameters	
content	string	Message content	
objid	string	Agent ID with agent-related messages	
ctime	Timestamp	Occurrence time	
status	string	Read status	Read: read; Unread: unread.
rtime	Timestamp	Read time	

A Message Types

The message types and subtypes in the Message Center are shown in the table below.

NEW_DEVICE	Device message
NEW_DEVICE_REMOVED	Device message
DEV_LICENSE	Device message
DEV_UPGRADE_CHECK	Device message
DEV_UPGRADE_DOWNLOAD	Device message
DEV_INFO	Device message
DEV_CASCADE	Device message
PLATFORM_UPGRADE_CHECK	System upgrade
PLATFORM_UPGRADE_RESULT	System upgrade
PLATFORM_LOG_LIMIT	System upgrade
APP_UPGRADE_RESULT	APP upgrade status
DEVICE_UPGRADE_RESULT	Device upgrade status
DEVICE_DEBUG_RESULT	Device debug
PLATFORM_LICENSE_EXPIRED	Certificate message
PLATFORM_LICENSE_WILL_EXPIRE	Certificate message
APP_LICENSE_EXPIRED	Certificate status
APP_LICENSE_WILL_EXPIRE	Certificate status

PLATFORM_LICENSE_NOT_IMPORTED	Certificate message
PLATFORM_LICENSE_NOT_ALLOW	Certificate message
DISK_CAPACITY_ALERT	Disk space alert
DISK_CAPACITY_INSUFFICIENT	Disk space alert
ALARM_MAIL_SERVER	Alert message
ALARM_MSG_SERVER	Alert message
ALARM_FTP_SERVER	Alert message
ALARM_LOGIN	Alert message
ALARM_NFS	NFS alert
ALARM_SERVICE	Alert message
BACKUP_AUTO	Automatic backup
BACKUP_MANUAL	Manual backup
RECOVER	Data recovery
PUSH_ASSET	Asset push
PUSH_DEVICE	Device push
CLEAN_AUDIT_AUTO	Threshold management
CLEAN_DEVICE_AUTO	Threshold management
PARTICIPATE_UE_IMPROVEMENT	User experience program
MONITOR_WAINING	Monitoring message
INFO_NTI_KEY	NTI message
FTP_TASK	FTP storage service
MESSAGE_INFO	SMS message
MAIL_INFO	Email message
LICENSE_ALLOW_DEVICE_NUMBER_WARNING	Node count alert
CLOUD_CONNECT_RESULT	Cloud platform connection
TOPOLOGY_ALARM	Topology discovery alert

TASK_FRAME_NOTIFICATION	Task management
COLLECT_TYPE	Collection type
SYSTEM_TYPE	System type
LICENSE_TYPE	Certificate type
DEV_REGISTER	Device registration
DEV_OFFLINE	Device message
DEV_ONLINE	Device message
DEV_INGEST	Device onboarding
DEV_PATCH_CHECK	Device upgrade package
DEV_PATCH_DOWNLOAD	Device upgrade package
DEV_ALARM_CPU	Device CPU alert
DEV_ALARM_MEM	Device memory alert
DEV_ALARM_DISK	Device disk alert
DEV_ALARM_MONITOR	Device monitoring alert
INCREASE_ALARM	Surge alert
DECREASE_ALARM	Plunge alert
SPARE_ALARM	Idle alert
PIPELINE_ACCESS_ALARM	Log ingestion alert
PIPELINE_PARSE_ALARM	Log parsing alert
AUTO_ACCESS_RESULT	Automatic log ingestion
SYS_OTHER_ERROR	Other system errors
SYS_CONF_CHECK	System configuration check
SYS_PATCH_CHECK	System upgrade
SYS_UPGRADE_RESULT	System upgrade
SYS_LOG_LIMIT	System log limit
SYS_LOGIN_ALARM	System login alert
SYS_ALARM_CPU	System CPU alert

SYS_ALARM_MEM	System memory alert
SYS_ALARM_DISK	System disk alert
SYS_SERVICE_ABNORMAL	System service exception
MAIL_SERVER_ABNORMAL	Mail server exception
MSG_SERVER_ABNORMAL	SMS server exception
FTP_SERVER_ABNORMAL	FTP file server exception
NFS_SERVER_ABNORMAL	NFS server exception
SYS_PROCESS_CHECK	Process restart
LOG_BACKUP_SUCCESS	Log backup
LOG_BACKUP_FAILED	Log backup
LOG_RESTORE_SUCCESS	Log restore
LOG_RESTORE_FAILED	Log restore
NFS_MIGRATE_RESULT	NFS data migration
SYS_LOG_TIME_LIMIT	System log timeout
SYS_AUDIT_LOG_TIME_LIMIT	System audit log timeout
CASCADE_POLICY_CONFIGURATION	Cascade policy configuration
SYS_LICENSE_EXPIRED	System certificate expired
SYS_LICENSE_WILL_EXPIRE	System certificate is about to expire
SYS_LICENSE_NOT_IMPORTED	System certificate not imported
SYS_LICENSE_NOT_ALLOW	System certificate operation prohibited
DEV_LICENSE_EXPIRED	Device certificate expired
DEV_LICENSE_WILL_EXPIRED	Device certificate is about to expire

DEV_LICENSE_RE_IMPORTED	Re-import device certificate
CASCADE_OFFLINE	Cascade node status
CASCADE_CONF_ERROR	Cascade node configuration exception
CASCADE_TRANSPORT	Cascade node transmission
KAFKA_OVERSTOCK	Kafka service alert
AGENT_STRATEGY_UPDATE	Agent policy update
SYS_PWD_WILL_EXPIRE	System login password is about to expire
EVENT_SIGN_ALARM	Cryptographic assessment signature alert
DATA_DISK_MOUNTING_EXECPTION	Data disk not mounted
STATISTICS_STORE_RESULT	Log storage statistics
S3_MIGRATE_RESULT	S3 data migration