**Use Case Name**

Proactive Server/Device Failure Detection

**Core Priority**

Build the backbone for AI economy

**Pretext of the Use Case**

Transition from this costly and disruptive reactive model to a data-driven, proactive one. Instead of waiting for a component to fail, we will leverage advanced analytics and AI to predict its impending failure. By doing so, we can schedule maintenance or replacement activities in advance, ensuring maximum uptime, minimizing operational risk, and optimizing resource allocation.

**Business Problem**

Our organization experiences significant and costly unplanned downtime across its critical IT infrastructure, including servers, network devices, and storage systems. This downtime is a direct result of relying on a reactive "break-fix" maintenance model, where failures are addressed only after they have occurred.

Impact On Stakeholders

unpredictability leads to Significant Financial Loss, Operational Disruption, Inefficient Resource Management, Erosion of Trust.

This enables a strategic shift from reactive crisis management to planned, preventative maintenance to maximize system uptime and ensure business continuity.

**Nice to have Features**

a. Ingest system logs (e.g., syslog, Windows Event Logs) to correlate with metric anomalies.

b. Build a real-time dashboard to monitor server health and alerts like an alert management dashboard.

**Business Benefits**

Increased Uptime and Business Continuity

Significant Cost Reduction

Reduced Emergency Repairs

Optimized Maintenance Spend

Avoided Financial Penalties

Minimized Revenue Loss

Enhanced Service Reliability and Customer Satisfaction

**Minimum Viable Product**

The MVP focus on the core loop of collecting data, analyzing it, and generating a single, high-value alert. The goal is to prove the concept delivers value with the minimum set of features.

Minimum Viable Product (MVP) Scope:

1. Limited Scope of Assets 5-10 servers

2. Basic Data Ingestion: This includes core performance metrics like: CPU utilization, Memory usage, Disk I/O rate & Network traffic (throughput, latency)

3. Time-to-Failure (TTF) Prediction

4. Baseline modelling: Use historical data to establish normal behavior and apply anomaly detection model. This model will establish a baseline of "normal" behavior for each metric on each server. The system will continuously monitor the incoming data stream and generate an alert when a metric deviates significantly from its established normal behavior

5. Alerting: Email notification with: server name, metric, deviation, timestamp; Optional: Teams integration for real-time visibility

6. Analyze cross-metric and cross-device anomalies to identify cascading failures

**Success Criteria:**

Detect at least one real-world failure or degradation before outage

Reduce reactive incident tickets by 20% for pilot servers

**DataSet**

<https://centurylink.sharepoint.com/:f:/r/sites/Lumen-Avinya-Hackathon-2025/Hackathon_Data_Set/ProactiveServer_DeviceFailure_Detection_Dataset?csf=1&web=1&e=grhs4o>