# VMware NSX for Intrinsic Security [V4.x] (NSXIS4)

**ID** NSXIS4 **Preis** 3.440,– € (exkl. MwSt.) **Dauer** 5 Tage

Dieser Advanced-Kurs wird direkt von VMware durchgeführt.

*Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.*

## Kursüberblick

Dieser fünftägige, praxisnahe Kurs vermittelt Ihnen das Wissen, die Fähigkeiten und die Tools, um Kompetenz bei der Konfiguration, dem Betrieb und der Fehlerbehebung von VMware NSX® für intrinsische Sicherheit zu erlangen. In diesem Kurs werden alle Sicherheitsfunktionen von NSX vorgestellt, einschließlich Distributed Firewall und Gateway Firewall, Intrusion Detection and Prevention (IDS/IPS), NSX Application Platform, NSX Malware Prevention, VMware NSX® Intelligence™ und VMware NSX® NDR™. Darüber hinaus werden in diesem Kurs häufige Konfigurationsprobleme vorgestellt und eine Methodik zu deren Behebung vermittelt.

Produktausrichtung

- VMware NSX 4.1.0

## Zielgruppe

Erfahrene Sicherheitsadministratoren

## Empfohlenes Training für die Zertifizierung zum

VMware Certified Professional – Network Virtualization 2024 (VCP-NV 2024)

## Voraussetzungen

Außerdem sollten Sie über die folgenden Kenntnisse verfügen:

- Gute Kenntnisse von TCP/IP-Diensten und -Protokollen
- Kenntnisse und praktische Erfahrung im Bereich der Netzsicherheit, einschließlich:
- L2 bis L7 Firewalling
- Systeme zur Erkennung und Verhinderung von Eindringlingen
- Systeme zur Verhinderung von Malware
- Kenntnisse von und Arbeitserfahrung mit VMware vSphere®-Umgebungen

Der Abschluss VMware Certified Technical Associate - Network Virtualization wird empfohlen.

## Kursziele

Am Ende des Kurses sollten Sie in der Lage sein, die folgenden Ziele zu erreichen:

- Definition der Konzepte der Informationssicherheit
- Erläuterung der verschiedenen Arten von Firewalls und ihrer Anwendungsfälle
- Beschreibung der Funktionsweise von Systemen zur Erkennung und Verhinderung von Eindringlingen
- Unterscheidung zwischen Ansätzen zur Malware-Prävention
- Beschreiben Sie das VMware-Portfolio für intrinsische Sicherheit
- Verwenden Sie NSX-Segmentierung, um Zero-Trust-Sicherheit zu implementieren.
- Konfigurieren Sie die Benutzer- und Rollenverwaltung
- Konfiguration und Fehlerbehebung von Distributed Firewall, Identity Firewall und zeitbasierten Richtlinien
- Konfigurieren und Beheben von Problemen mit der Gateway-Sicherheit
- Verwenden Sie VMware Aria Operations™ for Logs und VMware Aria Operations™ for Networks, um NSX-Firewalls zu betreiben.
- Erläuterung der bewährten Sicherheitspraktiken in Bezug auf Gruppierung, Markierung und Regelkonfiguration
- Beschreiben Sie die Einführung von Nord-Süd- und Ost-West-Diensten
- Beschreiben Sie den Endpunktschutz
- Konfiguration und Fehlerbehebung von IDS/IPS
- Bereitstellung der NSX-Anwendungsplattform
- Konfigurieren und Beheben von Problemen mit NSX Malware Prevention

- Beschreiben Sie die Funktionen von NSX Intelligence und NSX NDR

## Kursinhalt

- Einführung in den Kurs
- Grundlagen der Sicherheit
- VMware-eigene Sicherheit
- Implementierung von Zero-Trust-Sicherheit
- Benutzer- und Rollenmanagement
- Verteilte Firewall
- Gateway-Sicherheit
- Betrieb interner Firewalls
- Netzwerk-Introspektion
- Endpunkt-Schutz
- Intrusion Detection und Prävention
- NSX-Anwendungsplattform
- NSX Malware-Prävention
- NSX Intelligence und NSX NDR

## Detaillierter Kursinhalt

### Einführung in den Kurs

- Einführung und Kurslogistik
- Kursziele

### Grundlagen der Sicherheit

- Definition der Konzepte der Informationssicherheit
- Erläuterung der verschiedenen Arten von Firewalls und ihrer Anwendungsfälle
- Beschreiben Sie die Funktionsweise von IDS/IPS
- Unterscheidung zwischen Ansätzen zur Malware-Prävention

### VMware-eigene Sicherheit

- Definieren Sie die VMware-eigene Sicherheitsstrategie
- Beschreiben Sie das VMware-Portfolio für intrinsische Sicherheit
- Erläutern Sie, wie sich NSX in die Strategie der inneren Sicherheit einfügt

### Implementierung von Zero-Trust-Sicherheit

- Definieren Sie Zero-Trust-Sicherheit
- Beschreiben Sie die fünf Säulen einer Zero-Trust-Architektur
- Definition der NSX-Segmentierung und ihrer Anwendungsfälle
- Beschreiben Sie die Schritte, die zur Durchsetzung von Zero-Trust mit NSX-Segmentierung erforderlich sind.

### Benutzer- und Rollenmanagement

- Integration von NSX und VMware Identity Manager™
- Integrieren Sie NSX und LDAP
- Beschreiben Sie die nativen Benutzer und Rollen in NSX
- Erstellen und Zuweisen benutzerdefinierter Benutzerrollen
- Erklären Sie objektbasiertes RBAC in einer mandantenfähigen Umgebung

### Verteilte Firewall

- Konfigurieren von Regeln und Richtlinien der verteilten Firewall
- Beschreiben Sie die Architektur der NSX Distributed Firewall
- Behebung allgemeiner Probleme im Zusammenhang mit NSX Distributed Firewall
- Konfigurieren Sie zeitbasierte Richtlinien
- Konfigurieren von Identity Firewall-Regeln
- Konfigurieren Sie die verteilte Firewall, um bösartige IPs zu blockieren

### Gateway-Sicherheit

- Konfigurieren von Gateway-Firewall-Regeln und Richtlinien
- Beschreiben Sie die Architektur der Gateway-Firewall
- Erkennen und Beheben häufiger Probleme mit der Gateway Firewall
- Konfigurieren Sie die TLS-Prüfung zur Entschlüsselung des Datenverkehrs für interne und externe Dienste
- URL-Filterung konfigurieren und häufige Konfigurationsprobleme erkennen

### Betrieb interner Firewalls

- Verwenden Sie VMware Aria Operations for Logs und VMware Aria Operations for Networks, um NSX-Firewalls zu betreiben.
- Erläuterung bewährter Sicherheitspraktiken in Bezug auf Gruppierung, Markierung und Regelkonfiguration

### Netzwerk-Introspektion

- Erläutern Sie die Introspektion des Netzes
- Beschreibung der Architektur und der Arbeitsabläufe bei der Einbringung von Nord-Süd- und Ost-West-Diensten
- Fehlerbehebung bei der Einführung von Nord-Süd- und Ost-West-Diensten

### Endpunkt-Schutz

- Erklären Sie den Endpunktschutz

- Beschreiben Sie die Architektur und die Arbeitsabläufe des Endpunktschutzes
- Fehlerbehebung beim Endpunktschutz

### Intrusion Detection und Prävention

- Beschreiben Sie den MITRE ATT&CK-Rahmen
- die verschiedenen Phasen eines Cyberangriffs zu erklären
- Beschreiben Sie, wie NSX-Sicherheitslösungen zum Schutz vor Cyberangriffen eingesetzt werden können.
- Konfiguration und Fehlerbehebung von verteilten IDS/IPS
- Konfiguration und Fehlerbehebung von Nord-Süd-IDS/IPS

### NSX-Anwendungsplattform

- Beschreiben Sie die NSX Application Platform und ihre Anwendungsfälle
- Identifizieren der Topologien, die für die Bereitstellung der NSX Application Platform unterstützt werden
- Bereitstellung der NSX-Anwendungsplattform
- Erläuterung der Architektur und der Dienste der NSX-Anwendungsplattform
- Validierung der NSX Application Platform-Bereitstellung und Behebung von allgemeinen Problemen

### NSX Malware-Prävention

- Identifizierung von Anwendungsfällen für NSX Malware Prevention
- Identifizierung der Komponenten in der NSX Malware Prevention-Architektur
- Beschreiben Sie die NSX Malware Prevention-Paketflüsse für bekannte und unbekannte Dateien
- Konfigurieren Sie NSX Malware Prevention für Ost-West- und Nord-Süd-Verkehr

### NSX Intelligence und NSX NDR

- Beschreiben Sie NSX Intelligence und seine Anwendungsfälle
- Erläuterung der NSX Intelligence-Funktionen zur Visualisierung, Empfehlung und Analyse des Netzwerkverkehrs
- Beschreiben Sie NSX NDR und seine Anwendungsfälle
- Erläuterung der Architektur von NSX NDR in NSX
- Beschreiben Sie die Visualisierungsfunktionen von NSX NDR

# Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

## Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

## Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

## Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

**Weltweit vertreten**
mit High-End-Trainingszentren rund um den Globus

**Mehrfach ausgezeichnet**
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

**Praxiserfahrene Experten**
mit insgesamt mehr als 19.000 Zertifizierungen


**Deutschland**
**Fast Lane Institute for Knowledge Transfer GmbH**
Tel. +49 40 25334610
info@flane.de / www.flane.de

**Österreich**
**ITLS GmbH**
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

**Schweiz**
**Fast Lane Institute for Knowledge Transfer (Switzerland) AG**
Tel. +41 44 8325080
info@flane.ch / www.flane.ch