FortiAnalyzer

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging and reporting. You will learn how to configure and deploy FortiAnalyzer, and identify threats and attack patterns through logging, analysis, and reporting. Finally, you will examine the management of events, incidents, playbooks, and some helpful troubleshooting techniques.

Product Version

- FortiAnalyzer 7.0.2

Course Duration

- Lecture time (estimated): 5 hours
- Lab time (estimated): 7 hours
- Total course duration (estimated): 12 hours/2 days

Who Should Attend

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

Certification

This course is intended to help you prepare for the *NSE 5 FortiAnalyzer* certification exam.

Prerequisites

- Familiarity with all topics presented in the *NSE 4 FortiGate Security* and *NSE 4 FortiGate Infrastructure* courses
- Knowledge of SQL SELECT syntax is helpful, but not required

Agenda

1. Introduction and Initial Configuration
2. Administration and Management
3. Device Registration and Communication
4. Logging
5. FortiSoC—Incidents and Events
6. FortiSoC—Playbooks
7. Reports

Objectives

After completing this course, you will be able to:

- Describe key features and concepts of FortiAnalyzer
- Deploy an appropriate architecture
- Use administrative access controls
- Monitor administrative events and tasks
- Configure high availability
- Understand HA synchronization and load balancing
- Upgrade the firmware of an HA cluster
- Verify the normal operation of an HA cluster
- Manage ADOMs
- Manage RAID
- Register supported devices
- Troubleshoot communication issues
- Manage disk quota
- Manage registered devices
- Protect log information
- View, search, manage, and troubleshoot logs
- Monitor and manage events
- Manage and customize event handlers
- Create and manage incidents
- Explore tools used for threat hunting
- Create, run, and troubleshoot playbooks
- Import and export playbooks
- Generate and customize reports
- Customize charts and datasets
- Manage and troubleshoot reports

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-FAZ

Self-Paced Training

Includes online training videos and resources through the NSE Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using the following methods:

- Credit card, through the course on the NSE Training Institute
- Purchase order (PO), through Fortinet Resellers or Authorized Training Partners

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-FAZ-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

(ISC)2

- CPE training hours: 5
- CPE lab hours: 7
- CISSP domains: Security Operations

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.