

UNIVERSAL LOG MANAGEMENT

HP ArcSight Logger delivers industry-leading, cost-effective management of any type of log data for all needs and use cases.

HP Enterprise Security Product Brief

HP ArcSight Logger is a universal log management solution that unifies searching, reporting, alerting and analysis across any type of enterprise log data – making it unique in its ability to collect, analyze and store massive amounts of data generated by modern networks. It supports multiple deployment options and can be installed as an appliance and as software.

The Need for a Universal Log Management Solution

Logs provide an audit trail that can be analyzed to detect and conduct detailed forensic analyses of cyberattacks, streamline regulatory audits, assist in application development and improve IT service levels. Previously, log analysis was largely asset-centric, and adoption of commercial tools was specific to an IT group and its managed assets. These solutions were designed to collect logs from specific sources and were optimized to solve a particular problem. However, these tools are inadequate to tackle the current challenges that IT teams face today.

Today, organizations face evolving security threats, the growing burden of compliance, and increased pressure to meet demanding service levels. The questions that need to be answered through log analysis are increasingly user-centric and can span any and all infrastructure. Traditional log management tools cannot be expanded to analyze logs across the enterprise because they are limited by the type of sources they can collect from; have restricted search/reporting capabilities intended to solve very specific problems; and are not scalable and breakdown under modern loads and scale.

Stretching first generation log management tools imposes significant trade-offs between log collection rates, log analysis speed and log storage efficiency. A next-generation, universal log management solution must eliminate the classic trade-off between performance and efficiency, and provide enterprise and infrastructure-wide visibility into log data. Unlike point solutions, it should be flexible enough so that it can be either used by individual teams or expanded into an enterprise-wide log management solution when needed.

ArcSight Logger – The Only Choice

Comprehensive Collection

ArcSight Logger can collect data from any and all log generating sources using out of the box functionality of ArcSight Connectors and support for raw logs from any syslog or file-based log source. ArcSight Connectors 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). Moreover, all raw data sent to ArcSight Logger is also 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 security 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, 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. Large organizations with multiple administrative domains or managed security service providers (MSSPs) can choose to deploy multiple ArcSight Logger products 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 primary 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 system content that can be used for cybersecurity, compliance, application development and IT operations monitoring. Additional content specific to regulations, such as PCI and SOX are available as add-on solution packages and are mapped to well-known standards, including NIST 800-53, ISO-17799 and SANS.

Audit-Quality Log Data

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 HP ArcSight ESM

ArcSight Logger integrates bi-directionally with the market-leading enterprise threat and risk management offering, HP ArcSight ESM, and is packaged along with ArcSight ESM into HP ArcSight Express. The integration allows ArcSight Logger to forward security events to ArcSight ESM for real-time, cross-device correlation. In turn, ArcSight ESM 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> ¹. The downloadable version of ArcSight Logger provides access to all enterprise features for a full year (see Figure 2). Using this version, organizations can collect up to 750 MB of log data per day and store up to 50 GB of compressed logs. It also comes with 90 days of phone and email support, followed by access to the ArcSight Logger user community. At anytime during the year, users may upgrade to an enterprise version.

Highlights

- Capture Everything: Raw log data as well as out of the box collection for more than 300 distinct sources
- Analyze Anything: High performance interactive searches, comprehensive drill-down reports and real-time alerting
- Use Anywhere: Uniquely architected solution to meet the needs of diverse teams and use cases around security, compliance, IT operations and application development

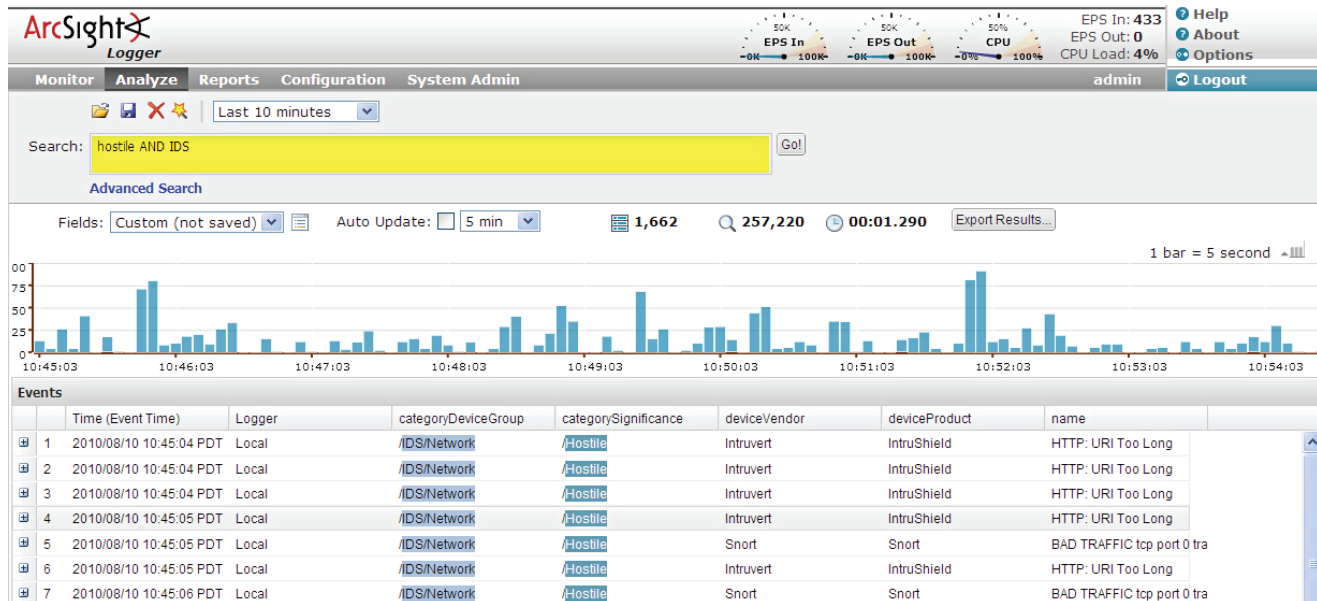


Figure 1: With ArcSight Logger, users can do a simple device- and vendor- independent search and analysis.

Functionality	ArcSight Logger (Downloadable Version – 1750MB)	ArcSight Logger (Enterprise Version)
Daily Limit on Log Data	750MB	License dependent
Total Searchable Space (Compressed)	50GB	License dependent
Distributed Search	No	Yes
Searching, Reporting and Real-Time Alerting	Yes	Yes
Granular Role-Based Access	Yes	Yes
Authentication and Authorization	Yes	Yes
ArcSight Community Support	Yes	Yes
Enterprise Support	90 days	Annual

Figure 2: ArcSight Logger Features for Downloadable and Enterprise Versions

System Requirements

Supported Operating Systems

- Redhat Enterprise Linux, version 5.4, 64-bit
- Oracle Enterprise Linux, version 5.4, 64-bit
- CentOS, version 5.4, 64-bit

CPU, Memory, Disk Space (for Small to Medium Deployments)

- CPU: 1 or 2x Intel Xeon Quad Core or equivalent
- Memory: 4-12 GB
- Disk Space: 100-120 GB

Storage

- Average compression of 10:1 (dependent on data type and data source)

Supported Browsers

- IE 7 and IE 8
- Firefox 3.0 and 3.5

¹ For download availability in your country, please check the website.

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

All other product and company names may be trademarks or registered trademarks of their respective owners.

ESP-PRB0190072710-09, Created August 2011

