Publication date : 01/15/2024

Course : Splunk, operational data analysis

Practical course - 3d - 21h00 - Ref. PUK
Price : 2470 CHF E.T.

4,3 / 5

BEST

Splunk is a tool that aims to help us collect and sort relevant information: a tool that could be described as [[event correlator]]. This training course will enable you to configure, analyze and generate reports on data based on your personalized alerts.

Teaching objectives

At the end of the training, the participant will be able to:

- Use Splunk to collect, analyze and report on data
- Enrich operational data with searches and feeds
- Create real-time, scripted and other intelligent alerts
- Integrating advanced JavaScript graphics
- Using the Splunk API

Intended audience

System and network administrators.

Prerequisites

Basic knowledge of networks and systems.

Course schedule

1 Configuring Splunk

- Obtain a Splunk.com account.
- Install Splunk under Windows.
- Index files and directories via Web interface, CLI or configuration files.
- Obtain data via network ports, script or modular inputs.
- Implementation of the Universal Forwarder.

Hands-on work

Configure Splunk. Implement definition of field extractions, event types and labels.

PARTICIPANTS

System and network administrators.

PREREQUISITES

Basic knowledge of networks and systems.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

2 Data mining

- SPL queries. Boolean operators, commands.
- Search using time ranges.

Hands-on work
Extract from log files, the most frequently visited Web pages, the most frequently used browser, the most frequently visited sites...

3 Dashboards

- Dashboards and operational intelligence, making data stand out. Types of graphs.

Hands-on work
Create and enhance a dashboard with graphs linked to searches carried out.

4 New application

- Install an existing Splunk or third-party application.
- Add dashboards and searches to an application.
- Interactive dashboards.
- Produce regular (scheduled) dashboards in PDF format.

Hands-on work
Create a new Splunk application. Install an application and view events related to Cisco switches.

5 Data models

- Data models.
- Take advantage of regular expressions.
- Optimize search performance.
- Rotate data.

Hands-on work
Use the template pivot command to display data.

6 Data enrichment

- Group related events, notion of transaction.
- Take advantage of multiple data sources.
- Identify relationships between fields.
- Predict future values.
- Discover abnormal values.

Hands-on work
Practice in-depth database searches.

TERMS AND DEADLINES
Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES
Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

7 Alert types

- Supervised conditions.
- Action taken in response to alerts.
- Become proactive with alerts.

Hands-on work
Execute a script when the Web server error 503 occurs, writing the details associated with the event to a file.

Dates and locations

REMOTE CLASS
2026 : 1 June, 16 Sep., 2 Dec.