Data sheet

HP Operations Log Intelligence

Collect, store, and analyze all your operations log data

Highlights

- Collect everything: Borderless collection of any data from any device in any format from log-generating sources.
- Efficient storage: HP OLI offers multiple storage options. Regardless of whether the storage is onboard or off-board, log data is efficiently compressed at an average ratio of 10:1.
- Analyze: High-performance interactive searches across all operations logs, comprehensive drill-down dashboards, and real-time alerting.
- Long-term retention of logs and events through high compression ratios with search capability.

HP Operations Log Intelligence (OLI) delivers an industry-leading, cost-effective log management solution to provide IT operations with the means to exploit all logs to solve issues faster.

What's your LogIQ?

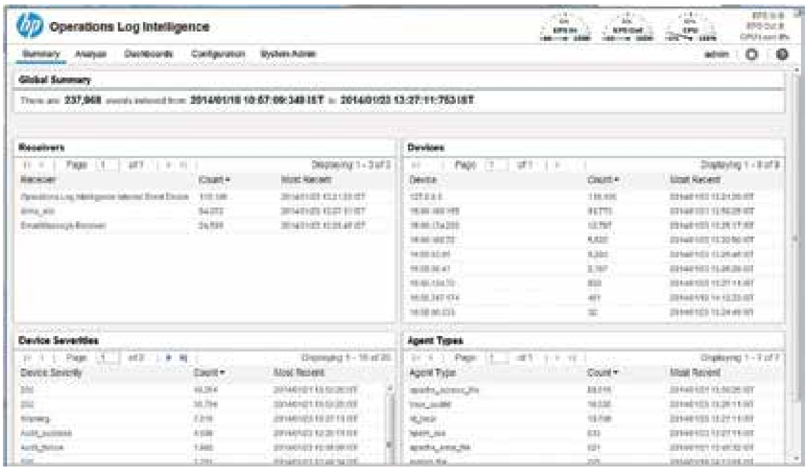
HP OLI is a log management solution to federate all your log data in a central location to facilitate and accelerate all your data searching via multiple dashboards including out-of-the-box examples particularly well suited to IT operations, alerting, and analysis across any type of enterprise log data making it unique in its ability to collect, store, and analyze massive amounts of data generated by modern IT ecosystems. It supports multiple deployments such as standalone application or in virtualized environments on virtual machines.

The need for an operations log management solution

As businesses strive for agility and competitiveness, they will increasingly exploit cloud services and create shadow IT projects without necessarily involving IT. Application developers choose from the wave of new tools and technologies integrating open source and many different emerging technologies to create differentiating business services. Users exploit more and more powerful devices used at home and later in the execution of daily business.

This context means that use of deterministic monitoring alone is no longer sufficient to govern business results. A collection of known and unknown issues arise, meaning IT requires new methods of gaining insight into issues when service delivery degrades. Even when these devices and the technologies they invoke are not covered by standard IT monitoring tools, instrumentation is typically included in all devices and technologies in the form of log data.

Figure 1. HP OLI provides a single screen summary of the operations data sources



Logs provide vital insight into the operational characteristics of IT services and the components that support them. However, this data is often overlooked or simply deleted to regain storage space. Furthermore, it is only used rarely and typically accessed by connecting to the devices that generates the log data. Some organizations have spent time to create home grown tools that federate specific data, but these empirical methods often don't scale, aren't equipped with industry-leading search capabilities, and create a maintenance issue that can be expensive.

Exploiting distributed logs is time consuming, and adoption of commercial tools is specific to an IT group and its managed assets. Such 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 where it is typically very hard or even impossible to know which data might be useful in the future. A more modern and less deterministic approach is required.

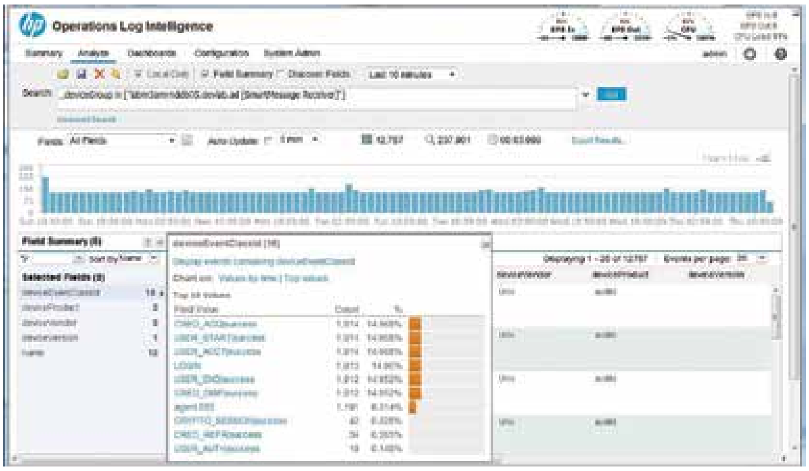
Now with HP OLI, IT operations teams can rapidly gain access to all logs from a single solution that automates the collection and archive management of all their data.
It provides industry-leading powerful search mechanisms, stores search commands for other colleagues to reuse, exploits all log data entries across all their operations log data, allowing IT operations to perform faster triage and improve IT service levels.

Improve visibility

Comprehensive collection

HP OLI collects data from log-generating sources using built-in operations focused connectors and support for raw logs from any syslog or file-based log source.

Figure 2. HP OLI provides IT operations with powerful search analysis capabilities

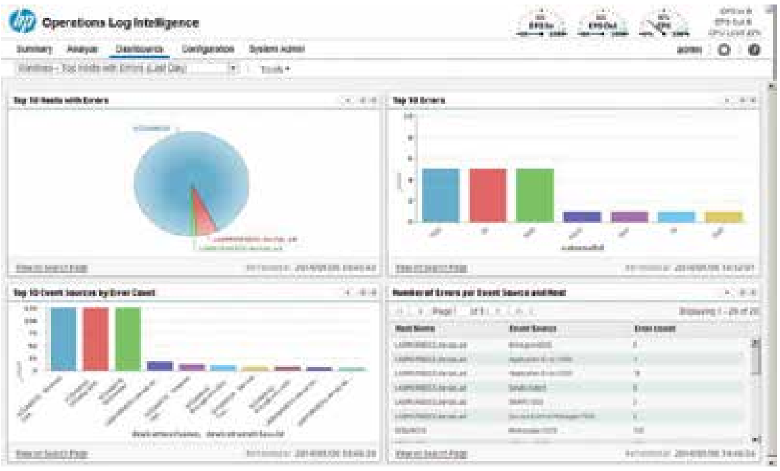


OLI connectors collect, categorize, and normalize log data from IT operations specific log-generating sources. Additionally, OLI FlexConnector tools extend log collection capabilities to include custom sources and in-house applications.

Data enrichment to simplify analysis

HP OLI leverages the ArcSight Common Event Format 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 HP OLI is also fully indexed and available for fast searching and dashboarding 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 IT operations issues.

Figure 3. HP OLI includes out-of-the-box IT operations dashboards to accelerate time to value



Features

- Centralized operations log management console
- Ease of deployment, management, and scalability
- Manage large deployments easily enabling high scalability
- Simplified configuration management through single console
- Out-of-the-box operations dashboards for Windows®, Linux, and VMware

Pre-packaged content

HP OLI ships with system content as follows:
Apache
Microsoft® AD
Microsoft DHCP
Microsoft DNS
Microsoft Exchange
Microsoft IIS
Microsoft ISA
Microsoft SQL Server
Microsoft SCOM
Microsoft Windows 2000
Microsoft Windows 2008
Microsoft Windows 2012
Squid Proxy
Sybase
Syslog (Cisco IOS, Cisco NX-OS, CiscoWorks, F5 BIG-IP, HP-UX, HP HP3, HP OpenVMS, HP Networking, SNARE, ISC BIND, ISC DHCP, Nagios, Sendmail, Sun ONE, UNIX® OS Logs)
VMware
WebLogic
WebSphere

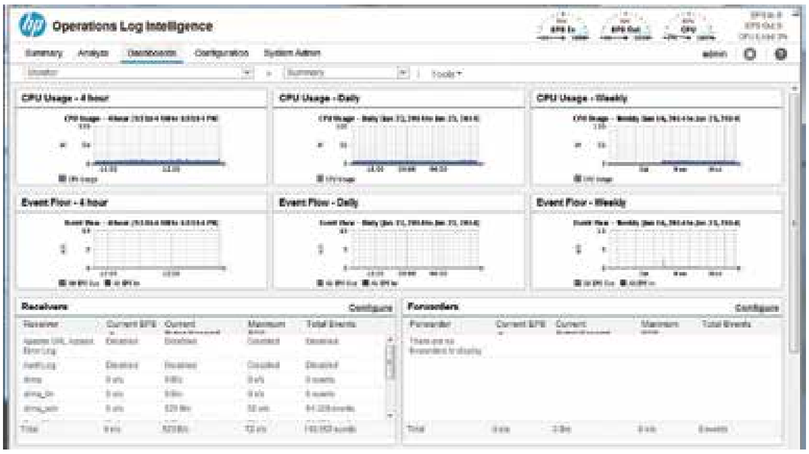
Unmatched performance

Most log management tools support fast log analysis only by compromising collection rates and storage efficiency, or by requiring more hardware. HP OLI is uniquely architected to overcome 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 42 TB of log data, and execute searches at millions of events per second.

Enterprise scalability

Large organizations with multiple administrative domains or managed security service providers can choose to deploy multiple HP OLI 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.

Figure 4. Custom dashboards are quick and easy to configure and use



Audit-quality log data

Several audit-quality controls are built into HP OLI 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.

Integration with HP and third-party IT operations management

OLI ships with connectors developed specifically to integrate with popular IT management tools. This includes connectors for HP software products such as OMi, OM, NNMi, and Service Manager, offering Device Event Mapping to ArcSight Data Fields, and certificate-based connectivity control. Integrations with Service Manager, OMi, and OM feature bidirectional communication of events. A variety of SNMP traps and network topology data are supported with NNMi.

HP OLI specifications (software)

Software generic spec	
Supported OS	Red Hat® Enterprise Linux v6.2, 64-bit Oracle Enterprise Linux, v6.1, 64-bit CentOS, v6.2, 64-bit Hyper-V on Windows Server 2008 R2, 64-bit VMware virtual image
Recommended minimum hardware	CPU: 1 or 2X Intel® Xeon® Quad Core or equivalent memory: 4–12 GB; Disk space: 4–12 GB
Storage	Average compression of 10:1 (dependent on data type and data source)

About HP Big Data Analytics for IT operations

HP is a leading provider of business service management software, details of which are available at hp.com/go/bsm. Analytics products now include:

- HP OLI providing Collect, Store, and Analyze for centralized log management.
- HP Operations Analytics a Big Data Analytics for IT operations solution providing a Prepare, Predict, and Pinpoint value proposition powered by HP Vertica and ArcSight Logger. More details can be found at hp.com/go/opsanalytics.

Get the support you need

HP Software Professional Services take a holistic approach to qualifying your requirements, your existing ecosystems, regulations and processes, to define an optimal implementation tailored to your time constraints, skills, and compliant with your operational processes as proven in projects successfully implemented for the needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized solution architects and consultants. Learn more about HP Software Professional Services at hp.com/go/software.

Learn more at
hp.com/go/opsanalytics

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-1241ENN, March 2014