Here’s a **complete, self-contained solution** for your **ISO 8583 monitoring and alerting system** designed for **150 switch cards** processing **100k–200k transactions per minute (TPM)**. The architecture uses **open-source tools**, **on-premises hardware**, and no virtualization/containerization.

**1. Architecture Overview**

**2. Data Collection & Ingestion**

**Tools**

* **Apache Kafka**: Distributed message broker for high-throughput ingestion.
* **Filebeat**: Lightweight agent to collect ISO 8583 logs from switches.
* **jPOS**: Java library to parse ISO 8583 messages (MTI, PAN, response codes).

**Hardware**

| **Component** | **Servers** | **Specs (Per Server)** | **Purpose** |
| --- | --- | --- | --- |
| **Kafka Brokers** | 10 | 32 vCPU, 256GB RAM, 8TB NVMe SSD | Handle 200k TPM with replication (RF=3). |
| **Log Collectors** | 5 | 16 vCPU, 64GB RAM, 2TB SATA SSD | Run Filebeat + jPOS parsers. |

**Configuration**

* **Kafka Topics**:
  + iso8583-transactions (16 partitions for parallel processing).
  + iso8583-logs (for raw message debugging).
* **Message Parsing**:
  + Use jPOS to decode ISO 8583 messages and extract critical fields (e.g., PAN, MTI, response code).
  + Mask PANs at ingestion using SHA-256 hashing.

**3. Stream Processing**

**Tools**

* **Apache Flink**: Stateful stream processing for real-time analytics.
* **Fraud Detection**: Custom Flink jobs for velocity checks, geolocation mismatches.

**Hardware**

| **Component** | **Servers** | **Specs (Per Server)** | **Purpose** |
| --- | --- | --- | --- |
| **Flink Task Managers** | 16 | 48 vCPU, 512GB RAM, 2TB NVMe SSD | Process 150 switches in parallel. |
| **Flink Job Manager** | 2 | 16 vCPU, 64GB RAM, 1TB SATA SSD | Orchestrate Flink jobs. |

**Key Jobs**

1. **Success/Error Rate Calculation**:

Java

DataStream<Transaction> transactions = ...;

transactions

.keyBy(Transaction::getSwitchId)

.timeWindow(Time.minutes(5))

.aggregate(new ErrorRateCalculator());

1. **Fraud Detection**:
   * Flag >5 transactions/minute per PAN.
   * Validate geolocation against card BIN.

**4. Storage**

**Tools**

* **VictoriaMetrics**: Time-series database for metrics (TPS, latency, error rates).
* **Elasticsearch**: Search and analyze transaction logs.
* **MinIO**: S3-compatible storage for cold logs (2-year retention).

**Hardware**

| **Component** | **Servers** | **Specs (Per Server)** | **Purpose** |
| --- | --- | --- | --- |
| **VictoriaMetrics** | 6 | 48 vCPU, 256GB RAM, 20TB SATA SSD | Store metrics (1M+ samples/sec). |
| **Elasticsearch** | 12 | 64 vCPU, 512GB RAM, 12TB NVMe SSD | Index hot logs (retain 60 days). |
| **MinIO** | 8 | 24 vCPU, 128GB RAM, 200TB HDD | Archive logs to HDD with erasure coding. |

**Configuration**

* **Elasticsearch**:
  + Index templates for ISO 8583 logs (e.g., transactions-2024-01-01).
  + Retention policy: Delete indices older than 60 days.
* **VictoriaMetrics**:
  + Retention: 1 year.
  + Replication: -replicationFactor=2.

**5. Visualization & Alerting**

**Tools**

* **Grafana**: Dashboards for real-time metrics (TPS, error rates, latency).
* **Kibana**: Investigate transaction logs (e.g., filter by response code 05).
* **Prometheus Alertmanager**: Threshold-based alerts (e.g., error rate >5%).
* **ElastAlert**: Anomaly detection on Elasticsearch logs (e.g., PAN velocity).

**Hardware**

| **Component** | **Servers** | **Specs (Per Server)** | **Purpose** |
| --- | --- | --- | --- |
| **Grafana** | 2 | 8 vCPU, 32GB RAM, 1TB SATA SSD | Dashboards for ops/fraud teams. |
| **Prometheus** | 2 | 16 vCPU, 64GB RAM, 2TB SATA SSD | Scrape VictoriaMetrics and system metrics. |

**Key Alerts**

1. **High Error Rate**:

Yaml

# prometheus/rules.yml

- alert: ISO8583\_High\_Error\_Rate

expr: (sum(rate(iso8583\_errors[5m])) / sum(rate(iso8583\_total[5m]))) > 0.05

for: 5m

1. **Switch Connectivity Loss**:

Yaml

# elastalert/rules/switch\_down.yaml

type: flatline

threshold: 1

timeframe: minutes: 5

filter:

- term:

component: "switch\_heartbeat"

**6. Network & Security**

**Tools**

* **Telegraf**: SNMP polling for switch/router health.
* **Wazuh**: File integrity monitoring (FIM) and intrusion detection.
* **HAProxy**: Load balancing for Kafka/Flink.
* **Vault by HashiCorp**: Tokenize PANs before storage.

**Hardware**

| **Component** | **Servers** | **Specs (Per Server)** | **Purpose** |
| --- | --- | --- | --- |
| **HAProxy** | 2 | 16 vCPU, 64GB RAM, 1TB SATA SSD | Load balance traffic to Kafka/Flink. |
| **Wazuh** | 2 | 8 vCPU, 32GB RAM, 1TB SATA SSD | Monitor server/network security. |

**Key Configurations**

* **Vault**:
  + Tokenize PANs using transit engine.
  + Store encryption keys in HSM (e.g., **Thales Luna**).
* **Telegraf**:
  + Poll SNMP metrics (e.g., switch port status, bandwidth).

Toml

[[inputs.snmp]]

agents = ["udp://switch-01:161"]

version = 3

[[inputs.snmp.field]]

name = "ifOperStatus"

oid = "IF-MIB::ifOperStatus"

**7. Disaster Recovery (DR)**

**Tools**

* **Rclone**: Sync MinIO backups to a secondary data center.
* **pgBackRest**: PostgreSQL backups.

**Implementation**

1. **Backups**:
   * Daily MinIO snapshots → Secondary site via rclone sync.
   * PostgreSQL WAL backups → MinIO.
2. **DR Testing**:
   * Quarterly failover drills using **Litmus** (simulate data center outage).

**8. Synthetic Monitoring**

**Tools**

* **Apache JMeter**: Simulate ISO 8583 transactions (auth, reversal).
* **Blackbox Exporter**: Probe switch/mainframe connectivity.

**Configuration**

* **JMeter Test Plan**:
  + Send 1k TPM synthetic transactions to validate end-to-end flow.
  + Alert if synthetic TPS drops below 95%.

**9. Hardware Summary**

| **Component** | **Total Servers** | **Total Cost (Est.)** |
| --- | --- | --- |
| **Kafka** | 10 | $800,000 |
| **Flink** | 18 | $1,200,000 |
| **Elasticsearch** | 12 | $960,000 |
| **VictoriaMetrics** | 6 | $360,000 |
| **MinIO** | 8 | $240,000 |
| **Network/Security** | 6 | $180,000 |
| **Support** | 6 | $120,000 |
| **Total** | **66** | **$3.86M** |

*(Costs assume Dell/HPE servers with 5-year support and NVMe/HDD storage.)*

**10. Validation Steps**

1. **Load Test**: Simulate 150 switches generating 200k TPM using JMeter.
2. **Chaos Test**: Kill 3 Kafka brokers + 2 Elasticsearch nodes to verify HA.
3. **DR Drill**: Restore PostgreSQL and MinIO backups in <1 hour.

**11. Why This Works**

* **Scalability**: 10 Kafka brokers and 16 Flink nodes handle 150 switches at 200k TPM.
* **Compliance**: PAN masking, Wazuh, and audit logs meet PCI DSS.
* **Resilience**: No single point of failure (SPOF) in Kafka, Flink, or Elasticsearch.

This solution provides **end-to-end visibility**, **real-time fraud detection**, and **24/7 reliability** for your ISO 8583 infrastructure.