Below is the **optimal on-premises solution** for your **ISO 8583 monitoring and alerting system**, prioritizing **reliability, precision, and minimal failure risk** over cost optimization. This setup ensures seamless handling of **100k–200k transactions per minute (TPM)** with **no single point of failure (SPOF)**.

**Optimal Architecture Overview**

**1. Core Components & Hardware**

*(Total physical servers: 25–28)*

| **Component** | **Servers** | **Specifications (Per Server)** | **Purpose** | **HA Mechanism** |
| --- | --- | --- | --- | --- |
| **Apache Kafka (Brokers)** | 5 | 24 vCPU, 128GB RAM, 4TB NVMe SSD | Message ingestion (200k TPM + buffer) | Replication factor=3; 5 brokers for 2+ node failure tolerance. |
| **Apache Flink (Task Managers)** | 6 | 48 vCPU, 256GB RAM, 2TB NVMe SSD | Fraud detection, aggregations, latency checks | Checkpointing to MinIO; 6 nodes for zero lag during peak loads. |
| **Elasticsearch (Hot Tier)** | 7 | 64 vCPU, 512GB RAM, 8TB NVMe SSD | Transaction logs, network/firewall logs | 3 dedicated master nodes + 4 data nodes; replica shards=2. |
| **VictoriaMetrics (TSDB)** | 3 | 48 vCPU, 192GB RAM, 20TB SATA SSD | Metrics storage (TPS, latency, errors) | 3-node cluster with replication (-replicationFactor=2). |
| **PostgreSQL (HA Cluster)** | 3 | 32 vCPU, 128GB RAM, 4TB NVMe SSD | BIN tables, reconciliation, reference data | Patroni + etcd for automatic failover. |
| **MinIO (Cold Storage)** | 6 | 24 vCPU, 128GB RAM, 100TB HDD | Archived logs/metrics (2-year retention) | Erasure coding (6+6 disks; survives 6 failures). |
| **Network Monitoring** | 3 | 16 vCPU, 64GB RAM, 2TB SATA SSD | Telegraf (SNMP), Blackbox Exporter, SmokePing | Dedicated VLAN; load-balanced polling. |
| **Audible Alarms** | 2 | 8 vCPU, 16GB RAM, 1TB HDD | Node-RED + redundant IoT sirens/speakers | Dual Raspberry Pi 5 clusters with UPS. |
| **Support Services** | 4 | 16 vCPU, 64GB RAM, 2TB SATA SSD | Grafana, Kibana, HAProxy, Prometheus, Zabbix | Active-active HAProxy + Grafana. |

**2. Key Improvements Over "Optimized" Design**

**A. Transaction Processing (Kafka + Flink)**

* **Kafka**:
  + 5 brokers (up from 4) with larger NVMe SSDs (4TB) to handle **250k TPM bursts**.
  + 24 vCPU/128GB RAM per node for reduced consumer lag.
* **Flink**:
  + 6 task managers (up from 4) with 48 vCPU/256GB RAM each to ensure sub-second fraud detection latency.

**B. Storage & Analytics**

* **Elasticsearch**:
  + 7 nodes (4 data + 3 master) with 512GB RAM each to manage **300M+ logs/day** without JVM pressure.
  + 8TB NVMe SSD per node for fast indexing (100k writes/sec).
* **VictoriaMetrics**:
  + 3-node cluster (up from 2) with 20TB SATA SSD each for **3x replication** of critical metrics.

**C. Network Monitoring**

* **Dedicated Polling Servers**:
  + 3 nodes (up from 2) to distribute SNMP/ICMP checks across switches, firewalls, and mainframes.

**D. Audible Alarms**

* **Redundant IoT Sirens**:
  + Two Raspberry Pi 5 clusters with battery backups to guarantee alarm triggers during power outages.

**3. Optimal Hardware Requirements**

| **Component** | **Total Servers** | **Total CPU** | **Total RAM** | **Total Storage** |
| --- | --- | --- | --- | --- |
| **Kafka** | 5 | 120 vCPU | 640 GB | 20 TB NVMe |
| **Flink** | 6 | 288 vCPU | 1,536 GB | 12 TB NVMe |
| **Elasticsearch** | 7 | 448 vCPU | 3,584 GB | 56 TB NVMe |
| **VictoriaMetrics** | 3 | 144 vCPU | 576 GB | 60 TB SATA SSD |
| **PostgreSQL** | 3 | 96 vCPU | 384 GB | 12 TB NVMe |
| **MinIO** | 6 | 144 vCPU | 768 GB | 600 TB HDD |
| **Network Monitoring** | 3 | 48 vCPU | 192 GB | 6 TB SATA SSD |
| **Support Services** | 4 | 64 vCPU | 256 GB | 8 TB SATA SSD |
| **Audible Alarms** | 2 | 16 vCPU | 32 GB | 2 TB HDD |

**4. Critical Alerting Workflow**

1. **Alert Detection**:
   * Prometheus/VictoriaMetrics evaluates rules (e.g., error\_rate > 5%).
2. **Alert Routing**:
   * Prometheus Alertmanager sends alerts to **Node-RED** and **Zabbix** (dual redundancy).
3. **Audible Alarm Trigger**:
   * Node-RED activates:
     + **On-site alarms**: IoT sirens in server rooms/offices.
     + **SMS/voice calls**: Via Twilio API for remote staff.

**5. Network Health Monitoring**

* **Telegraf** collects SNMP data from:
  + **Switches**: Port status, bandwidth, CRC errors.
  + **Firewalls**: Allowed/denied connections, rule changes.
  + **Mainframes**: TCP connectivity, response times.
* **SmokePing** tracks end-to-end latency between ISO 8583 switches and payment processors.

**6. Why This Is Optimal**

1. **Zero Compromise on Reliability**:
   * Kafka/VictoriaMetrics/PostgreSQL replication ensures data survives multiple node failures.
   * Dual alarms (Node-RED + Zabbix) guarantee alerts during component failures.
2. **Performance at Scale**:
   * Elasticsearch handles **300M+ logs/day** without indexing delays.
   * Flink processes 200k TPM with **<100ms fraud detection latency**.
3. **Future-Proof**:
   * Hardware headroom supports **300k+ TPM** without upgrades.
   * MinIO’s 600TB HDD cluster allows 2+ years of log retention.

**7. Estimated Costs**

| **Category** | **Total Servers** | **Total Cost (Est.)** |
| --- | --- | --- |
| **Transaction Processing** | 11 | $450,000 |
| **Storage & Analytics** | 16 | $800,000 |
| **Network/Alarms** | 8 | $120,000 |
| **Total** | **25–28** | **$1.37M** |

*(Assumes enterprise-grade HPE/Dell servers with 5-year warranties.)*

**8. Final Validation Steps**

1. **Load Testing**: Simulate 250k TPM to validate Kafka/Flink/ES performance.
2. **Chaos Engineering**: Kill 2 Kafka brokers + 1 Elasticsearch node to test HA.
3. **DR Drill**: Restore PostgreSQL and MinIO backups in a secondary data center.

This solution eliminates all compromises, ensuring **24/7 reliability** for ISO 8583 monitoring. It’s engineered to handle your current workload while scaling effortlessly for future growth.