V1.0

Training Program on

Basics of Monitoring & Alerting

4P Advisory Services

www.4pa.in

What are Monitoring & Alerts?

Monitoring and alerts in IT infrastructures refer to the practice of actively monitoring various components of an IT system or infrastructure to detect and respond to any issues or incidents. This typically involves using tools and technologies to continuously monitor critical components such as servers, applications, databases, networks, and storage devices, and generate alerts.

The alerts generated by the monitoring system can be used to quickly identify and diagnose any problems, and take appropriate action to resolve them before they impact the end-users or customers. This is critical for maintaining the health and availability of Telecom Infrastructures, IT systems and services, and ensuring that they meet the performance and reliability expectations of the business.

Why should organizations have Monitoring & Alerting?

- Early Detection of Issues: Alerts can be set up to notify IT teams when an issue is detected, allowing them to take corrective action quickly, which can prevent the issue from becoming critical and causing more downtime.
- Proactive Maintenance: Monitoring and alerts can help in proactively maintaining the infrastructure by identifying potential issues before they cause bigger problems to minimize downtime, and improve the overall performance and reliability.
- Resource Optimization: Monitoring can help in optimizing resource utilization by providing insights into the usage of resources such as CPU, memory, and storage. to improve overall efficiency.
- Capacity Planning: Monitoring can also help in capacity planning by providing data on the utilization of resources over time to identify trends and forecast future resource requirements
- Compliance: Monitoring and alerts are often necessary to meet compliance requirements for security, availability, and performance.

Why learn about Monitoring & Alerting?

- This knowledge helps to identify potential issues early on and prevent them from becoming major problems that can lead to system downtime.
- IT teams can identify areas that require improvement and take steps to optimize system performance.
- Learning about monitoring and alerting also provides valuable insight into the tools and technologies used in the IT industry, staying up-to-date with the latest technologies is essential to remain competitive in the job market.
- To understand the importance of collaboration and communication within IT teams. Monitoring and alerting often involve multiple stakeholders, including system administrators, network engineers, and security teams, all working together to ensure that the infrastructure is running smoothly.

Audience

The audience for this training program would typically be individuals who are interested in or working in information technology. This may include IT professionals, system administrators, network engineers, or software developers. ***It is also for the students who are likely to join large organizations in entry-level positions.***

Learning Objectives:

- Understanding the key concepts and terminology related to system and network monitoring and alerting.
- Know how to monitor system performance metrics, including CPU usage, memory usage, disk usage, network traffic, and application performance.
- Knowing how to analyze monitoring data to identify trends, patterns, and potential issues.
- Understanding how to implement best practices for incident management, problem resolution, and continuous improvement.
- Understanding how to use monitoring tools.

Candidate Prerequisites

- Basic knowledge of IT operations, including system administration, network engineering, and cloud computing.
- Familiarity with basic operating systems such as Windows or Linux
- Understanding of networking concepts, including TCP/IP, and routing
- Basic understanding of cloud-based services, including Amazon Web Services (AWS) or Microsoft Azure, and their respective monitoring tools.

Lab requirements for the classroom:

Software:

- Operating systems such as Windows Server / Windows OS and Linux
- Web browsers such as Google Chrome, Mozilla Firefox, or Microsoft Edge

Hardware

- Desktop or a laptop computer per student with a good internet connection

Cloud Infrastructure:

Require access to AWS and Microsoft Azure cloud platforms, which may require creating accounts and configuring the necessary permissions to access and use the required services.
Requires an account on the relevant platforms, such as AWS(Amazon Web Services), Microsoft Azure and GCP (Google Cloud Platform)

Training Outline:

Day 1

Session 1: Introduction to Monitoring and Alerting

- *Overview of monitoring and alerting*
- *Key terminology and concepts*

Session 2: System Monitoring

- *Basics of system monitoring*
- *CPU, memory, and disk monitoring*
- *Activity: Using Amazon Cloud Watch or Microsoft Azure Monitor to monitor a virtual machine*

Session 3: Network Monitoring

- *Basics of network monitoring*
- *Network traffic monitoring and analysis*
- *Activity: Setting up network monitoring using Amazon CloudWatch or Microsoft Azure Monitor*

Session 4: Event Management and Alerting

- *Introduction to event management and alerting*
- *Configuring alerts and notifications*
- *Activity: Setting up alerts and notifications in Amazon CloudWatch or Microsoft Azure Monitor*