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

Updated on 02/05/2026

Register

NSX-Advanced Services Training

3 days (21 hours)

Overview

The NSX-Advanced Services training course teaches you how to deploy and operate advanced network services in a virtualized data center: micro-segmentation, load balancing, VPN, and IDS/IPS. It focuses on real-world use cases: Zero Trust security, application publishing, and site interconnection.

You will learn how to design robust NSX architectures, apply granular security policies, and automate routine operations. The focus is on risk reduction, configuration standardization, and change traceability.

The approach is decidedly practical: guided workshops, demos, followed by independent exercises (troubleshooting, validation, hardening). Deliverables include sample configurations, an operating checklist, and test scenarios (connectivity, performance, rule compliance).

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Deploy and configure advanced NSX services (LB, VPN, security).
- Design a micro-segmentation strategy and translate it into rules.
- Implement consistent Gateway Firewall and DFW services.
- Diagnose and correct incidents (flow, routing, NAT, certificates).
- Automate tasks via API/CLI and produce operational documentation.

Target audience

- Virtualization and data center administrators
- Network and security engineers
- Infrastructure architects
- Operators/OPS in charge of production

Prerequisites

- Good foundation in IP networks (VLAN, routing, NAT, DNS)
- Basic knowledge of security (firewalls, segmentation, certificates)
- Experience with VMware vSphere (vCenter, ESXi, distributed switches)
- Fundamental knowledge of NSX (objects, segments, T0/T1)

Technical prerequisites

- PC with at least 16 GB RAM (32 GB recommended) and 4-core+ CPU
- Windows 11, macOS, or Linux with administrator access
- SSH client and recent browser (Chrome/Firefox)
- Tools: text editor, terminal, and access to an NSX lab environment provided

Our NSX-Advanced Services training program

[Day 1 - Morning]

NSX advanced services architecture and lab preparation

- NSX-T reminders: segments, Tier-0/Tier-1, groups, and policies
- Prerequisites for advanced services: Edge Nodes, uplinks, MTU, routing, and capabilities
- Flow reading: DFW vs. Gateway Firewall, processing order, and impacts
- Best design practices: management/data separation, HA, capacity, and licensing
- Hands-on workshop: Checking the status of the fabric/edges and validating end-to-end connectivity.

[Day 1 - Afternoon]

NSX Load Balancing: concepts, objects, and initial services

- Components: Virtual Server, Pool, Members, Health Monitors, and profiles
- Modes and topologies: one-arm vs. inline, SNAT, persistence, and timeouts
- Monitoring: statuses, metrics, logs, and health checkpoints
- Incident resolution: monitor failures, asymmetry, NAT/route and associated firewall rules
- Hands-on workshop: Deploy an HTTP/HTTPS service with monitor and validate distribution.

[Day 2 - Morning]

Advanced load balancing: L7, TLS, and policies

- L7 functions: content rules, URL/header rewriting, and redirects
- TLS: certificates, SSL termination, SNI, and encryption best practices
- Persistence and affinity: cookies, IP source, impacts on scalability
- High availability: placement on Edge Cluster, failover, and validation
- Hands-on workshop: Setting up an HTTPS Virtual Server with SNI and L7 routing rules.

[Day 2 - Afternoon]

NSX VPN: site-to-site IPsec and L2VPN

- IPsec: IKEv1/v2, proposals, PFS, DPD, and security settings
- Topologies: route-based vs. policy-based, integration with Tier-0/Tier-1
- Troubleshooting: IKE negotiation, selectors, NAT-T, routes, and MTU/MSS
- L2VPN: use cases (migration), constraints, and points to watch out for
- Hands-on workshop: Create an IPsec tunnel and validate application traffic via routes and firewall rules.

[Day 3 - Morning]

IDS/IPS and advanced security: prevention, visibility, and tuning

- IDS/IPS activation: prerequisites, profiles, severity, and detection/prevention modes
- Signature management: categories, exceptions, false positives, and tuning strategy
- Chaining with micro-segmentation: DFW/Gateway Firewall consistency and zones
- Operations: events, alerting, investigation workflows, and reporting
- Hands-on workshop: Enable IDS/IPS on a segment, generate an event, and apply targeted tuning.

[Day 3 - Afternoon]

Advanced service operations and troubleshooting

- Diagnostic tools: Traceflow, port mirroring, Edge captures, and connectivity tests
- Logs and metrics: where to look (Manager/Edge), correlation, and key indicators
- Runbooks: standard checks (routes, NAT, firewall, LB, VPN) and validation criteria
- Automation: API/Policy, configuration export/import, and GitOps approach
- Hands-on workshop: Resolving a multi-layer incident (LB + firewall + routing) with a step-by-step method.

Target companies

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific business knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training course complies with Qualiopi quality criteria. Once they have finalized their registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training course, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

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

Assessment

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

Certification

A certificate will be issued to each trainee who has completed the entire training course.