Log Management System Design

Summit Digital Solutions, Inc.

Document Version: 2.4

Last Updated: January 9, 2024

Classification: Confidential

1. Purpose and Scope

1. This document establishes the architectural design and operational requirements for Summit Digital Solutions' enterprise-grade Log Management System ("System"), which serves as a critical component of the Peak Performance Platform(TM).

2. The System is designed to collect, process, store, and analyze log data generated by client enterprise environments, supporting compliance requirements and operational intelligence capabilities.

2. System Architecture

1. Collection Layer

- Distributed log collectors deployed across client infrastructure

- Support for standard logging protocols (Syslog, SNMP, Windows Event Log)

- Custom API endpoints for proprietary application logs

- Real-time log ingestion capabilities up to 50,000 events per second

2. Processing Layer

- Multi-threaded log parsing engine

- Field extraction using machine learning algorithms

- Data normalization and enrichment

- Real-time correlation engine

3. Storage Layer

- Primary storage: Distributed NoSQL database cluster

- Hot storage retention: 30 days

- Warm storage retention: 90 days

- Cold storage retention: 7 years

- Data compression ratio: minimum 10:1

3. Security Controls

1. Data Protection

- AES-256 encryption at rest

- TLS 1.3 encryption in transit

- Role-based access control (RBAC)

- Multi-factor authentication for administrative access

2. Compliance Features

- GDPR compliance mechanisms

- SOC 2 Type II controls

- HIPAA-compliant data handling

- PCI DSS logging requirements

4. Performance Requirements

1. System Performance

- Maximum ingestion latency: 2 seconds

- Query response time: <5 seconds for last 24 hours of data

- System availability: 99.99% uptime

- Maximum data loss threshold: 0.001%

2. Scalability

- Horizontal scaling capabilities

- Automatic node addition/removal

- Load balancing across processing nodes

- Dynamic resource allocation

5. Integration Capabilities

1. Standard Integrations

- REST API endpoints

- MQTT protocol support

- Kafka stream processing

- Elasticsearch compatibility

2. Custom Integrations

- Peak Performance Platform(TM) native integration

- Custom webhook support

- Third-party SIEM integration

- Export to business intelligence platforms

6. Retention and Archival

1. Data Lifecycle Management

- Automated tiering based on access patterns

- Configurable retention policies

- Compliance-driven archival rules

- Data purge verification procedures

2. Archive Access

- Indexed search capabilities

- Restore SLA: 4 hours for warm storage

- Restore SLA: 24 hours for cold storage

- Chain of custody documentation

7. Monitoring and Alerting

1. System Health Monitoring

- Real-time performance metrics

- Capacity trending

- Resource utilization tracking

- Automated failure detection

2. Alert Management

- Configurable alert thresholds

- Escalation procedures

- Integration with incident management systems

- Alert correlation capabilities

8. Disaster Recovery

1. Backup Procedures

- Real-time replication to secondary site

- Daily incremental backups

- Weekly full backups

- Monthly backup verification

2. Recovery Procedures

- Recovery Time Objective (RTO): 4 hours

- Recovery Point Objective (RPO): 15 minutes

- Automated failover capabilities

- Manual failback procedures

9. Intellectual Property Rights

1. All intellectual property rights, including but not limited to patents, copyrights, and trade secrets related to the System design and implementation, are the exclusive property of Summit Digital Solutions, Inc.

10. Confidentiality

1. This document contains confidential and proprietary information of Summit Digital Solutions, Inc. and shall not be disclosed to third parties without express written authorization.

11. Document Control

Document Owner: James Henderson, Chief Digital Officer

Technical Reviewer: Michael Chang, CTO

Security Reviewer: Sarah Blackwell, COO

Version: 2.4

Last Review Date: January 9, 2024

Next Review Date: July 9, 2024

Approval

APPROVED AND ADOPTED this 9th day of January, 2024.

SUMMIT DIGITAL SOLUTIONS, INC.

By: _

Dr. Alexandra Reeves

Chief Executive Officer

By: _

Michael Chang

Chief Technology Officer