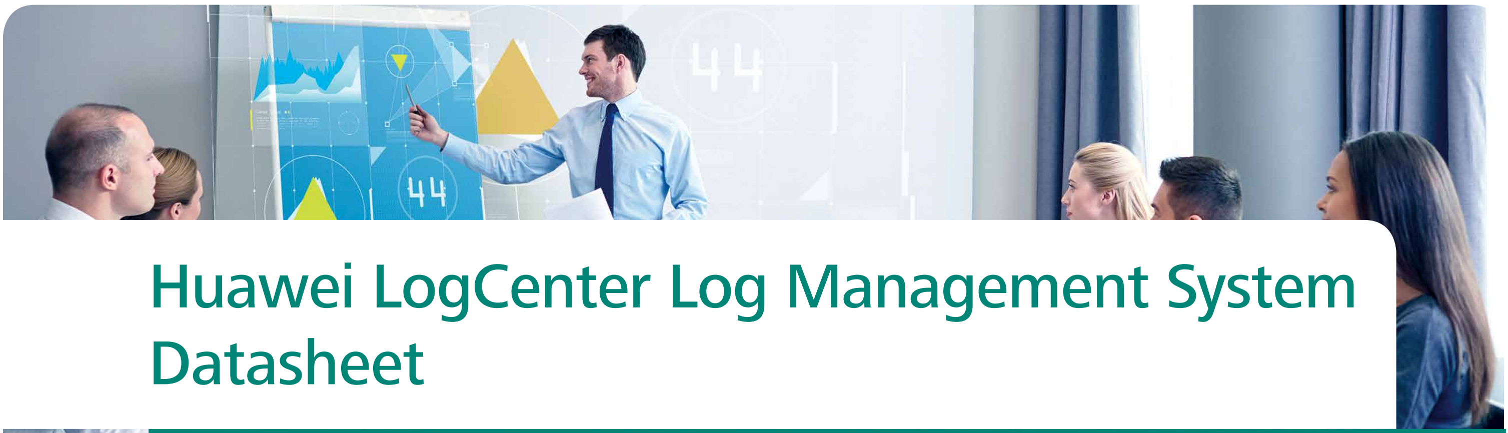


Huawei LogCenter Log Management System Datasheet

Product Overview

Massive application systems and network devices are deployed in an enterprise, including hosts, databases, other application systems, switches, and firewalls. Due to varying device log formats, poor intelligibility, and difficulties in storing massive logs, major security risks cannot be promptly detected from logs.

Government agencies and industrial organizations provide guidance and use internal control laws and standards to impose higher requirements on the completeness, accuracy, and effectiveness of run logs and user logs.

LogCenter:

- Provides a platform for collecting, storing, and auditing multiple types of large-scale logs in a unified manner.
- Supports log management of Huawei and other vendors.
- Provides industry-leading NAT tracing function and security event analysis.

Features

Unified Log Management and Quick Matching Capability

- LogCenter supports multiple log collection modes, including Syslog, session, SFTP, FTP static file, FTP dynamic file. Users can collect, classify, filter, summarize, analyze, store, and monitor logs reported from the application systems or NEs to help the administrator manage massive logs and learn NE running status, trace network user behaviors, and quickly recognize and eliminate security risks.
- LogCenter supports prompt notifications of critical logs. The administrator can customize keywords, log type, and log level thresholds. When logs match customized keywords, log type, or log level, LogCenter generates alarms in real time and notifies administrators through SMS messages or emails.

Professional NAT Tracing and Automatic Association with User information

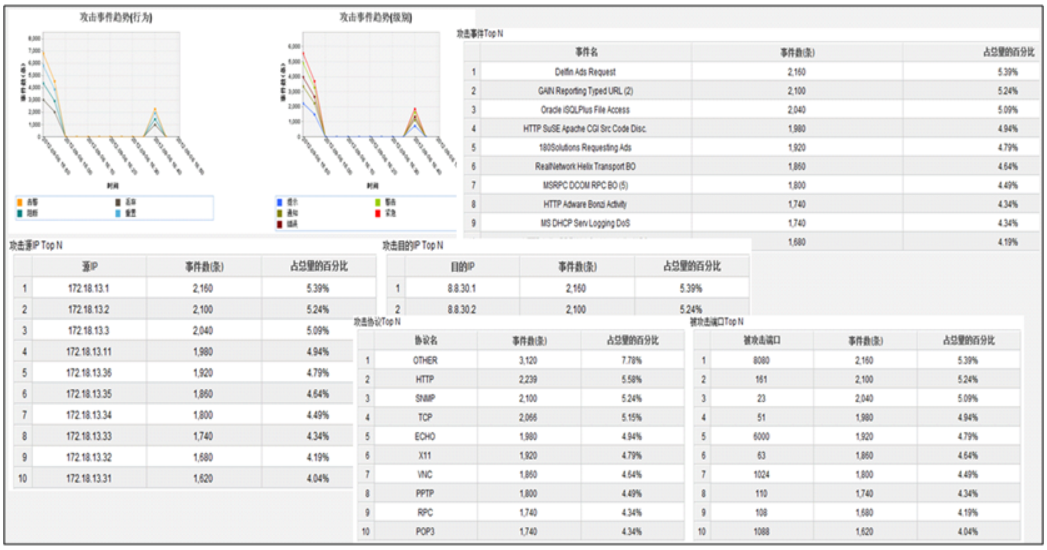
LogCenter collects and analyzes logs about sessions on NAT devices to obtain NAT information, including the IP address, destination port, NAT source IP address, and protocols. LogCenter uses the NAT information and the data source provided by the Authentication, Authorization and Accounting (AAA) server to ensure secure audit and traffic investigation.

In-Depth User Online Behavior Analysis

LogCenter works with Huawei USG and ASG devices to analyze user online behaviors, including user traffic, online duration, keywords, web access trends, emails, applications, network threats, and outgoing files.

Rich Security Event Analysis Reports

LogCenter collects security event logs about network security devices and systems, such as Huawei network UTM system, firewalls, intrusion protection system, and Anti-DDoS system, analyzes them, and generates reports to provide visibility into the network security status. LogCenter supports DDoS attack event, plug-in block, access control event, policy matching, IPS, URL filter, and email filter analysis.



攻击事件Top N

	事件名	事件数(条)	占总量的百分比
1	Delfin Ads Request	2,160	5.39%
2	GAIN Reporting Typed URL (2)	2,100	5.24%
3	Oracle iSQLPlus File Access	2,040	5.09%
4	HTTP SuSE Apache CGI Src Code Disc	1,980	4.94%
5	180Solutions Requesting Ads	1,920	4.79%
6	RealNetwork Helix Transport BO	1,860	4.64%
7	MSRPC DCOM RPC BO (5)	1,800	4.49%
8	HTTP Adware Bonzi Activity	1,740	4.34%
9	MS DHCP Serv Logging DoS	1,740	4.34%
		1,680	4.19%

攻击源IP Top N

	源IP	事件数(条)	占总量的百分比
1	172.18.13.1	2,160	5.39%
2	172.18.13.2	2,100	5.24%
3	172.18.13.3	2,040	5.09%
4	172.18.13.11	1,980	4.94%
5	172.18.13.36	1,920	4.79%
6	172.18.13.35	1,860	4.64%
7	172.18.13.34	1,800	4.49%
8	172.18.13.33	1,740	4.34%
9	172.18.13.32	1,680	4.19%
10	172.18.13.31	1,620	4.04%

攻击目的IP Top N

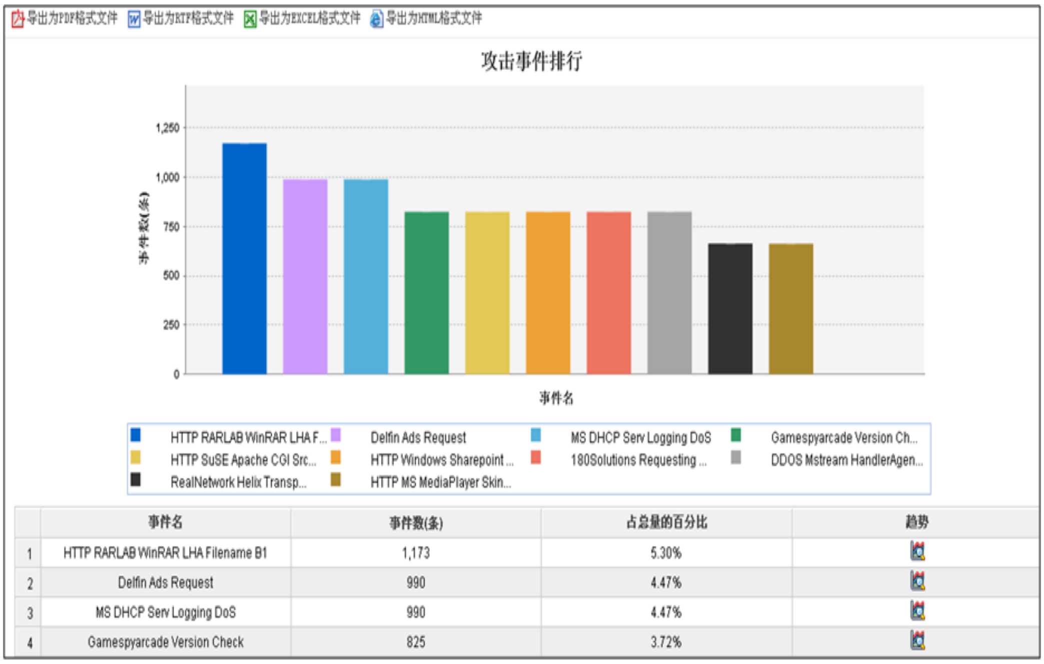
	目的IP	事件数(条)	占总量的百分比
1	8.8.30.1	2,160	5.39%
2	8.8.30.2	2,100	5.24%

攻击协议Top N

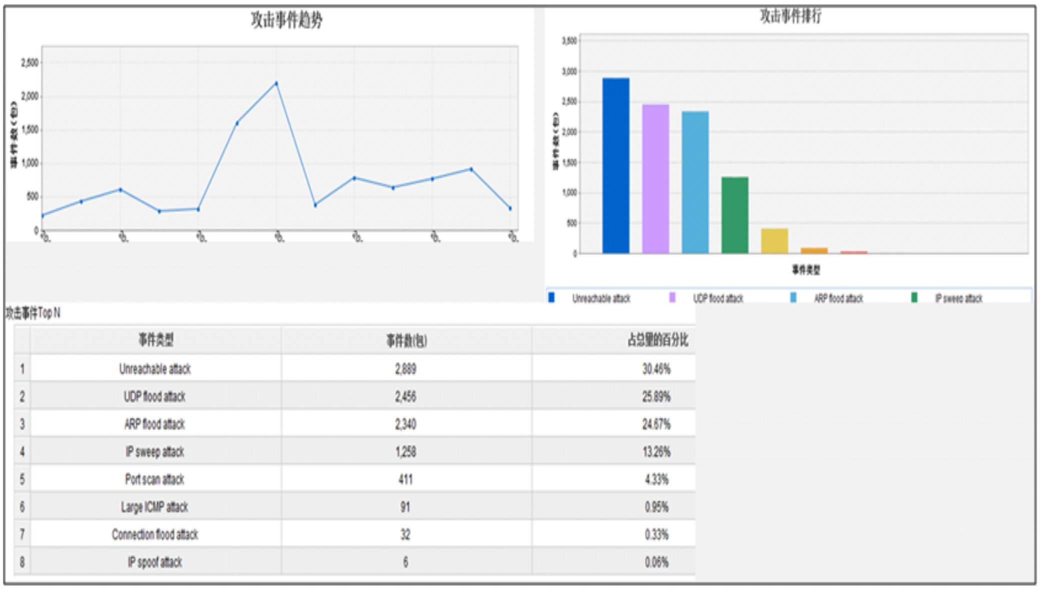
	协议名	事件数(条)	占总量的百分比
1	OTHER	3,120	7.78%
2	HTTP	2,239	5.58%
3	SNMP	2,100	5.24%
4	TCP	2,066	5.15%
5	ECHO	1,980	4.94%
6	X11	1,920	4.79%
7	VNC	1,860	4.64%
8	PPTP	1,800	4.49%
9	RPC	1,740	4.34%
10	POP3	1,740	4.34%

被攻击端口Top N

	被攻击端口	事件数(条)	占总量的百分比
1	8080	2,160	5.39%
2	161	2,100	5.24%
3	23	2,040	5.09%
4	51	1,980	4.94%
5	6000	1,920	4.79%
6	63	1,860	4.64%
7	1024	1,800	4.49%
8	110	1,740	4.34%
9	108	1,680	4.19%
10	1088	1,620	4.04%


导出为PDF格式文件
导出为RTF格式文件
导出为EXCEL格式文件
导出为HTML格式文件
攻击事件排行
事件数(条)
1,250
1,000
750
500
250
0
事件名
HTTP RARLAB WinRAR LHA F...
Delfin Ads Request
MS DHCP Serv Logging DoS
Gamespyarcade Version Ch...
HTTP SuSE Apache CGI Src...
HTTP Windows Sharepoint ...
180Solutions Requesting ...
DDOS Mstream HandlerAgen...
RealNetwork Helix Transp...
HTTP MS MediaPlayer Skin...

	事件名	事件数(条)	占总量的百分比	趋势
1	HTTP RARLAB WinRAR LHA Filename B1	1,173	5.30%	
2	Delfin Ads Request	990	4.47%	
3	MS DHCP Serv Logging DoS	990	4.47%	
4	Gamespyarcade Version Check	825	3.72%	



攻击事件Top N

	事件类型	事件数(条)	占总量的百分比
1	Unreachable attack	2,889	30.46%
2	UDP flood attack	2,456	25.89%
3	ARP flood attack	2,340	24.67%
4	IP sweep attack	1,258	13.26%
5	Port scan attack	411	4.33%
6	Large ICMP attack	91	0.95%
7	Connection flood attack	32	0.33%
8	IP spoof attack	6	0.06%

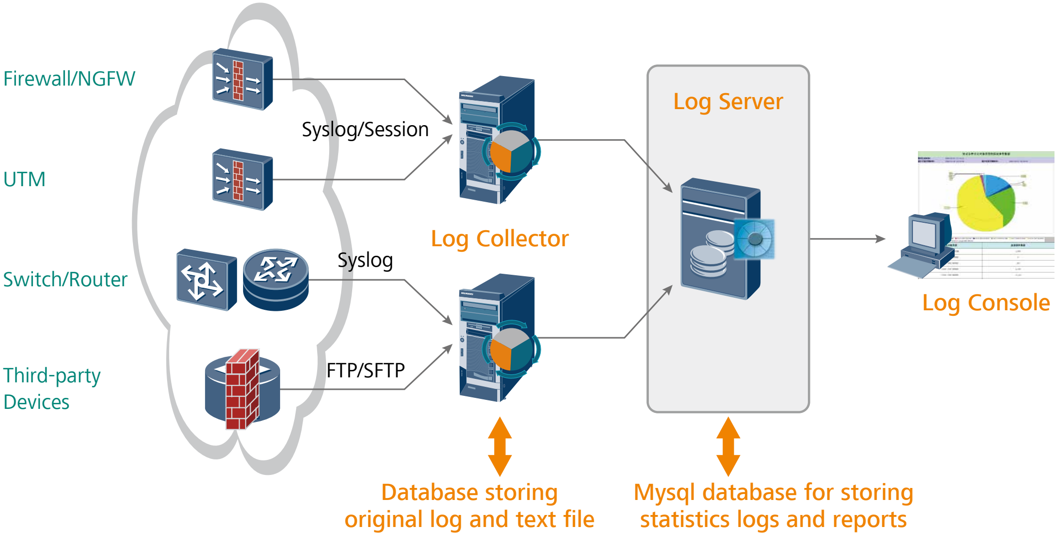
Million-level Log Processing per Second

LogCenter meets the performance requirements of nation-wide network auditing and collects and audits millions of system logs in a second, supporting high-performance log collection, storage, and audit functions for large and ultra large networks.

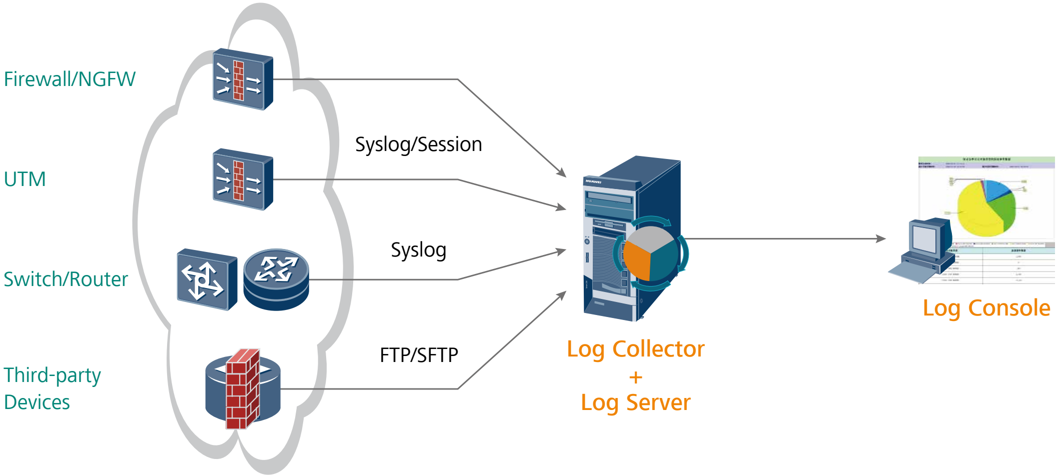
Deployment Scenarios

LogCenter network can be deployed in centralized or distributed ways.

- Distributed deployment: The Log Collector and the Log Analyzer are deployed separately on two servers.



  - Log Collector: Receives, aggregates, formats, filters, counts, and stores logs and generates alarms.
  - Log Analyzer: Manages policies, reports, devices, systems, and users.
  - Log Console: Provides an interaction GUI for managing foreground and background using the web.
- Centralized deployment: When performance requirements are low, LogCenter can also be deployed in a centralized way.



Product Specifications

Performance			
Maximum log recording speed (standalone mode)	250,000 EPS		
Maximum number of NEs supported by the LogCenter	2000		
Recommended Server Model	LogCenter All-In-One	LogCenter Analyzer	LogCenter Collector
Height	2 U		
Dimensions (H x W x D) mm	86.1 mm (2 U) x 447 mm x 748 mm		
Weight (full configuration)	30 kg	27 kg	30 kg
Fixed ports	4 x USB, 1 x VGA, 1 x Console, 1 x MGT, 8 x GE		
Memory	32 GB		
Storage space	2 x 300 GB SAS, 12 x 6-TB SATA	2 x 300 GB SAS, 6 x 2-TB SATA	2 x 300 GB SAS, 10 x 6-TB SATA
RAID	RAID 1 & RAID 6		
Redundant power modules	Standard		
AC power supply	100 V to 240 V; 50/60 Hz; 9 A to 4.5 A		
DC power supply	-48 V to -60 V; 26 A		
Maximum power	750 W AC/800 W DC		
Operating environment	Operating temperature: 5°C to 45°C (41°F to 113°F) Operating humidity: 8% RH to 90% RH non-condensing		
Non-operating environment (storage environment)	Storage temperature: -40°C to +65°C (-40°F to 149°F) Storage humidity: 5% RH to 95% RH non-condensing		

Authentication	CCC, RCM, CE, VCCI, FCC, IC, UL, BIS
Function/Feature	
Dashboard	• Dashboard layout customization, which can be saved for further use • Ranking of user IP application behaviors and users by Internet traffic volume, network threat classification and user ranking, attack defense event trend, traffic statistics based on protocol categories, application-layer threat event trend and ranking
Resource management	• Log source management, device group management, and discovery of specific IP network segments based on SNMP • Real-time collector status management, collector whitelist mode, and interworking between the collector and NEs • Log collection modes: syslog, security syslog, jdbc, heartbeat, dataflow, session, RADIUS, netflow, FTP dynamic/static file, and SFTP
Network security analysis	• Access control event log analysis: attack event trend, top 50 attack events/attack sources • ActiveX and Applet content filtering log analysis: distribution of filtered packets, top 50 source/destination IP addresses of filtered packets • IPS attack behavior analysis: attack event trend by behavior, attack event trend by severity, top 50 attack source IP addresses, attack destination IP addresses, attack protocols, and attacked ports • Antivirus log analysis: virus infection trend, top 50 virus events, most infected destination IP addresses, and source IP addresses that send most infected files • URL filtering log analysis: top 50 source IP addresses with most web access times as well as most accessed websites and URLs • Email filtering log analysis: email connection and matching trend, top 50 IP addresses for email connections that are permitted, blocked, and alerted on. • ACL rule and forwarding policy matching analysis: ACL rule trend, policy trend, top 50 most-hit interzone security policies • IM login and logout audit log analysis: firewall syslog analysis
Session analysis	• Million-level IPv4/IPv6 session log query • Query of NAT port range, user port pre-allocation, URL session, and IM session logs • Display of session trend and top 50 session source/destination IP addresses
Traffic analysis	• Real-time traffic trend based on physical ports' IP application protocols, top 50 users or IP addresses by incoming and outgoing traffic, and region-based traffic ranking report • NGFW application traffic ranking and trend; top 50 users or IP addresses by Internet traffic volume

Online behavior analysis	• Top 50 Internet access duration by user/IP address, Internet access trend • Top 50 keywords most matched by online behavior (application types include email, web page, and search engine) • User URL audit log analysis: top 50 websites by visit count or volume of uploaded content • Email filtering log analysis and application service type analysis: top 50 application service types • Top 50 users whose online behaviors match most threats, including virus and intrusion threats • Analysis of file sending logs: top 50 email, FTP, and HTTP-based file sending logs
SSL VPN analysis	• Analysis and top 50 SSL VPN users by traffic volume, users by virtual gateway traffic volume, connections, online users, intranet resource access, and mobile terminal access types
Log audit	• Top 50 log types with specific NE types, NEs, or time ranges • Setting of log audit rules for NEs, so that audit events are generated for logs matching the log audit rules

* For detailed parameters, contact the local Huawei sales agents.