+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 23/07/2025

Sign up

Nagios Core Monitoring Training

3 days (21 hours)

Presentation

Master all aspects of Nagios Core with this comprehensive training course, designed for system administrators, DevOps engineers and infrastructure managers wishing to build a reliable, scalable and customized monitoring system.

From the very first modules, you'll be immersed in Nagios Core's architecture, its key configuration files, object logic (hosts, services, templates), and the operation of the monitoring engine. Step-by-step installation is accompanied by immediate practice on a Linux infrastructure.

You will then learn how to use and create plugins, exploit NRPE, SNMP or SSH for remote supervision, and structure your notifications according to alert levels, with period management and automatic escalations.

The course goes further, covering optimization, load management, securing the web interface, file organization and possible integration with external tools to enhance your dashboards.

As with all our training courses, this one will be presented with the latest Nagios Core Monitoring updates.

Objectives

- Understand Nagios Core's modular architecture, key components and inner workings
- Configure and deploy comprehensive monitoring of heterogeneous infrastructures via files objects and templates
- Master the creation, integration and customization of Nagios plugins
- Be able to structure an advanced notification system with conditional alerts, escalations and hierarchical contacts
- Know how to supervise distributed environments with NRPE, SNMP or SSH

- Be able to industrialize supervision with a modular organization

Target audience

- System administrators
- DevOps engineers

Prerequisites

- Mastery of basic Linux commands

Nagios Core Monitoring training program Introduction to monitoring and Nagios

- Objectives of monitoring
- Types of monitoring: active/passive, agentless/agent-based
- Components monitored: hosts, services, applications, network
- Nagios Core history and architecture
- Differences between Nagios Core and Nagios XI
- Global operation

Installing Nagios Core

- Recommended Linux distribution
- Packages required
- Administrative privileges
- Downloading and compiling Nagios Core
- Installing official plugins
- Apache configuration for web interface
- Service startup and verification

Architecture and basic configuration

- Nagios file structure
- Object hierarchy and inheritance

- Creating host definitions
- Defining associated services
- Using templates
- Host and service groups
- Parent/child relationships for dependencies

Nagios plug-ins

- How a plugin works
- Plugins supplied by default
- Writing a plugin in Bash, Python or Perl
- Respecting the return code convention
- Testing and integrating Nagios
- Where to find them
- Installation and security

Notifications and escalations

- Defining contacts and contact groups
- Allocation to hosts/services
- Methods: email, SMS, webhook
- Frequency, notification period
- Trigger escalations after x failures
- Redirection to higher-level contacts

Planning and checks

- Verification schedule
- Supervision periods
- Verification queue
- Resource management and optimization

Web interface management

- Display of hosts and services
- Overview, history, logs
- User configuration with .htpasswd

- Access control (ACL) to restrict views
- HTTPS with SSL certificate

Distributed and remote monitoring

- Installation of NRPE service
- Setting up remote commands
- Securing NRPE
- Using check_snmp
- Network device detection
- Secure remote commands with SSH
- Public/private keys

Problem management and logs

- Locating and reading logs
- Log rotation
- Enabling verbose mode
- Command traces and common errors

Best practices and optimization

- Modularization with cfg_dir
- Using templates to factor
- Limiting redundant checks
- Using parent hosts and dependencies
- Monitoring CI/CD applications
- Exporting data for external dashboards

Case studies and final workshop

- Web server supervision
- Supervision of databases
- Supervision of a network infrastructure
- Deployment of a complete supervision infrastructure
- Creation of files, plugins, alerts and escalations
- Documentation and presentation of the solution

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check that skills have been correctly acquired.

Certification

A certificate will be awarded to each trainee who completes the training course.