SRS (Software Requirement Specification)
Log Management Platform

Version: 1.0 **Date:** 2026-01-17

1. Introduction

1.1 Purpose: This document specifies the requirements for a Log Management Platform that collects, stores, searches, analyzes, and monitors logs from multiple sources for operational troubleshooting and security monitoring.

1.2 Scope: The platform will ingest logs from servers, applications, containers, cloud services, and network/security devices; normalize them; store them reliably; and provide dashboards, alerting, reporting, and audit support.

1.3 Intended Audience: Product owners, developers, DevOps/SRE teams, SOC analysts, auditors, and QA/testers.

1.4 Definitions & Acronyms

Term	Meaning
Log Event	A single record of an action/state change generated by a system or application.
Ingestion	Process of receiving logs and storing them into the platform.
Normalization	Converting various log formats into a common schema/fields.
RBAC	Role-Based Access Control.
Retention	Duration for which logs remain searchable before deletion/archival.
SIEM	Security Information and Event Management (optional integration).

2. Overall Description

2.1 Product Perspective: A centralized on-prem or cloud platform acting as a single place for all logs. It includes agents/collectors, an ingestion pipeline, storage/indexing, search UI, dashboards, and alerting.

2.2 User Roles: Admin, Security Analyst (SOC), DevOps/SRE, Auditor/Compliance, Viewer.

Role	Typical Work
Admin	Manage users, sources, retention policies, integrations, system configuration.
Security Analyst	Threat hunting, detection, investigations, alert tuning.
DevOps/SRE	Debug errors, track incidents, monitor services via logs.
Auditor	Review access, verify retention, generate compliance evidence.
Viewer	Read-only dashboards and searches.

2.3 Assumptions & Dependencies

- Time synchronization (NTP) is enabled on sources.
- Connectivity exists between collectors and platform.
- Storage capacity depends on ingestion rate and retention.

3. External Interface Requirements

3.1 User Interface: Web-based UI with dashboard, search page, alert rule builder, and admin console.

3.2 Software Interfaces:

Interface	Description
Syslog (UDP/TCP)	RFC3164/RFC5424 syslog receiver (TLS optional).
Agent/Collector	Shipper for file/journald/container logs with buffering.
REST API	Ingest logs, search/query, manage alerts, export reports.
Cloud Connectors	AWS/Azure/GCP connectors (optional).
Notifications	Email, Slack/Teams, Webhook, SMS (via provider).

4. Functional Requirements (FR)

FR-1 Authentication & Authorization: Login, RBAC (Admin/Analyst/Viewer), optional 2FA and optional SSO (OIDC/SAML).

FR-2 Log Collection: Collect logs via agents, Syslog, API ingestion, and cloud integrations.

FR-3 Parsing & Normalization: Parse JSON/CSV/syslog/plain logs; extract standard fields.

FR-4 Enrichment: Add metadata like environment, tags, geo-IP (optional), and asset ownership.

FR-5 Storage & Retention: Time-based indexing; hot/warm/cold tiers; retention policies; archive support.

FR-6 Search & Query: Keyword search, filters (time/host/service/severity), advanced query syntax, saved searches.

FR-7 Dashboards & Visualization: Custom dashboards with charts and widgets; share controls.

FR-8 Alerting System: Rule-based alerts with throttling, deduplication, and suppression windows.

FR-9 Reporting & Export: Scheduled reports; export to CSV/JSON/PDF with audit logging.

FR-10 Audit Logging: Track user logins, searches, exports, admin changes, and rule updates.

FR-11 Integrity & Tamper Protection: Hash/sign logs; optional immutable/WORM storage.

FR-12 Multi-Tenant (Optional): Separate organizations/teams with isolated data and permissions.

FR-13 Health Monitoring: Health endpoints, ingestion lag view, queue depth, storage usage metrics.

5. Non-Functional Requirements (NFR)

Performance

- Search results within 2–5 seconds for typical queries.
- Scalable ingestion (example target 10,000+ events/sec).

Security

- HTTPS/TLS for UI and ingestion endpoints.
- Sensitive data masking rules for secrets/tokens.
- Least-privilege RBAC and immutable audit trail.

Reliability

- 99.9% uptime target (production).
- Backup/restore support and optional replication.

Scalability

- Horizontal scaling supported with distributed indexing.
- Load balancing and sharded storage.

Usability

- Simple UI, quick filters, saved searches, user-friendly dashboards.

Compatibility

- Supports Linux/Windows sources and modern browsers.

6. Data Model (Example Fields)

Field	Type	Description
timestamp	datetime	Event time (UTC recommended).
host	string	Hostname or asset name.
service	string	Application/service generating log.
level	string	Severity (info/warn/error/critical).
message	string	Raw log message.
src_ip	string	Source IP address (if present).
user	string	Username/account involved (if present).
tags	array	Custom labels for filtering.

7. Use Cases

- UC-1: DevOps searches error spikes for a service for last 24 hours and compares with last 7 days.
- UC-2: SOC analyst detects brute force: >10 failed logins in 5 minutes from same IP and triggers alert.
- UC-3: Auditor exports a user activity report for a selected time window for compliance evidence.

8. Future Enhancements (Optional)

AI anomaly detection, threat intelligence integration, SIEM integration, and automated ticketing (Jira/ServiceNow).