FT-FAZ
FortiAnalyzer

Overview

In this one-day class, students will learn the fundamentals of using FortiAnalyzer for centralized logging and reporting. Students will learn how to configure and deploy FortiAnalyzer, and identify threats and attack patterns through logging, analysis, and reporting. Finally, students will examine some helpful troubleshooting techniques.

In interactive labs, students will explore administration and management; register devices for log collection with FortiAnalyzer; use FortiAnalyzer to centrally collect logs; perform a forensic analysis of logs based on simulated network attacks; create reports; and explore solutions to common misconfiguration issues.

Who Should Attend

Anyone who is responsible for the day-to-day management of FortiAnalyzer devices and FortiGate security information.

Prerequisites

- Familiarity with all topics presented in FortiGate Security and FortiGate Infrastructure.
- Knowledge of SQL SELECT syntax is helpful.

Objectives

After completing this course, you should be able to:

- Describe key features and concepts of FortiAnalyzer
- Deploy an appropriate architecture
- Use administrative access controls
- Monitor administrative events and tasks
- Understand FortiAnalyzer
- Configure high availability
- Understand HA synchronization and load balancing
- Upgrade an HA cluster's firmware
- Verify the normal operation of an HA cluster
- Manage ADOMs
- Configure RAID
- Register supported devices
- Troubleshoot communication issues

- Manage disk quota
- Manage registered devices
- Protect log information
- View and search logs
- Troubleshoot and manage logs
- Monitor events
- Generate and customize reports
- Customize charts and datasets
- Manage reports
- Troubleshoot reports

Agenda

- Introduction and Initial Configuration
- Administration and Management
- Device Registration and Communication
- Logging
- Reports

Certification

This course is part of the preparation for the NSE 5 certification exam.