+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-Security : microsegmentation & Zero Trust

3 jours (21 heures)

Présentation

La formation NSX-Security vous apprend à mettre en œuvre une microsegmentation efficace et une démarche Zero Trust pour réduire la surface d'attaque et contenir les mouvements latéraux. Vous saurez traduire des besoins métiers (app tiers, PCI, environnements multi-tenant) en politiques de sécurité opérationnelles.

Vous construirez une stratégie de segmentation basée sur l'inventaire des flux, la définition de groupes dynamiques et l'application de règles distribuées au plus près des workloads. L'accent est mis sur la lisibilité des politiques, la réduction des exceptions et la gestion du cycle de vie (changement, audit, rollback).

L'approche est pratique : ateliers guidés, démos, exercices de troubleshooting et validation par tests de connectivité. Les livrables incluent une matrice de flux, un modèle de nommage, des règles NSX documentées et une checklist de durcissement et d'exploitation.

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

Objectifs

- Cartographier les flux applicatifs et définir une stratégie de microsegmentation.
- Créer des Groupes dynamiques et des Security Policies cohérentes.
- Appliquer le Zero Trust (deny by default, least privilege) sur des cas concrets.
- Mettre en place journalisation, traçabilité et validation (logs, tests, audit).
- Dépanner des problèmes de connectivité liés aux règles et au service insertion.

Public visé

- Administrateurs/ingénieurs virtualisation VMware (vSphere/NSX)
- Ingénieurs sécurité réseau / SOC
- Architectes infrastructure / cloud privé
- Ops/DevOps en charge d’applications multi-tiers

Pré-requis

- Bonnes bases réseaux : TCP/IP, VLAN, routage, pare-feu L3/L4
- Notions de sécurité : segmentation, ACL, principes Zero Trust
- Connaissances vSphere : VM, vNIC, vSwitch/portgroups
- Lecture de logs et diagnostic (ping, traceroute, ports)

Pré-requis techniques

- PC avec 16 Go RAM (8 Go minimum), CPU 4 cœurs recommandés
- Windows, macOS ou Linux avec navigateur moderne
- Accès à un lab NSX (fourni par l’organisme) et client VPN si nécessaire
- Outils : terminal (PowerShell/Bash), éditeur de texte, client SSH

Programme de notre formation NSX-Security : microsegmentation & Zero Trust

[Jour 1 - Matin]

Fondamentaux NSX Security et approche Zero Trust

- Positionnement de NSX dans l’architecture (NSX Manager, Transport Nodes, segments, T0/T1)
- Principes Zero Trust : moindre privilège, vérification explicite, réduction de la surface d’attaque
- Concepts clés sécurité NSX : Distributed Firewall (DFW), groupes, services, politiques
- Modèles de microsegmentation : par application, par environnement (dev/test/prod), par zone de confiance
- Atelier pratique : Prise en main de l’interface NSX et repérage des objets sécurité (DFW, Groups, Services).

[Jour 1 - Après-midi]

Microsegmentation avec le Distributed Firewall (DFW)

- Comprendre le DFW L2/L3/L4 et les impacts sur les flux Est-Ouest
- Construire des Groupes dynamiques (tags, naming, critères VM) et éviter les règles “IP-based”
- Rédiger des règles efficaces : sources/destinations, services, scope, log, règle par défaut
- Bonnes pratiques : policy structure, priorités, nommage, gestion du changement

- Atelier pratique : Créer une politique DFW “deny by default” et autoriser uniquement les flux applicatifs nécessaires.

[Jour 2 - Matin]

Découverte des flux et sécurisation progressive

- Collecter et interpréter les flux : logs DFW, outils de visibilité, identification des dépendances applicatives
- Approche “observe > model > enforce” pour limiter les interruptions de service
- Stratégies de bascule : monitoring, enforcement partiel, exceptions temporaires
- Gestion des services : ports, protocoles, service groups et standardisation
- Atelier pratique : Établir une matrice de flux (app tiers) et la traduire en règles DFW.

[Jour 2 - Après-midi]

Administration avancée des politiques et dépannage

- Organisation des politiques : sections, policy tiers, règles globales vs applicatives
- Traçabilité et audit : journalisation, justification des règles, gestion des exceptions
- Dépannage : analyse “rule hit”, logs, vérification des groupes, résolution des conflits de règles
- Optimisation : réduction du nombre de règles, réutilisation d’objets, performance et lisibilité
- Atelier pratique : Diagnostiquer un flux bloqué et corriger la politique sans élargir excessivement les accès.

[Jour 3 - Matin]

Zero Trust appliqué : segmentation par zones et contrôle d’accès

- Définir des zones de confiance (users, app, data, management) et leurs règles d’interconnexion
- Modéliser des politiques “default deny” avec exceptions contrôlées
- Gestion des identités d’objets : tags, conventions, intégration avec le cycle de vie VM
- Cas d’usage : isolation d’un environnement sensible (bastion, management, sauvegarde)
- Atelier pratique : Concevoir une segmentation 3 zones (Front/App/DB) et appliquer les règles minimales nécessaires.

[Jour 3 - Après-midi]

Industrialisation, conformité et préparation à l’exploitation

- Standardiser : modèles de politiques, catalogues de services, règles “golden”
- Automatiser : principes d’Infrastructure as Code pour objets et règles (approche API/outil interne)
- Contrôles opérationnels : revues périodiques, nettoyage des règles, gestion des changements
- Reporting sécurité : preuves de conformité, indicateurs (règles actives, exceptions, logs)
- Atelier pratique : Produire un plan d’exploitation (runbook) microsegmentation et une checklist de revue de règles.

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.