Proactive Network Monitoring and Performance Analysis Training Course



23 - 27 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #NO6885_119408

Course Introduction / Overview:

This course provides a comprehensive exploration of proactive network monitoring and performance analysis, shifting the paradigm from reactive troubleshooting to predictive and preventative network management. In today's hyper-connected digital landscape, network downtime or degradation directly impacts business continuity and revenue, making proactive oversight a critical competency. This program, offered by BIG BEN Training Center, is meticulously designed to equip participants with the methodologies and analytical skills needed to anticipate issues before they affect end-users. We will delve into the principles outlined by leading experts in the field, such as the concepts of network forensics and monitoring detailed by authors like Richard Bejtlich in his influential work, "The Practice of Network Security Monitoring". Participants will learn to establish robust performance baselines, analyze complex network traffic patterns, and utilize advanced diagnostic tools to perform effective root cause analysis. The curriculum moves beyond theoretical knowledge, focusing on the practical application of network observability, capacity planning, and performance optimization techniques. By mastering these skills, attendees will be empowered to ensure network reliability, enhance user experience, and support strategic business objectives through a resilient and high-performing network infrastructure.

Target Audience / This training course is suitable for:

- Network Administrators and Engineers.
- IT Operations Managers.
- Systems and Infrastructure Architects.
- Cybersecurity Analysts.
- NOC (Network Operations Center) Technicians and Specialists.
- IT Professionals responsible for network performance and reliability.
- Technical Support Engineers (Level 2 and 3).
- DevOps and Site Reliability Engineers (SREs).

Target Sectors and Industries:

- Telecommunications and Internet Service Providers.
- Financial Services, Banking, and Insurance.
- Healthcare and Medical Institutions.
- E-commerce and Retail.
- Governmental Agencies and Public Sector Organizations.
- Manufacturing and Industrial Operations.
- Technology and Software Development.
- Education and Academic Institutions.

Target Organizations Departments:

- Information Technology (IT) Operations.
- Network Engineering and Architecture.
- Cybersecurity and Information Security.
- Infrastructure Management.
- Technical Support and Help Desk.
- Data Center Operations.
- Research and Development (R&D).
- Quality Assurance and Testing.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop and implement a proactive network monitoring strategy.
- Utilize key monitoring protocols like SNMP, NetFlow, and sFlow effectively.
- Establish and maintain accurate network performance baselines.
- Analyze network traffic and packet data to identify performance bottlenecks.
- Perform systematic root cause analysis for complex network issues.
- Create comprehensive network performance and health reports for stakeholders.
- Conduct network capacity planning based on trend analysis and predictive modeling.
- Apply Quality of Service (QoS) policies to optimize network performance.
- Correlate data from disparate sources to gain holistic network visibility.
- Evaluate and select appropriate network monitoring tools for specific environments.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring that participants can immediately apply their learned skills in a real-world context. This course moves beyond traditional lecture-based formats by integrating a blend of expert-led instruction, in-depth case study analysis, and collaborative group workshops. Participants will engage in hands-on simulated labs where they will configure monitoring tools, analyze captured network traffic, and diagnose pre-configured performance problems. These practical exercises are designed to reinforce theoretical concepts and build confidence in troubleshooting complex scenarios. Team-based activities will encourage peer-to-peer learning and the exchange of diverse industry experiences, fostering a richer educational environment. Throughout the course, our expert instructors facilitate dynamic discussions, provide personalized feedback, and guide participants through complex topics. The learning process emphasizes a problem-solving approach, empowering attendees not just with knowledge of tools, but with the critical thinking and analytical frameworks necessary to maintain a high-performing and resilient network infrastructure long after the course concludes.

Course Agenda (Course Units):

Unit One: Foundations of Proactive Network Management

- Fundamentals of network monitoring and performance analysis.
- Reactive vs. proactive vs. predictive network management models.
- Key performance indicators (KPIs) and metrics (latency, jitter, packet loss, throughput).
- Understanding network baselining and its importance.
- The relationship between network performance and user experience.
- Introduction to network observability principles.
- Mapping business objectives to network performance goals.

Unit Two: Core Monitoring Protocols and Technologies

- Deep dive into Simple Network Management Protocol (SNMP).
- Exploring flow-based monitoring with NetFlow, sFlow, and IPFIX.
- Techniques for packet capture and analysis using tools like Wireshark.
- Leveraging ICMP for availability and latency testing.
- Introduction to log analysis and syslog for network devices.
- Understanding Application Performance Monitoring (APM) basics.
- Comparing agent-based vs. agentless monitoring approaches.

Unit Three: Performance Analysis and Anomaly Detection

- Techniques for establishing a dynamic performance baseline.
- Statistical methods for trend analysis and forecasting.
- Identifying anomalies and deviations from the baseline.
- Correlating events across different network domains and systems.
- Visualizing network data for effective analysis and reporting.
- Building effective network performance dashboards.
- Introduction to thresholding and intelligent alerting strategies.

Unit Four: Advanced Troubleshooting and Root Cause Analysis

- Structured methodologies for network troubleshooting.
- Isolating problems in a multi-tiered network architecture.
- Advanced packet analysis for diagnosing application-level issues.
- Performing root cause analysis (RCA) for intermittent problems.
- Troubleshooting common issues: congestion, latency, and configuration errors.
- Utilizing monitoring data for post-mortem incident analysis.
- Collaborative troubleshooting techniques for cross-functional teams.

Unit Five: Optimization, Capacity Planning, and Future Trends

- Strategies for network performance optimization and tuning.
- Implementing Quality of Service (QoS) for traffic prioritization.
- Fundamentals of network capacity planning and management.
- Predictive analytics for forecasting future resource needs.
- Automating monitoring tasks and responses.
- Introduction to AIOps (AI for IT Operations) in network management.
- Reporting network performance and value to business stakeholders.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As networks become increasingly software-defined and ephemeral with the rise of cloud and containerization, how must proactive monitoring strategies evolve beyond device-centric metrics to effectively measure and ensure application performance and end-user experience?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing on a strategic, vendor-agnostic mindset rather than proficiency in a single monitoring tool. While many programs teach the "how-to" of specific software, our curriculum emphasizes the "why" and "what-if" of network performance management. We cultivate a deep, analytical skill set that empowers participants to select, implement, and interpret data from any monitoring platform effectively. The core of the program is built around proactive and predictive methodologies, shifting the professional's role from a reactive firefighter to a strategic guardian of network health. Furthermore, the course integrates concepts from network security monitoring, recognizing that performance and security are intrinsically linked; an anomaly in one domain is often a symptom in the other. By analyzing real-world case studies of complex outages and performance degradations, participants learn not just to solve problems, but to deconstruct them to prevent recurrence. This holistic approach, which combines foundational principles with advanced analytical frameworks and a forward-looking perspective on trends like AIOps, ensures that the skills acquired are both immediately applicable and enduringly relevant in a rapidly evolving technological landscape.