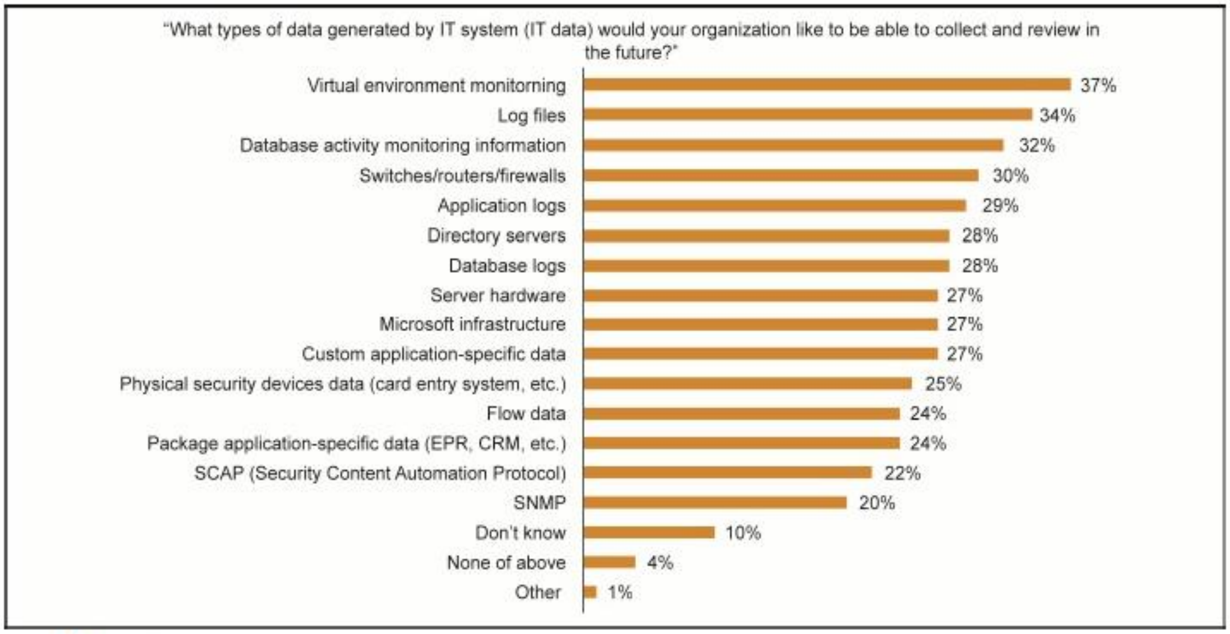
CloudFabrix

Extracting Hidden Insights with Log Analysis Using AI/ML

Log Management Challenges

Effective Log Management is a common challenge for many IT organizations and this is due to ever expanding complexity and dynamic nature of IT logs. The logs are generally spread out in many different systems, and are of many different formats (structured and unstructured) and generated at high velocity, making it difficult to analyze the logs.

A recent study from Forrester consulting highlights the widespread nature and complexity of this problem, where IT organizations want to capture and analyze log data from at least 20+ different systems and functional domains.



KÜRT

Further, IT teams are not able to reconcile the logs to gain insights into performance or security issues. In regulated environments, logs must be accessible anytime and also stored for several years for compliance reasons. All of this makes log management a challenging task for IT.

- Volume, variety and velocity of log data
- Logs from many disparate sources
- Unable to extract actionable insights from logs
- Unable to detect security threats easily. Compliance/ Audit Risks
- Stringent short-term and long-term log archival requirements
- Security risks, multi-tenancy and role based access support

Effective Log and Event Monitoring & Analytics is becoming an essential IT operations practice

An effective log and event monitoring & analytics solution enables IT teams to identify performance blind spots, detect abnormal usage patterns, establish top talkers, chatty applications or perform forensic and threat analysis. The solution should also have the ability to detect issues and patterns automatically based on trends and abnormalities, rather than using static rules and regex patterns.

Modern log management and analytics solution should encompass the following key capabilities:

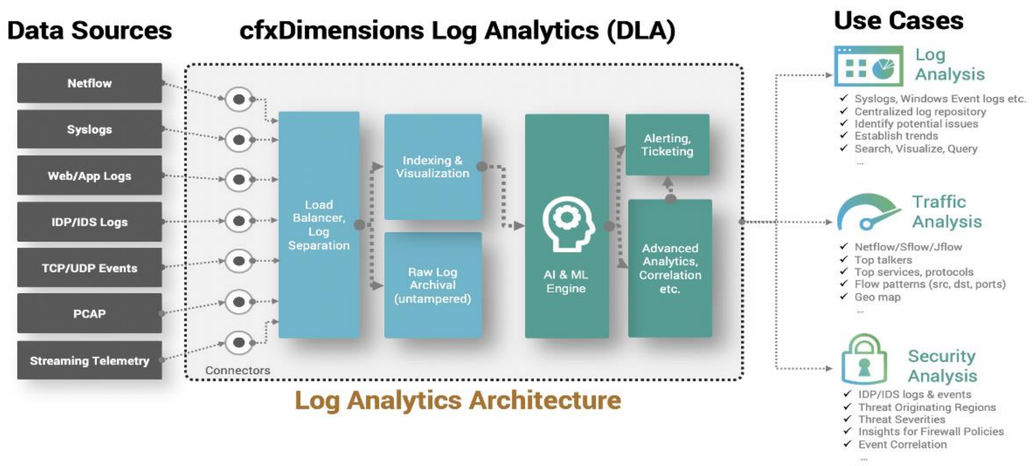
- **AI/ML:** Leverage AI/ML capabilities to learn trends / patterns and automatically identify potential errors and anomalous behaviors
- **Scalability:** Handle huge volumes and variety logs:
- **Centralized:** Should be Centralized, preferably operate in SaaS environment
- **Multi-Tenant:** Should provide secure multi-tenancy & isolation for shared environments
- **Analytics:** Should have built-in analytics and visualizations for standard data sources
- **Intelligent Alerting:** Advanced alerting capability to alert on anomalous patterns, instead of static rules
- **Data Ingestion:** Support hundreds of data sources with readily available connectors or plugins
- **Raw Data Export:** Should provide raw log/event data export in addition to indexed data
- **Long term archival:** Should support raw, untampered and unaltered log archival for regulated environments
- **Extensible:** Extensible to support new data sources with ease of use and community support

CloudFabrix Solution

cfxDLA is the centralized log management solution that can be deployed on-prem or used as a service through CloudFabrix SaaS portal. The solution ingests logs from multiple tools and enables IT teams with advanced analytics and insights. The solution also leverages AI & ML capabilities to perform event correlation, failure root cause detection and event categorization. Log and event data can be ingested from any managed asset using readily available connectors or plugins. Remote or on-premises environments can use cfxCollector as a proxy between customer environment and cfxDLA.

The solution focuses on 3 key areas:

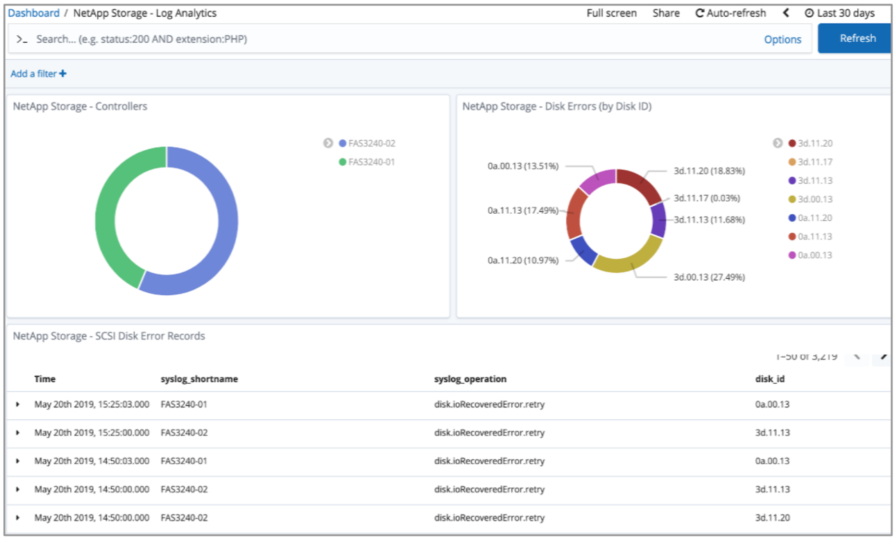
- **Log Analysis**
- **Traffic Analysis**
- **Security Analysis**


Data Sources
cfxDimensions Log Analytics (DLA)
Use Cases
Netflow
Syslogs
Web/App Logs
IDP/IDS Logs
TCP/UDP Events
PCAP
Streaming Telemetry
Connectors
Load Balancer, Log Separation
Indexing & Visualization
Raw Log Archival (untampered)
AI & ML Engine
Alerting, Ticketing
Advanced Analytics, Correlation etc.
Log Analysis
✓ Syslogs, Windows Event logs etc.
✓ Centralized log repository
✓ Identify potential issues
✓ Establish trends
✓ Search, Visualize, Query
...
Traffic Analysis
✓ Netflow/Sflow/Jflow
✓ Top talkers
✓ Top services, protocols
✓ Flow patterns (src, dst, ports)
✓ Geo map
...
Security Analysis
✓ IDP/IDS logs & events
✓ Threat Originating Regions
✓ Threat Severities
✓ Insights for Firewall Policies
✓ Event Correlation
...
Log Analytics Architecture

Log Analysis

IT teams can ingest logs from any managed IT asset, index and archive logs, and get summary analytics, advanced visualization and reporting. Typical logs include Syslogs, Web logs, Application logs, User Activity logs etc.

The app also supports long-term archival of untampered, unaltered logs that may be required for regulated environments for compliance and audit purposes. Archived logs can be organized based on customer desired structure (ex: Datacenter/Date/Hour) and can also be accessed on-demand from portal anytime for download and offline review.



NetApp Storage - SCSI Disk Error Records

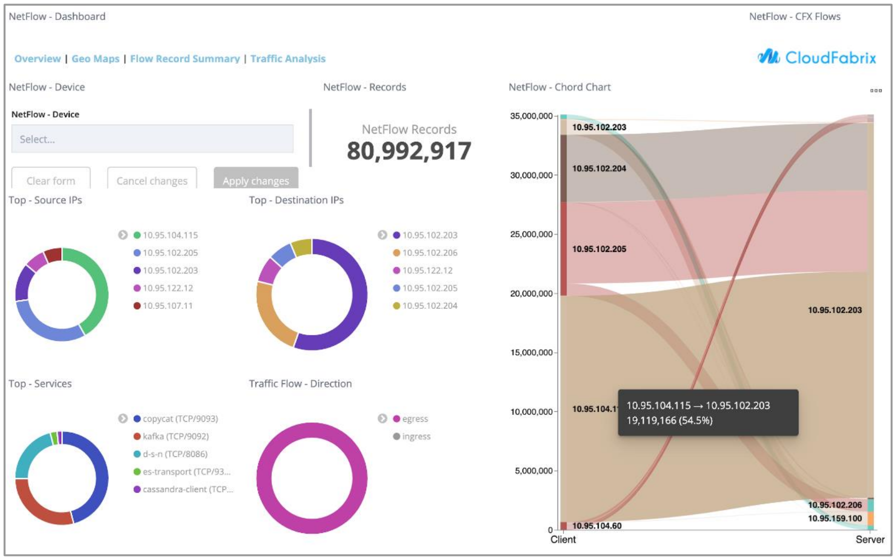
1–50 of 3,219

Time	syslog_shortname	syslog_operation	disk_id
May 20th 2019, 15:25:03.000	FAS3240-01	disk.ioRecoveredError.retry	0a.00.13
May 20th 2019, 15:25:00.000	FAS3240-02	disk.ioRecoveredError.retry	3d.11.13
May 20th 2019, 14:50:03.000	FAS3240-01	disk.ioRecoveredError.retry	0a.00.13
May 20th 2019, 14:50:00.000	FAS3240-02	disk.ioRecoveredError.retry	3d.11.13
May 20th 2019, 14:50:00.000	FAS3240-02	disk.ioRecoveredError.retry	3d.11.20

Traffic Analysis

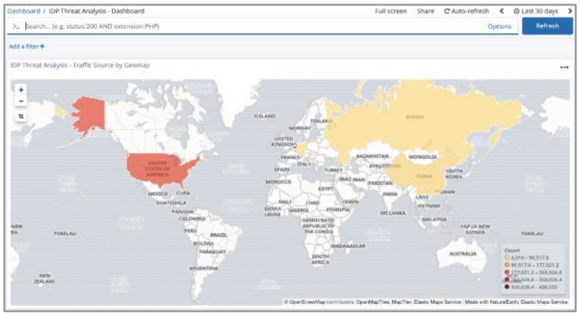
Traffic analysis is vital to any Network operations team. cfxDLA can ingest Netflow records, flow logs, SIP call logs, packet captures, from various network devices to provide insights about traffic usage patterns, top talkers, noisy neighbors and top services, ports or protocols.

An intuitive chord diagram widget maps out flow pattern between various sources and destinations. Network admins can also drill-down to particular device or interface and gain deeper insights about traffic patterns. Customers can perform basic and advanced search queries or retrieve raw flow records.



Security Analysis

Security information and event management (SIEM) is an essential practice of every security organization. Within the broader SIEM practice, security event management is a key aspect that enables customers to analyze or detect breaches or vulnerabilities based on logs and events collected from firewalls, IDP, IDS and other perimeter or east-west firewall devices.



With cfxDLA, customers can ingest IDP, IDS logs from various network endpoints and gain insights into hidden security patterns. Portal shows a geomap view of threat originating regions. Suspicious traffic patterns or threats are also aggregated and categorized based on severity. Top traffic originating internal systems can also be easily identified. Suspicious hosts can be selected for further drill down and analysis.

Key Benefits:

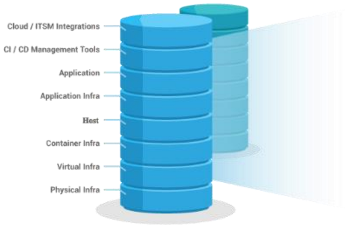
cfxDLA solution provides significant benefits to IT organizations in strengthening their IT operations practice by providing a highly scalable and secure multi-tenant solution to collect, analyze and archive wide variety of logs and events.

- Centralized logging, indexing and analytics
- Advanced search, visualization and dashboards
- Intrusion detection and analysis from IDP/IDS logs
- Untampered, unaltered logs for regulatory compliance
- Periodic and On-demand reports/archive file generation

Key capabilities:

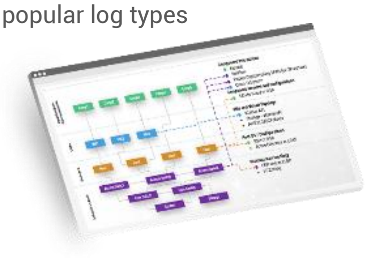
Ingest Logs, Events from Any Data Source:

- Using hundreds of available connectors
- Connect on-premises or remote environments
- Structured and Unstructured Data



Analytics & Machine Learning:

- Predefined visualization for popular log types
- Event correlation, root cause analysis
- Intelligent Alerting based on Anomaly detection



Security & Multi-tenancy:

- Enables hardening of security policy/firewall
- Isolation & log separation for multiple tenants
- Highly scalable supporting millions of logs

Enterprise Integrations & Extensibility:

- Integrations with ITSM tools like ServiceNow, Remedy, Jira, FreshDesk etc.
- Single Sign-On (SSO) support
- Extensible to support new data sources

Use Case Examples

Log Analysis	Traffic Analysis	Security Analysis
SysLog Analysis • Syslogs from Linux hosts • Syslogs from Windows hosts using Winlogbeat	NetFlow Analysis • Flows from switches, routers • sFlow, jFlow, IPFIX etc. • AWS VPC flow logs	Threat Analysis • IDP/IDS log analysis • Security event analysis • Insights for Firewall hardening

© Copyright 2015-2019