



Log Intelligence Solution

# LogCentral



LogCentral from Infracore is a robust and scalable log intelligence solution directly targeted at meeting the compliance and risk mitigation requirements of the most demanding enterprises and service providers. With all log data available for queries and reports, users can pinpoint the locations of threats or other network problems, creating graphical or text-based reports for management, audits, network planning, and policy validation. LogCentral can store terabytes of log data to make a high-volume of logs instantly accessible to support decision-making and problem resolution.

## WINDOWS EVENT LOGS (AGENT-BASED)

LogCentral can collect Windows Event Logs with the use of an agent. The agent converts the Event logs to SysLog and sends it to the LogCentral. Many windows-based applications write their logs to the Application Event Log or a custom Event Log.

Examples of supported log sources using this method include:

- ▶ Windows System Event Log
- ▶ Windows Security Event Log
- ▶ Microsoft Exchange Server application logs

## SysLog

SysLog is a standard for transmitting log messages across the network. LogCentral includes an integrated SysLog server for receiving and processing these messages.

Example systems supported via this mechanism include the following:

- ▶ Cisco and other SysLog reporting routers
- ▶ Cisco and other SysLog reporting switches
- ▶ Cisco PIX, Netscreen, and other SysLog reporting firewalls
- ▶ Cisco, Snort and other SysLog reporting intrusion detection/prevention systems
- ▶ HP-UX, Solaris, and other SysLog reporting Unix-based operating systems
- ▶ Host based intrusion detection/prevention systems

## FLAT FILE LOGS

LogCentral can collect logs written to any ASCII based text file.

Examples of supported log sources using this method include:

- ▶ Apache and IIS web servers
- ▶ Linux system logs
- ▶ Windows ISA server logs
- ▶ DNS and DHCP server logs

## Features

- ▶ High performance, multi platform log collection
- ▶ Centralized and scalable log organization
- ▶ Agent based Windows event log, SysLog & flat file support
- ▶ Automated log archiving
- ▶ Fast search & recovery of archived logs
- ▶ Automatic, real-time identification of important events
- ▶ Centralized analysis and correlation
- ▶ Role-based monitoring & alerting
- ▶ Easy search & analysis
- ▶ Flexible & comprehensive reporting
- ▶ The ability to collect any type of log data regardless of source
- ▶ The ability to collect log data with or without installing an agent on the logging device
- ▶ The ability to "normalize" any type of log data for more effective reporting and analysis
- ▶ Single and Distributed architecture
- ▶ An open architecture allowing direct and secure access to log data via third-party analysis and reporting tools
- ▶ A role based security model providing user accountability and access control

# LogCentral



## CENTRALIZED AND DISTRIBUTED ARCHITECTURE

A single server collecting and reporting for all the logs and a distributed architecture for organizations with a lot of remote branches to reduce congestions and latency.

The distributed architecture has the option of one server acting as the UI and database server and a lot of small servers or collectors collecting events at different locations and sending the events to the Central server at a scheduled time.

## REPORTS

The users can sort and filter logs by running queries and using an advanced search option. The query based search option gives the user more insight into the logs and makes the retrieval process very easy.

Dozens of built-in reports including traffic reports using SysLog from routers and firewalls. Exportable to MS-Word, MS-Excel and PDF formats.

## ROLE BASED SECURITY

Role based security giving different users access to different logs wherein router administrators have access to router logs, windows administrators have access only to windows logs and security administrators have access to security logs.

## LOG ARCHIVING AND RECOVERY

Many businesses have a compliance requirement to keep historic log data especially for Auditing purposes. Collecting, maintaining and recovering historic log data can be expensive. Imagine trying to recover logs from a specific server two years in the past. Were the logs archived, if so, where have the logs been stored? What format are they in? Can the correct archived log files be identified among the tens of thousands (or millions) of other archive files?

LogCentral completely automates the process of archiving and restoring log data. Based on your policy, LogCentral automatically archives log data to archive files. Archive files are saved in a compressed format resulting in a 90% reduction in storage requirements and associated cost.

Recovering historic logs is a simple process. The Restoration process restores log data which can be analyzed using the same LogCentral analysis tools.

## ALARMS

Alarms can be flagged and defined to be sent as Emails and SMS to specified users. Role based security gives the administrator more control over sending of alarms based on the users defined thereby reducing the number of false or unwanted alarms to users.



Infrascope, Inc.

Suite 1200, 1000 N West Street

Wilmington, Delaware 19801, United States

Toll Free : 1.877.80.INFRA (1.877.804.6372)

Email: [info@infrascope.com](mailto:info@infrascope.com)