Conflux

Description

Conflux is an LMaaS (Log Management as a Service) module offered as part of the Cloudaware platform. Conflux discovers, enhances and aggregates logs from cloud providers such as AWS, Azure and GCP. Besides standard log management functionality such as search and visualization, Conflux provides enhanced capabilities including security, monitoring, alerting, reporting, anomaly detection and forecasting.

Key Features

- Automatically discovers new logging data sources
- Decorates event data with CMDB data such as tags
- Secure API to endpoints for customers to feed custom logs, e.g. application logs, machine syslogs, etc
- Provides complete visibility across all infrastructure tiers:
  - Cloud, e.g. CloudTrail
  - Network, e.g. VPC Flow Logs
  - Operating System, e.g. Syslog
- Analyzes network logs to discover relationships
- Leverages Machine Learning to detect anomalies and perform forecasting
- Long term data retention (up to 7 years)

Competitors and Key Differentiators

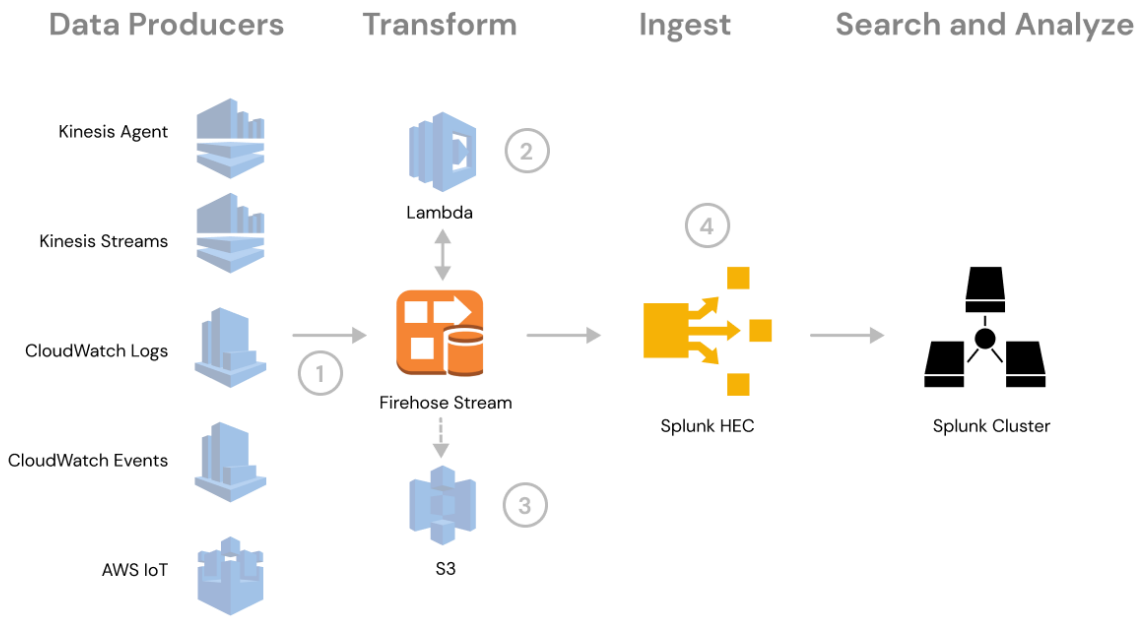
- Conflux competes primarily with products like:
    - Sumo Logic
    - Splunk
    - Graylog
    - Loggly

- Key Differentiators:
    - Discovers new log sources, such as buckets and API endpoints, automatically without depending on human input
    - Decorates event data with cloud provider tags
    - Automatically archives older data into less expensive storage, resulting in a lower cost of ownership
    - Uses Open Standard "Lucene" and "Elasticsearch" query languages
    - Advanced capabilities, such as anomaly detection and forecasting without extra cost

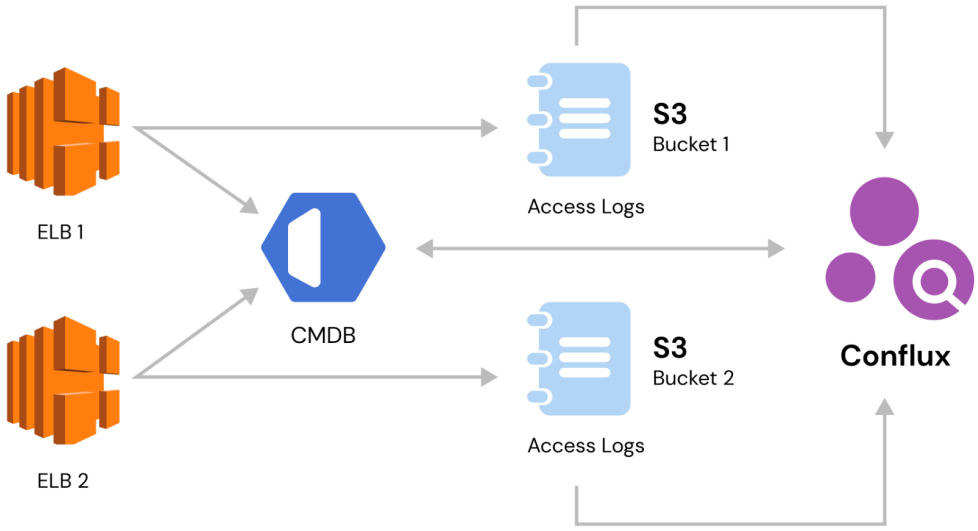
Automatic Log Discovery

Whenever a user creates new objects - e.g. AWS Load Balancers, S3 Buckets and RDS Databases - the cloud provider requests the user to provide a destination logging location, like a bucket or BigQuery table. This flexibility is great, but large cloud consumers end up with hundreds of locations for log storage. This often results in fragmented data.

Traditional vendors, like Splunk and Sumo, rely on customers to configure "push" pipelines. However, as the number of cloud services and application components that generate logging data increases, they often have missing or incomplete data. Another key problem with the traditional "push" approach is that it requires manual action. See step 1.



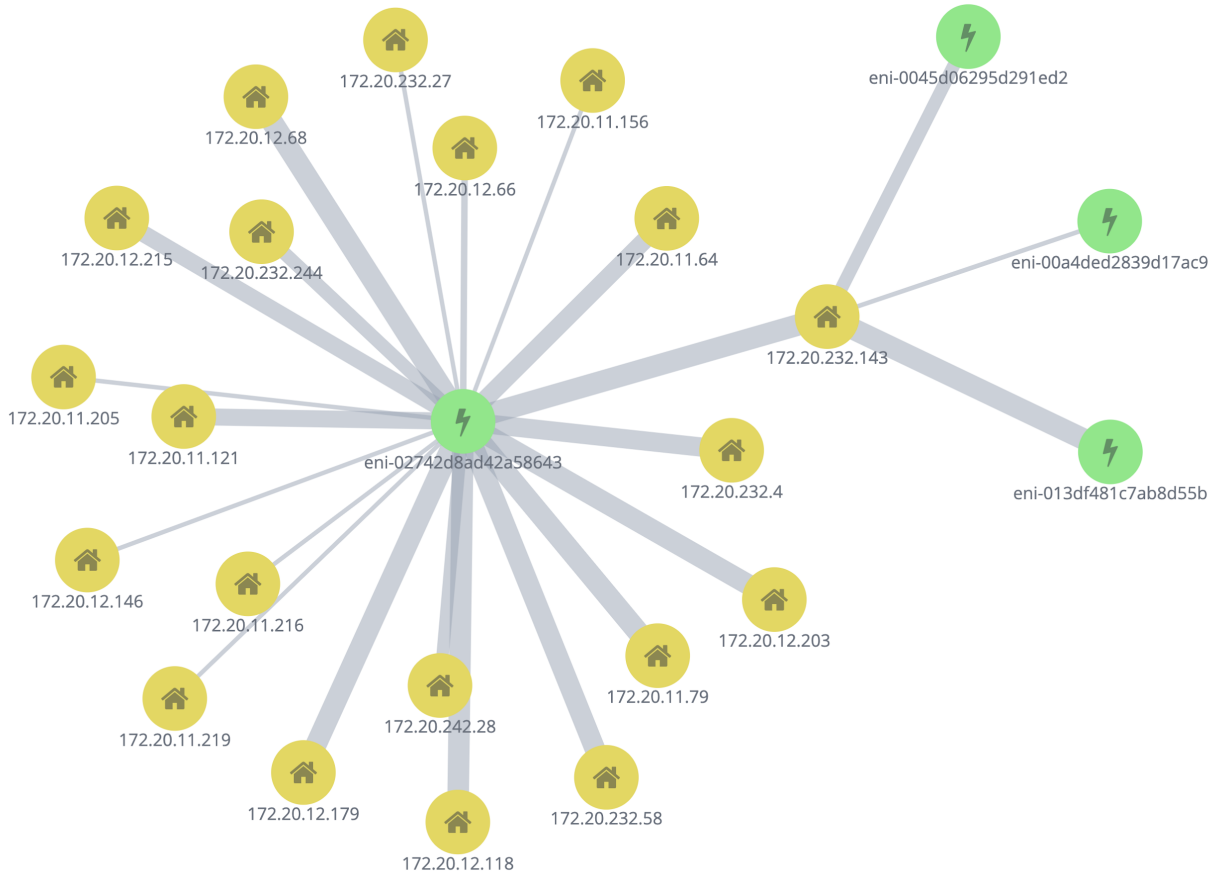
Conflux takes a different approach. Instead of relying on users to manually push logs into a log management solution, it relies on CMDB to discover log sources and notify Conflux.



This approach based on automated discovery eliminates the need for manual configurations and reduces the possibility of missing log data.

Graph API and Automated Relationship Detection

Conflux analyzes network, spending and security logs to identify relationships and dependencies between objects in CMDB. Using Graph API, users can perform an in-depth impact analysis necessary in security, availability and disaster recovery use cases.

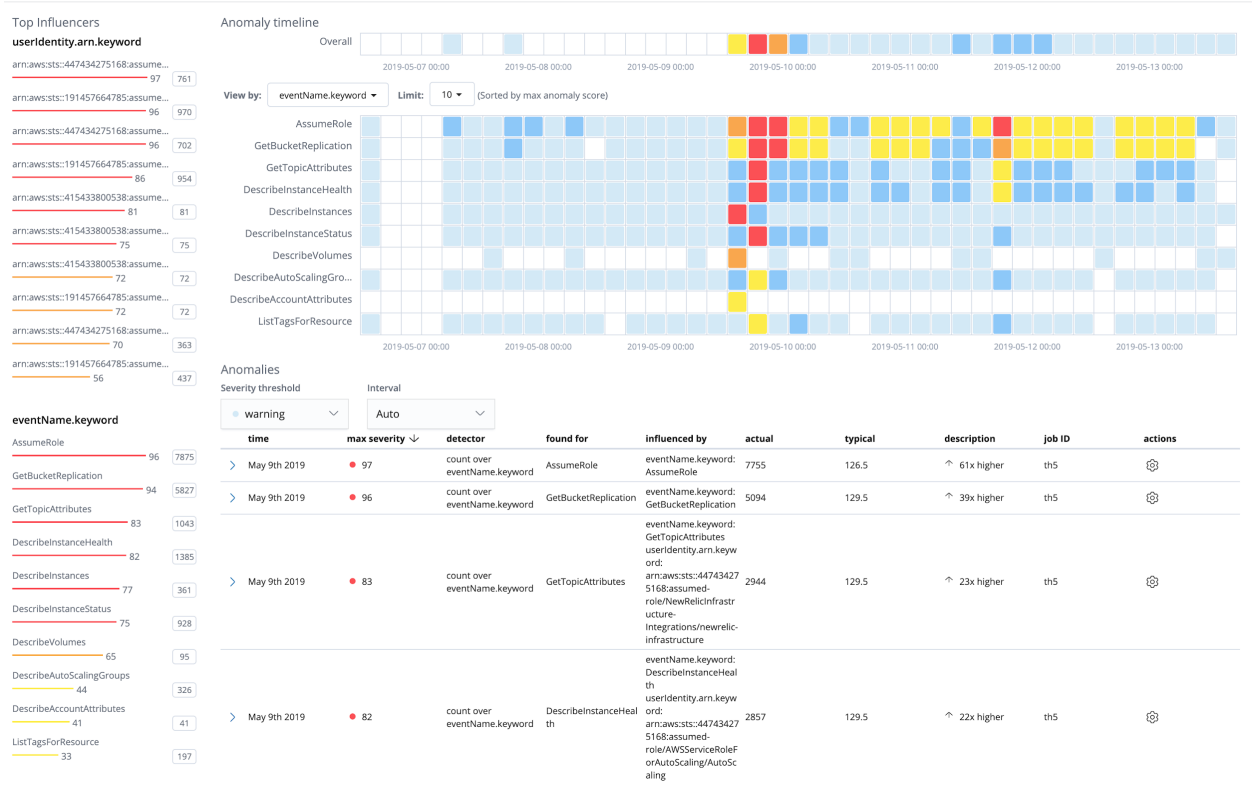


cloudaware

Anomaly Detection

Conflux offers three types of anomaly detection for all of its data:

- Single Metrics - detect anomalies in single time series, e.g. Total Spending By Day
- Multi-Metrics - detect anomalies across multiple time series, e.g. CPU
- Network Traffic by Instance and Population - detect activity that is unusual compared to the behavior of the population, e.g. console users' logins.



cloudaware

Auto Discovered Log Sources

Provider	Log
AWS	ALB Access Logs
AWS	AWS Config
AWS	Billing Cost Allocation, DBR and CUR
AWS	CloudFront
AWS	CloudTrail
AWS	ELB Access Logs
AWS	EKS Logs
AWS	RDS Logs
AWS	Route53 Logs
AWS	S3 Access Logs
AWS	VPC Flow Logs
AWS	WAF Logs
GCP	GCP Billing Data
GCP	Google Audit Logs
Azure	Azure Activity Logs
Azure	Azure Billing Data
Azure	Azure Flow Logs
Operating System	Metric Beat
Operating System	File Beat
Operating System	Winlogbeat
Operating System	Packetbeat

Custom Push Via Syslog	Any custom log file
Custom Pull Via Breeze/LogBeat	Any custom log file

Supported Alert Mechanisms

- Email
- Webhook (Generic, PagerDuty, Slack, JIRA, Cloudaware)
- SNS

Reliability and Scalability

Conflux is a highly redundant service with data replicated across multiple cloud providers and regions. Customers can request specific data center locations such as US Only, EU Only, etc.

cloudaware

Security

Granular Access and Audit Controls

Role-based access and audit controls allow you to control and monitor the actions your Conflux users can take, and what data, tools and dashboards they can access.

User Authentication

Conflux supports SAML integration for single sign-on (SSO) via SAML v2 compliant identity providers including Okta, PingFederate, Azure AD, ADFS, CA SiteMinder, OneLogin, Centrify, SecureAuth, IdentityNow, Oracle OpenSSO, Google SAML2 provider and Optimal Id. Conflux can also integrate with other authentication systems, such as LDAP, Active Directory and e-Directory.

Data Encryption In-Transit and At-Rest

Conflux uses industry-standard SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption for data in transit. All forwarders and user sessions are secured in this manner. Electronic messaging is secured by opportunistic TLS encryption on the email gateways.

Conflux encrypts data at rest using Advanced Encryption Standard (AES) 256-bit encryption.

Environment Segmentation

Conflux deployments run in a compartmentalized secure environment, and your data exists on virtually dedicated servers to ensure it remains isolated from other customers' data.