System and Network monitoring tools and techniques

Hands-on course of 3 days - 21h
Ref.: SUR - Price 2024: €2 290 (excl. taxes)

THE PROGRAMME

last updated: 01/2018

1) Network and system administration principles

- What to monitor : Processes, system resources usage, file systems, users.
- Network traffic and Network equipments.
- Monitoring tools.
- Basic system commands, scripts. Log files.
- Network observers and network scanner.
- File system audit tools. SNMP tools. Global monitoring tools.

Hands-on work : Define a strategy for the administration.

2) Deploying a TCP/IP Network

- TCP/IP architecture. Services and protocols.
- Addressing and routing. Address classes and network masks.
- Configuring routers. Routing protocols.
- Configuring servers and services.
- Setting up FTP, HTTP, and DNS services.
- Network and application services monitoring.
- Open Source Software. Smokeping. Munin.

Hands-on work : Network setup. Routers and switches. Configuring Windows and Linux systems. Using network testing basic tools. Smokeping. Configuration. Munin configuration.

3) Network Observers

- Using network sniffer applications.
- Adresses and protocols observation.
- From Tcpdump to Wireshark.
- How they work. Other tools.

Hands-on work : Using Etherape on Linux. Using Wireshark to analyze network traffic. Creating Capture and/or Display filters with Wireshark.

4) System protection

- Monitoring network services .
- The netstat command.
- Network scanners. Nmap. Nessus.
- Monitoring files and directories.
- Application software. Checking file and directory integrity.
- Intrusion detection tools. AIDE (Advanced Intrusion Detection Environnement).

Hands-on work : Using Nmap on Windows. Using AIDE on Linux.

5) Simple Network Management Protocol

- SNMP operation and messages : get, get-next, set, response. Agents.
- Management Information Bases.
- Scalar vs. tabular data.

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.

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.

- SNMP tools. Net-SNMP Software. MIB Browsers.
Hands-on work : Configuring SNMP agents on WIndows, Linux, and Cisco routers ans switches. Using Net-SNMP commands. Using a MIB Browser.

6) Multiple Router Traffic Grapher

- MRTG Principles
- Creating traffic graphs. Publishing graphs on a Web Server.
- RRDtool. Data storage.
- Graph creation. Exemple of CACTI.

Hands-on work : Configuring MRTG and CACTI on Linux.

7) Supervision tools

- Nagios origin. Monitored systems and services. Plugins.
- Configuration files. Test scheduling.
- CENTREON. Advanced interface. Graphical configuration.
- Big Brother. Monitoring principles.

Hands-on work : Configuring and using Nagios on Linux and Big Brother on Windows.

DATES

Contact us