**CloudWatch**

1. **Definition**

CloudWatch monitors AWS resources and applications using metrics, logs, alarms, and dashboards.

1. **Core Components**

**Metrics**

- Built-in metrics for EC2, RDS, Lambda, etc.

- Custom metrics can be published via API or agent.

- Example: Monitor CPUUtilization, NetworkIn/Out.

**Logs**

- Collect logs from applications, Lambda, VPC Flow Logs, etc.

- Analyze with CloudWatch Logs Insights.

**Alarms**

- Alert based on metric thresholds.

- Actions: SNS notification, auto-scale, or recover EC2.

**Events (EventBridge)**

- Automate actions on specific events.

- Example: Run Lambda on EC2 StartInstances.

**Dashboards**

- Visualize metrics across multiple services in one place.

3. **Use Cases**

Application Monitoring

- Monitor latency, error rate, and resource usage.

Infrastructure Health

- EC2, RDS, ELB performance tracking.

Security Monitoring

- Combine with CloudTrail to detect unauthorized activities.

Automation

- Trigger auto-scaling or system recovery with alarms.

Cost Optimization

- Alert when usage goes beyond expected.

4. **Integration Examples**

**With CloudTrail**

- Log IAM activity in CloudTrail -> Send to CloudWatch Logs -> Create metric filter -> Alarm on

suspicious activity.

With Auto Scaling

- CloudWatch Alarm -> Triggers Scaling Policy when CPU > 80%.

5. **Best Practices**

- Set up alarms for critical resources.

- Use custom metrics for application-specific monitoring.

- Centralize logs in CloudWatch Logs.

- Use dashboards for executive visibility.