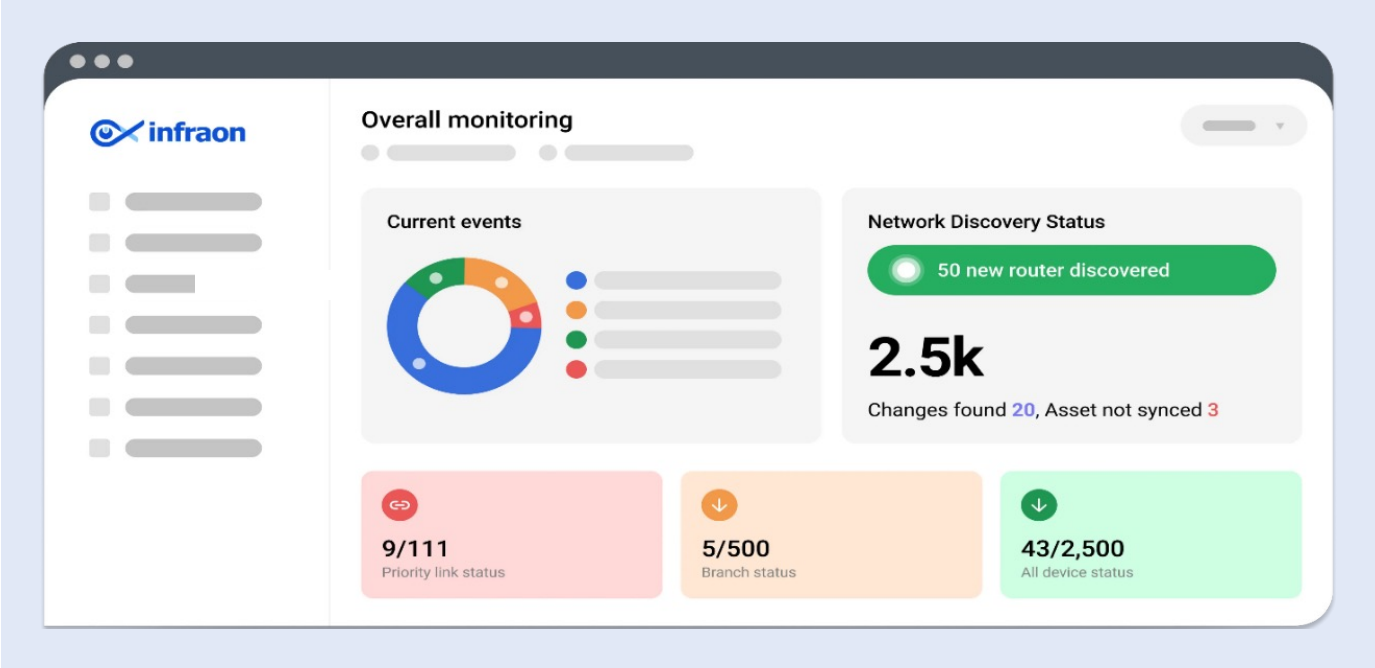
Data Sheet

Infraon Log Management

Comprehensive visibility into enterprise data

Overview

The Infraon Log Management tool helps you reduce downtime and move from reactive to proactive monitoring with advanced analytics powered by a robust platform. From behind a single pane of glass, you can gain comprehensive visibility into enterprise data across on-premises and cloud-based environments.



Key Highlights

- Centralized log management & analytics
- Powerful & fast search for your logs
- Smart alerts on any log stream
- Find application performance issues faster

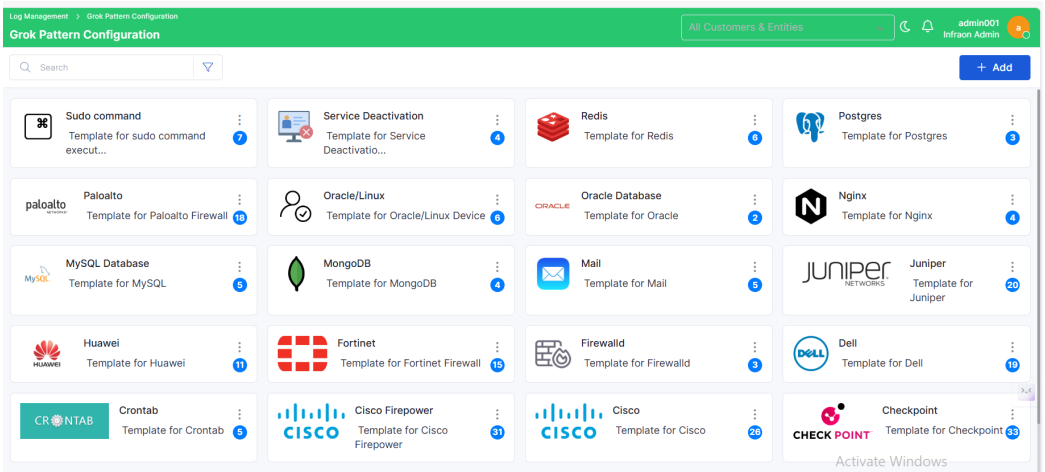
Infraon Log Management Datasheet

Key Capabilities

- Scalability & high availability with clustering of nodes. A Node can be added at any point in time and is horizontally scalable.
- Auto load balancing between nodes.
- Capable of processing 15,000+ events per second and is horizontally scalable to handle higher loads.
- Configurable Log retention duration per type of log.
- Log retention on a tiered approach for Storage Cost Optimization.
- Automated backup and Archival processes.
- All communications to the log store will be on SSL/TLS, ensuring security.
- System employs a compression mechanism that achieves a log index storage reduction ratio of 8:1 or higher, delivering significant cost optimization.
- Possesses robust enrichment options for the collected raw logs, turning them into valuable information.
- Transformation options span “append, convert, date, dissect, drop, fail, grok, join, remove, set, split, sort, trim, and more.
- Log store supports multiple types: textual, structured, unstructured, numerical, and geo points.
- Can perform a full text search across all the documents and store collections with automated indexing to offer fast search results.
- Query engine to acquire the exact logs to be filtered and stored for future reference and audits

Log Collection

- System supports log collection using Syslog-NG (extendable to any syslog format), native Linux agents, native Windows agents, along with agentless connectors via PowerShell and SSH
- Ready-made parser for most standard networking devices, servers & applications.
- Easily adaptable for all new sources and in-house developed applications.
- Supports most cloud environments such as Azure, AWS, and GCP.
- Collects, Parses, and transforms the logs on the fly and at scale.
- Parses structured and unstructured data to transform them into a standard format for detailed analysis and deeper insights.
- Enriches the data with DNS lookup, Geo information, Hashing, Translation, and truncation to make it more meaningful.
- Supports multiple downstream for analytics, auditing, raw data compliance, forensic purposes, etc.
- Supports clustering environment for scale and availability.
- Uses Persistent Queues for guaranteed processing of collected logs.
- De-duplicates across the collectors.
- Agent-based for servers and applications, which converts into a standard format and transfers the logs.
- Readymade agents for applications - Containers, Cloud providers, streaming engines, web apps, databases, etc.
- Agents perform auto-load balancing across the collectors.



Infraon Log Management Datasheet

Infraon Log Management combines the power of metrics, logs, user monitoring and alerts, allowing you to cut troubleshooting time in half.

Log Management Main Features

- Log Collection with centralized Log Aggregation
- Log Archival and Retention for an extended period of time
- Log Analysis
- Log Retention

Key Features

- Rules
- Log Search
- Widgets
- Alarm Events
- Alarm Dashboard
- Log Archival
- Log Reports
- Schedule Reports
- Notification Config
- Index Config
- Monitoring

Log Dashboard

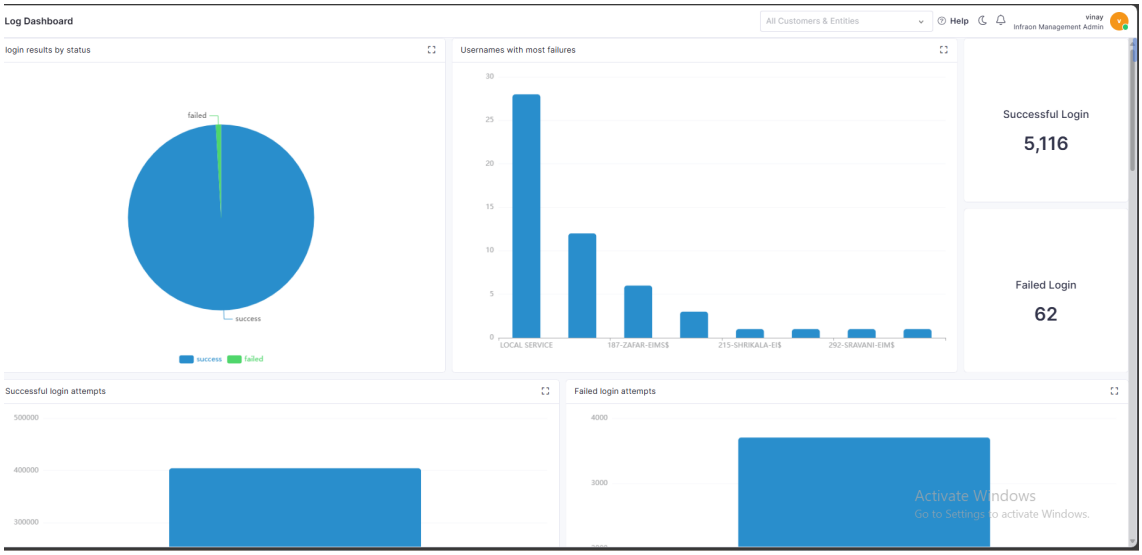
- Easy to understand, graphical view of logs
- Enables the user to identify issues easily.
- Customizable with option to add multiple widgets and tabs, as required.
- Pre-configured dashboards.
- View, edit, and delete

Alarm Dashboard

- Consolidated list of alarms in a dashboard view.
- Filter by
    - Host Name
    - Rule Name.
    - Fields
    - Time Stamp
- Displays the count of events matched.
- Duplicate alarm, alert count, and information.
- Download reports in PDF, CSV, or Excel.

Index Management

Indices are tags used to group similar logs and can be applied across archival, rules, reports, and search operations.



Infraon Log Management Datasheet

Reports

- Provides a detailed graphical understanding of logs.
- View the log rate based on the selected time.
- Customizable Reports
- Preconfigured Reports for compliance purposes.

Log Archival and Scheduled Archival

- Allows download of Log Data from the Elasticsearch server.
- Can be stored in the local machine for auditing and compliance.
- Archived based on Indices, Tag Value match and/or Time.
- Choice in the Download File Type.
- Create a Schedule to archive Logs, periodically.
- Add, edit and delete schedules, based on the requirement.
- Enable/Disable option for the schedule.

Rules

- Pre-defined scenarios, which trigger Alarms, Events, etc.,
- Robust rule engine supports multiple options
- Each rule defines
    - Query to perform
    - Parameters for a rule match
    - List of alarms/alerts to be raised.
- Configurable to raise alarms or mail/SMS notifications.
- Comes with pre-configured rules.

Notifications

- Email
- Twilio
- Slack
- SMS

Rule Types

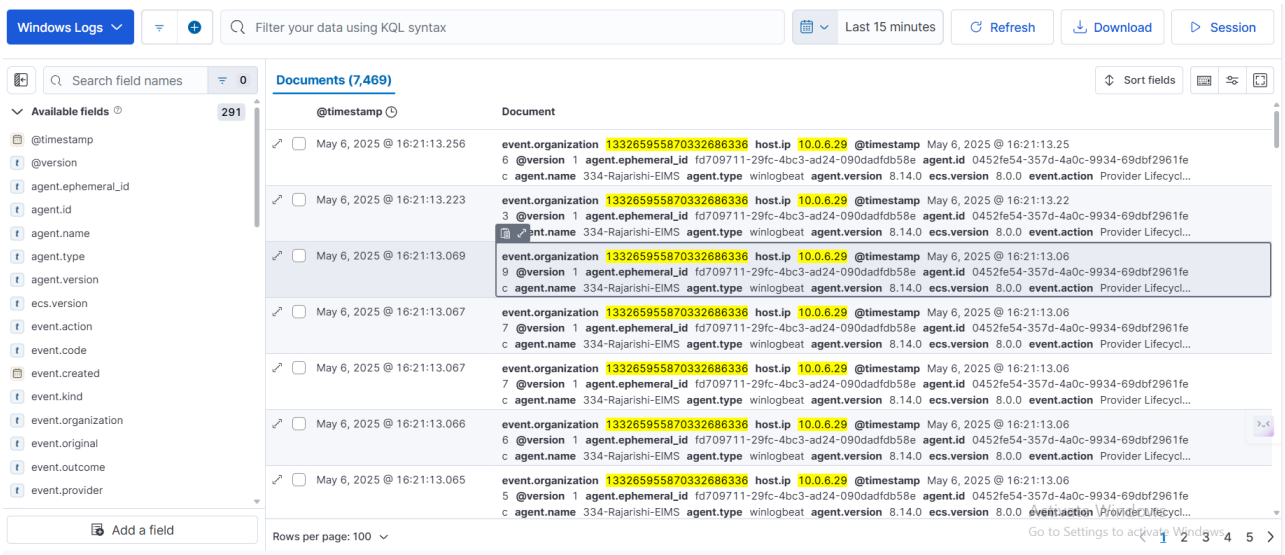
- Blacklist
- Whitelist
- Change
- Frequency
- New Term

Rule Filters Used:

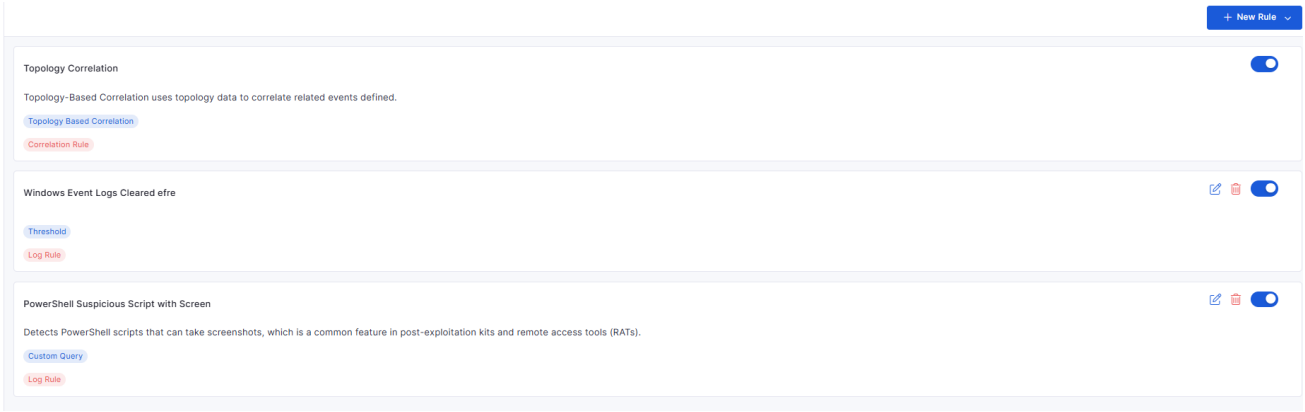
- Query String
- Term
- Wildcard
- Range

Log Search

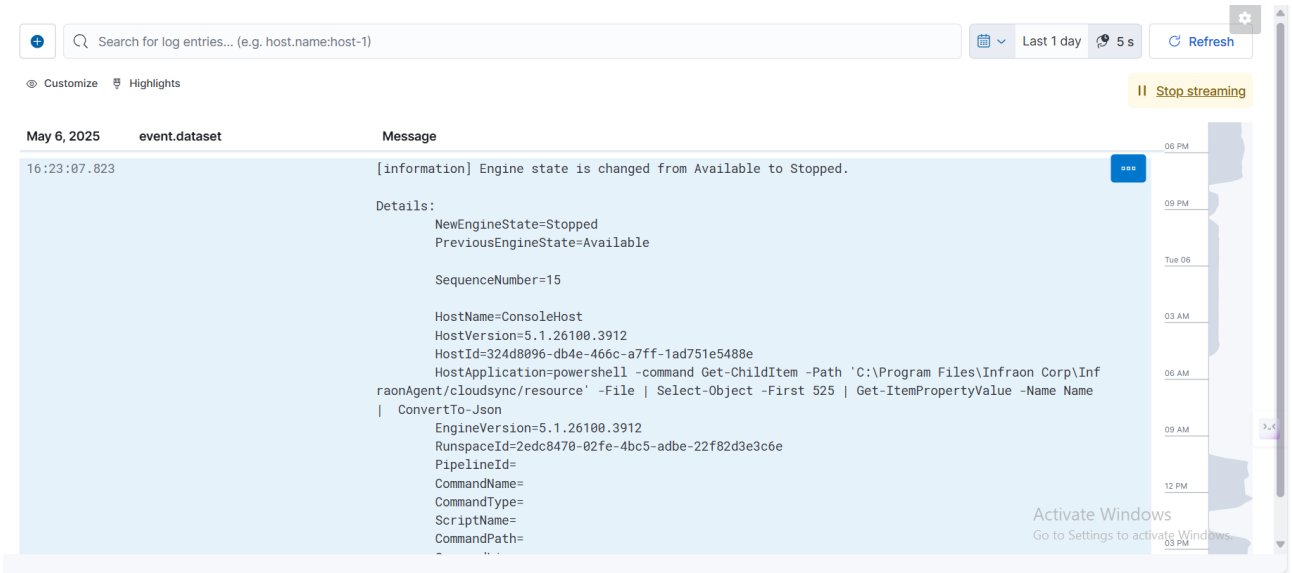
- Multiple filters available
    - By the values.
    - By the timestamp.
    - By the indices.
- Auto reload of logs.
- Around 10000 log entries readily accessible.



- Rules engine comes with default sets to ensure rapid use of the alerts out of the box.
- Rules engine allows the user to add N number of rules further based on the need in their environment.
- Offers Easy options to create, modify, import, and export to acquire defined rules across the board easily.
- Rules supported with,
    - Blacklist – when it discover black listed values in the any of the field
    - Whitelist – when it finds whitelisted or other than the mentioned set of items in any field.
    - Change – when it finds that the specific field values have been changed from the default set.
    - Frequency – when the count of the specific log fields received is more than the specified number in a specific duration
    - New Term – when it finds the field's value is something new that has not yet occurred.
    - Threshold – when suddenly the rate reduces or breaches specified levels.
    - Match – one or more fields match certain conditions, or the string pattern match occurred in the collected logs.
- Based on one or more rule matches, the system will generate user-defined alarms and relevant notifications will be triggered
- Alarms will be viewed in central dashboards along with monitoring fault and performance alarms dashboards



Log Stream View



About EverestIMS Technologies

EverestIMS Technologies Ltd. (Everest) is a leading software company – offering ITOM, AIOps, and Telecom OSS solutions. Backed with rich market experience in the I&O, AI, IoT, and digital transformation space, Everest has widespread global footprints through its focused product portfolio. We provide integrated IT solutions, operations, and infrastructure to empower corporations, enterprises, and telecoms to deliver future-ready services to end users. We aim to ensure they adapt and stay competitive in evolving digital landscapes.

Certifications: ISO 20000-1:2018, ISO 9001:2015, ISO/IEC 27034-1:2011, ISO/IEC 27001:2013,ISO 55000:2024, ISO 45001:2018 OWASP, SOC II.

Navigate here for more details about us: www.everestims.com

300+
Enterprise Customers

1M+
Interfaces Monitored

5M+
Assets Monitored

100+
Vendors Supported

Reach Us

Phone
+91 80 4656 7100

Email
sales@everestims.com

Web
www.everestims.com

Address

Sree Gururaya Mansion, SN 1, No 759, 8th Main Rd, South Wing, KSRTC Layout 3rd Phase, J. P. Nagar, Bengaluru, 560 078. Karnataka, India

ITIL PRACTICES 9 ACCREDITED TOOL VENDOR Infraon Infinity 7 Silver by PeopleCert

PinkVERIFY® Certified 14 PROCESSES