



## CUT THE TIME AND EFFORT OF TROUBLESHOOTING AND REPORTING

ArcSight Logger provides better visibility into IT data to help manage applications, servers and enterprise infrastructure.

HP Enterprise Security Solutions Brief

**“Our network operations group needed a better way to troubleshoot problems. Now, if a router is down or a firewall rule is blocking traffic that needs to get in, they can simply look at the event data in ArcSight Logger and instantly understand what is happening.”**

—Eric J. Hussey, Security Manager,  
Fiserv Enterprise Technology

### Importance of Effective Log Management

Organizations generate millions of logs a day and struggle with centralized collection, storage and analysis of those logs. Information technology teams are pressured more than ever before to maintain and improve service levels, as downtime of even a few minutes can mean capital loss and loss of trust and reputation. Ongoing log analysis helps avoid downtime and improve mean time to repair (MTTR). Many organizations initially attempt to perform log analysis using device-specific tools, but are quickly overwhelmed by the effort and time required to search across multiple devices.

Effective log management copies logs from the many devices in an enterprise to a centralized location for fast searching, reporting and alerting. This helps keep MTTR low, and also benefits other scenarios.

### Application Management

Log management assists in managing already-deployed applications, as well as the deployment process itself. It can be used for fast forensic analysis on faults, code exceptions, errors, connectivity issues, etc. Log management can provide additional value by converting proprietary application log formats into simple, plain English language that eliminates the need for experts at every level of analysis.

### Usage and User Management

Log management can effectively answer questions, such as who is on the network, what are they seeing, where are they going and how did they gain access? Scheduled reports or on-the-fly investigations support both regular audits and post-incident response. In addition, log management can be used to find usage stats on applications, servers and networks. Log data can also be used to analyze network traffic for better bandwidth utilization and planning.

### Change Management

Most organizations need to track who changed what, and whether the change was authorized. With hundreds of systems and applications deployed, configuration change tracking becomes extremely difficult. As all changes are captured in digital fingerprints, change management can be simplified by consolidating all logs into a single place and running scheduled searches and reports. Categorization plays a key role here as it takes away the need to understand cryptic log syntax. For example, a simple query on “modify configuration” can return all the logs from all the devices that were impacted by a configuration change.

### Network and Infrastructure Management

Even the smallest organizations around the globe have deployed multiple networking devices, servers, security systems and desktops. It becomes humanly impossible to pay attention to every warning, error and alert generated by these devices. Local analysis on each device is not practical, and even consolidation using an agent-based collection does not scale. Enterprise-wide log management can provide both agent-based and agent-less collection for logs



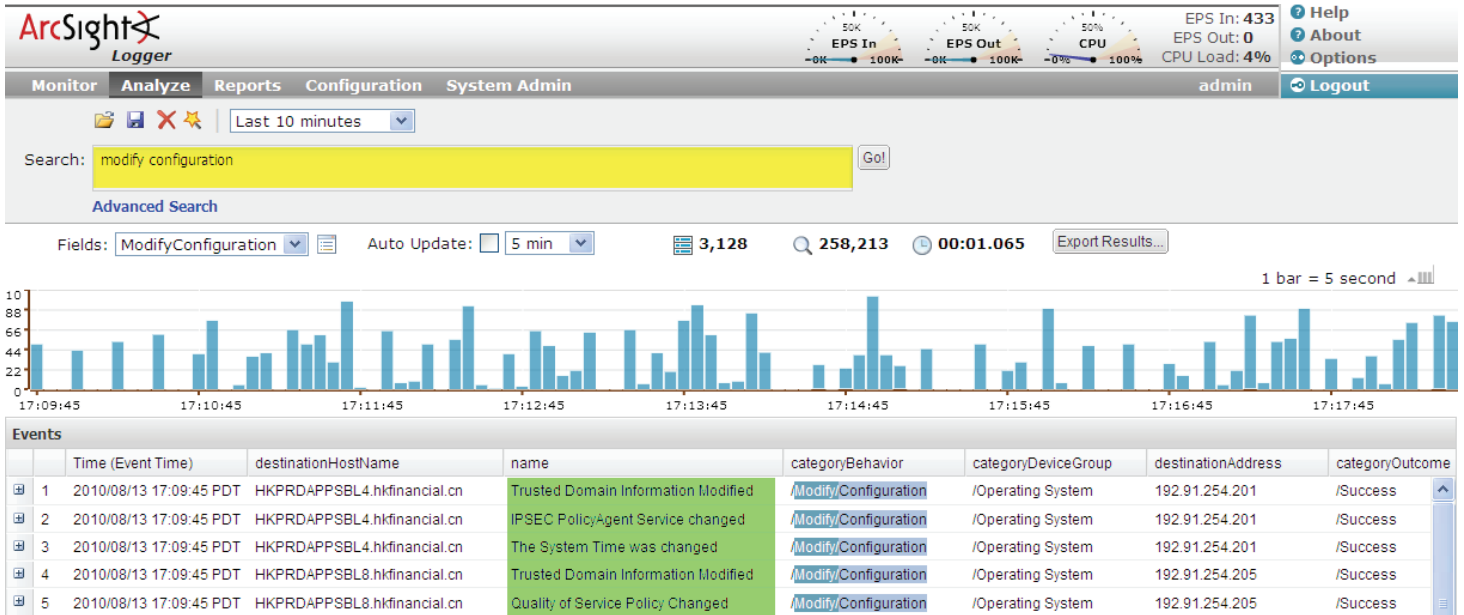


Figure 1: With ArcSight Logger, users can simply search for “modify configuration” to return all the logs from all the devices that were a result of a configuration change.

from all these devices to assist in fault, configuration, accounting, performance and security (FCAPS) issues.

### Virtualization Management

Organizations around the world are rapidly deploying virtual servers to cut down cost. Virtualization brings additional challenges to the already complex operations landscape. Plus, it is difficult to maintain and analyze silos of physical and virtual logs. Effective log management can provide a single location for combined search and analysis on all types of logs. Whether an organization is already using virtualization or preparing to begin, performance reports on CPU, memory and disk utilization can assist in better planning.

### ArcSight Logger – The Only Choice

ArcSight Logger is a Universal Log Management solution that unifies searching, reporting, alerting and analysis across any type of IT data. It consolidates silos of logs into a single indexed repository for fast detection and mitigation of operational issues. Several key differentiators make ArcSight Logger the only choice.

### Capture and Index All IT Data

ArcSight Logger collects and indexes data from any and all log generating sources, both physical and virtual. Users can choose to send raw data from any syslog or file-based log source, or use the built-in functionality of ArcSight SmartConnectors. ArcSight SmartConnectors collect, categorize and normalize log data from more than 300 distinct log generating sources. Additionally, ArcSight FlexConnector tools extend log collection capabilities to include custom sources and in-house applications.

### Data Enrichment to Simplify Analysis

ArcSight Logger leverages the ArcSight Common Event Format (CEF) that does not require familiarity with source-specific log formats – thereby avoiding the need for device- or vendor-specific analysis or knowledge (see Figure 1). All raw data sent to ArcSight Logger is fully indexed and available for fast searching and reporting via a simple Google-like search interface. Interesting search patterns can easily be converted into real-time alerts via SMTP, SNMP or syslog for fast detection and mitigation of FCAPS issues.

### Unmatched Performance

Most log management tools support fast log analysis only by compromising collection rates and storage efficiency, or by requiring more hardware. ArcSight Logger is uniquely architected to minimize that trade-off, thus enabling a single instance to capture raw logs at rates of up to 100,000 events per second, compress and store up to 42TB of log data per instance, and execute searches at millions of events per second.

### Enterprise Scalability

ArcSight Logger is available in a range of performance options, both as an appliance and as software. Deployments can range from a single instance running on a desktop, to organizations with multiple administrative domains or managed security service providers (MSSPs) deploying multiple ArcSight Logger instances in a distributed, hierarchical or peer-to-peer manner to extend capacity and performance. Role-based access controls protect both system and event data.

## Flexible Storage Options

ArcSight Logger offers multiple storage options. In addition to RAID-enabled onboard storage for appliances, both software and appliance solutions can also leverage an existing NAS, DAS or SAN investment as the data store. Regardless of whether the storage is onboard or off-board, log data is efficiently compressed at an average ratio of 10:1.

## Pre-Packaged Content

ArcSight Logger ships with built-in rules and dashboards that can be used for standard IT operation use cases around network activity, IT security, user activity, build errors, stack traces, etc. Additional content specific to regulations, such as PCI and SOX, and best practices around IT governance are available as add-on solution packages and are mapped to well-known standards, including NIST 800-53, ISO-17799 and SANS.

## Secure and Reliable Log Collection

Several audit-quality controls are built into ArcSight Logger to ensure confidentiality, integrity and availability of data. Integrity checks are enforced in accordance with the NIST 800-92 Log Management standard. ArcSight Connectors offer secure transmission, bandwidth controls, log traffic prioritization, local caching and other measures to minimize data loss and any impact on business-critical traffic.

## Bi-Directional Integration with ArcSight ESM

ArcSight Logger integrates bi-directionally with the market-leading enterprise threat and risk management offering, ArcSight ESM, and also supports ArcSight Express, an all-in-one security and compliance monitoring appliance. The integration allows ArcSight Logger to forward security events to ArcSight ESM or ArcSight Express for real-time, cross-device correlation. In turn, ArcSight ESM and ArcSight Express users can search longer-term data on ArcSight Logger using a simple click of a mouse, without switching user interfaces. ArcSight is unique in offering a tightly integrated platform for both log management and SIEM, leveraging a common collection infrastructure to ensure a low TCO and high ROI.

## Getting Started

Download, install and get instant value with ArcSight Logger at <http://www.arcsight.com/logger><sup>1</sup>. The downloadable version of ArcSight Logger provides access to all enterprise features for a full year. Using this version, organizations can collect up to 750MB of log data per day and store up to 50 GB of compressed logs. The product also comes with 90 days of phone and email support, followed by access to the ArcSight Logger user community. At anytime during the year, customers may upgrade to an enterprise version.

<sup>1</sup> For download availability in your country, please check the website.

## Highlights

- Capture and index all IT data: Raw log data collection as well as out of the box collection and data enrichment for more than 300 distinct sources
- Search and analyze anything: Centralized high performance interactive searches, comprehensive drill-down reports and real-time alerting to keep mean time to repair (MTTR) low
- Deploy and use anywhere: Available as an appliance and software, and deployable in minutes

