FORTINET - NSE5 - FortiAnalyser

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

Anyone in charge of log management and reporting on the FortiAnalyzer

Training objectives

- Describe the features of the FortiAnalyzer
- Deploy the right architecture in relation to the needs expressed by your customers
- Administer ADOMs
- Configure RAID
- Register the devices that will send the logs
- Encrypt communications between the devices and the FortiAnalyzer (SSL and IPSEC)
- Visualize and analyze the logs
- Monitor events and set up alerts
- Apply disk quotas for each device
- Backup, Restore and export logs
- Use the content archive
- Understand the different steps of log processing
- Understand the SQL queries used in datasets
- Create a dataset, a chart and then use it in a report
- Generate on-demand or scheduled reports

Summary

Fortinet's FortiAnalyzer platform provides network logging, analysis, and reporting functions within a single system. This one-day training will teach you how to use FortiAnalyzer. First, you'll learn about the administration interface, how to enroll new devices, and how to secure communications with the FortiAnalyzer. Then you will manipulate logs and archives, existing reports and configure custom

reports. Upon completion of this course, you will have a solid understanding of the FortiAnalyzer and know how to deploy it in simple or complex environments.

Course outline

- Introduction to the FortiAnalyzer
- Configuration and administration
- Registration of devices that will send their logs to the FortiAnalyzer
- Logs and archives
- Reports

Approach and methodology

The training is based on a hands-on approach centered on technical labs, allowing participants to directly manipulate logs, equipment and reports. It combines guided demonstrations and progressive exercises to develop operational proficiency with the FortiAnalyzer. The learning is oriented towards concrete cases of analysis and monitoring, close to the realities on the ground.

Recommendations

Having taken the NSE 4 Certification - FortiGate I and II: Network Security Professional (NSE4) or equivalent content is a real plus to approach this training in good conditions