Checklist

Cloud Monitoring and Alerts Checklist

1. Monitor Key Metrics

- [ ] **CPU Usage:**
  Set up monitoring for CPU utilization to detect overuse or under-provisioning..

- [ ] **Memory Usage:**
  Monitor memory consumption to prevent resource exhaustion, which could lead to slowdowns or crashes.

- [ ] **Network Throughput:**
  Keep an eye on network traffic to detect bottlenecks or bandwidth limitations.

- [ ] **Response Times:**
  Ensure that system response times remain within acceptable limits during peak traffic periods.

- [ ] **Disk I/O:**
  Monitor read/write operations to prevent bottlenecks in storage performance.

2. Set Up Alerts Based on Thresholds

- [ ] **CPU Alerts:**
  Set an alert for high CPU usage when utilization exceeds 80% for a sustained period.

- [ ] **Memory Consumption Alerts:**
  Trigger an alert if memory consumption stays above 90%, indicating potential issues such as a memory leak.

- [ ] **Network Traffic Alerts:**
  Set up alerts for sudden spikes in network traffic that could indicate a DDoS attack or misconfiguration.

3. Use Predictive Alerts for Proactive Issue Detection

- [ ] **Enable Machine Learning-Based Alerts:**
  Set up predictive alerts using machine learning features (e.g., Datadog, AWS CloudWatch) to identify abnormal patterns in traffic spikes, resource consumption, or performance drops before they escalate..

- [ ] **Anomaly Detection for Resource Usage:**
  Enable anomaly detection to catch unusual resource consumption patterns early.

4. Centralize Logs and Monitor for Errors

- [ ] **Set Up Centralized Logging:**
  Use tools like AWS CloudWatch Logs or Google Cloud Logging to capture all performance data, errors, and incidents in a single location.

- [ ] **Monitor and Analyze Logs:**
  Regularly analyze logs to identify recurring issues or inefficiencies that can be addressed.

5. Automate Incident Response

- [ ] **Auto-Scaling Response:**
  Automate auto-scaling actions when performance thresholds (e.g., CPU, memory) are breached, using tools like AWS CloudWatch Alarms.

- [ ] **Automated Instance Restarts:**
  Automate instance restarts or redirection of traffic to healthier instances when certain alerts are triggered.

- [ ] **Use Azure Automation Runbooks:**
  In Azure, automate responses with runbooks that execute corrective actions when performance degrades.

6. Best Tools for Cloud Monitoring

- [ ] **Amazon CloudWatch (AWS):**
  Set up real-time metrics, logging, alarms, and automated responses for AWS resources.

- [ ] **Azure Monitor (Microsoft Azure):**
  Use Azure Monitor for comprehensive monitoring, analytics, and alerts across Azure services.

- [ ] **Google Cloud Monitoring (GCP):**
  Implement Google Cloud Monitoring for monitoring and logging across hybrid cloud environments.

- [ ] **Datadog:**
  Integrate Datadog for multi-cloud infrastructure insights and proactive issue detection

- [ ] **Prometheus & Grafana:**
  Set up Prometheus for open-source monitoring and alerting in containerized environments, and Grafana for real-time performance visualizations.

Have questions or need help?
Find us at Aknostic.com