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

Mis à jour le 05/02/2026

S'inscrire

Formation NSX-Advanced services

3 jours (21 heures)

Présentation

La formation NSX-Advanced services vous permet de déployer et d'exploiter des services réseau avancés dans un datacenter virtualisé : micro-segmentation, load balancing, VPN et IDS/IPS. Elle cible des cas d'usage concrets : sécurisation Zero Trust, publication d'applications et interconnexion de sites.

Vous apprendrez à concevoir des architectures NSX robustes, à appliquer des politiques de sécurité granulaires et à automatiser les opérations courantes. L'accent est mis sur la réduction du risque, la standardisation des configurations et la traçabilité des changements.

L'approche est résolument pratique : ateliers guidés, démos, puis exercices d'autonomie (troubleshooting, validation, durcissement). Les livrables incluent des configurations types, une checklist d'exploitation, et des scénarios de tests (connectivité, performance, conformité des règles).

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Déployer et paramétrer les services avancés NSX (LB, VPN, sécurité).
- Concevoir une stratégie de micro-segmentation et la traduire en règles.
- Mettre en œuvre des services Gateway Firewall et DFW cohérents.
- Diagnostiquer et corriger les incidents (flux, routage, NAT, certificats).
- Automatiser des tâches via API/CLI et produire une documentation d'exploitation.

Public visé

- Administrateurs virtualisation et datacenter
- Ingénieurs réseau et sécurité
- Architectes infrastructure
- Exploitants/OPS en charge de la production

Pré-requis

- Bonnes bases en réseaux IP (VLAN, routage, NAT, DNS)
- Notions de sécurité (pare-feu, segmentation, certificats)
- Expérience VMware vSphere (vCenter, ESXi, switches distribués)
- Connaissances fondamentales NSX (objets, segments, T0/T1)

Pré-requis techniques

- PC avec 16 Go RAM minimum (32 Go recommandé) et CPU 4 cœurs+
- Windows 11, macOS ou Linux avec accès administrateur
- Client SSH et navigateur récent (Chrome/Firefox)
- Outils : éditeur de texte, terminal, et accès à un environnement de lab NSX fourni

Programme de notre formation NSX-Advanced services

[Jour 1 - Matin]

Architecture des services avancés NSX et préparation du lab

- Rappels NSX-T : segments, Tier-0/Tier-1, Groupes et policies
- Prérequis pour services avancés : Edge Nodes, uplinks, MTU, routage et capacités
- Lecture des flux : DFW vs Gateway Firewall, ordre de traitement et impacts
- Bonnes pratiques de design : séparation management/data, HA, capacité et licences
- Atelier pratique : Vérifier l’état du fabric/edges et valider la connectivité de bout en bout.

[Jour 1 - Après-midi]

Load Balancing NSX : concepts, objets et premiers services

- Composants : Virtual Server, Pool, Members, Health Monitors et profils
- Modes et topologies : one-arm vs inline, SNAT, persistance et timeouts
- Supervision : états, métriques, logs et points de contrôle de santé
- Résolution d’incidents : échecs de monitor, asymétrie, NAT/route et règles firewall associées
- Atelier pratique : Déployer un service HTTP/HTTPS avec monitor et valider la répartition.

[Jour 2 - Matin]

Load Balancing avancé : L7, TLS et politiques

- Fonctions L7 : règles de contenu, réécriture d'URL/headers et redirections
- TLS : certificats, terminaison SSL, SNI et bonnes pratiques de chiffrement
- Persistance et affinité : cookies, source IP, impacts sur la scalabilité
- Haute disponibilité : placement sur Edge Cluster, bascule et validation
- Atelier pratique : Mettre en place un Virtual Server HTTPS avec SNI et règle L7 de routage.

[Jour 2 - Après-midi]

VPN NSX : IPsec site-à-site et L2VPN

- IPsec : IKEv1/v2, propositions, PFS, DPD et paramètres de sécurité
- Topologies : route-based vs policy-based, intégration avec Tier-0/Tier-1
- Dépannage : négociation IKE, sélecteurs, NAT-T, routes et MTU/MSS
- L2VPN : cas d'usage (migration), contraintes et points de vigilance
- Atelier pratique : Créer un tunnel IPsec et valider le trafic applicatif via routes et règles firewall.

[Jour 3 - Matin]

IDS/IPS et sécurité avancée : prévention, visibilité et tuning

- Activation IDS/IPS : prérequis, profils, sévérité et modes de détection/prévention
- Gestion des signatures : catégories, exceptions, faux positifs et stratégie de tuning
- Chaînage avec la micro-segmentation : cohérence DFW/Gateway Firewall et zones
- Exploitation : événements, alerting, workflows d'investigation et reporting
- Atelier pratique : Activer IDS/IPS sur un segment, générer un événement et appliquer un tuning ciblé.

[Jour 3 - Après-midi]

Opérations et troubleshooting des services avancés

- Outils de diagnostic : Traceflow, port mirroring, captures sur Edge et tests de connectivité
- Logs et métriques : où chercher (Manager/Edge), corrélation et indicateurs clés
- Runbooks : vérifications standard (routes, NAT, firewall, LB, VPN) et critères de validation
- Automatisation : API/Policy, export/import de configuration et approche GitOps
- Atelier pratique : Résoudre un incident multi-couches (LB + firewall + routage) avec une méthode pas à pas.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.