



Enterprise Computing Solutions - Education Services

OFERTA FORMATIVA

Detalles de contacto

Avda Europa 21, 28108 Alcobendas

Email: formacion.ecs.es@arrow.com

Phone: +34 91 761 21 51

CÓDIGO:	DURACIÓN:	Precio:
VMW_NSXTIS32	40 Hours (5 días)	A consultar

Description

This five-day, hands-on training course provides you with the knowledge, skills, and tools to achieve competency in configuring, operating, and troubleshooting VMware NSX-TTM Data Center for intrinsic security. In this course, you are introduced to all the security features in NSX-T Data Center, including Distributed Firewall and Gateway Firewall, Intrusion Detection and Prevention (IDS/IPS), NSX Application Platform, NSX Malware Prevention, VMware NSX® Intelligence™, and VMware NSX® Network Detection and Response™.

In addition, you are presented with common configuration issues and given a methodology to resolve them.

This course is also available in an On Demand format. For more information, select this link: [VMware NSX-T Data Center for Intrinsic Security \[V3.2\] - On Demand](#).

Product Alignment

- VMware NSX-T Data Center 3.2.x

Objetivos

By the end of the course, you should be able to meet the following objectives:

- Define information-security-related concepts
- Explain the different types of firewalls and their use cases
- Describe the operation of intrusion detection and intrusion prevention systems
- Differentiate between Malware Prevention approaches
- Describe the VMware intrinsic security portfolio
- Implement Zero-Trust Security using VMware NSX® segmentation
- Configure user and role management
- Configure and troubleshoot Distributed Firewall, Identity Firewall, and time-based policies
- Configure and troubleshoot Gateway Security
- Use VMware vRealize® Log Insight™ for NSX™ and VMware vRealize® Network Insight™ to operate NSX firewalls
- Explain the security best practices related to grouping, tagging, and rule configuration
- Describe north-south and east-west service insertion
- Describe endpoint protection
- Configure and troubleshoot IDS/IPS
- Deploy NSX Application Platform
- Configure and troubleshoot NSX Malware Prevention
- Describe the capabilities of NSX Intelligence and NSX Network Detection and Response

Público

Experienced security administrators

Requisitos Previos

You should also have the following understanding or knowledge:

- Good understanding of TCP/IP services and protocols
- Knowledge and working experience of network security, including:
 - L2 through L7 firewalling
 - Intrusion detection and prevention systems
 - Malware prevention systems
- Knowledge of and working experience with VMware vSphere® environments and KVM-based environments

The VMware Certified Technical Associate - Network Virtualization is recommended.

Programa

1 Course Introduction

- Introductions and course logistics
- Course objectives

2 Security Basics

- Define information-security-related concepts
- Explain the different types of firewalls and their use cases
- Describe the operation of IDS/IPS
- Differentiate between Malware Prevention approaches

3 VMware Intrinsic Security

- Define the VMware intrinsic security strategy
- Describe the VMware intrinsic security portfolio
- Explain how NSX-T Data Center aligns with the intrinsic security strategy

4 Implementing Zero-Trust Security

- Define Zero-Trust Security
- Describe the five pillars of a Zero-Trust Architecture
- Define NSX segmentation and its use cases
- Describe the steps needed to enforce Zero-Trust with NSX segmentation

5 User and Role Management

- Integrate NSX-T Data Center and VMware Identity Manager™
- Integrate NSX-T Data Center and LDAP
- Describe the native users and roles in NSX-T Data Center
- Create and assign custom user roles

6 Distributed Firewall

- Configure Distributed Firewall rules and policies
- Describe the NSX Distributed Firewall architecture
- Troubleshoot common problems related to NSX Distributed Firewall
- Configure time-based policies
- Configure Identity Firewall rules

7 Gateway Security

- Configure Gateway Firewall rules and policies
- Describe the architecture of the Gateway Firewall
- Identify and troubleshoot common Gateway Firewall issues
- Configure TLS Inspection to decrypt traffic for both internal and external services
- Configure URL filtering and identify common configuration issues

8 Operating Internal Firewalls

- Use vRealize Log Insight for NSX and vRealize Network Insight to operate NSX firewalls
- Explain security best practices related to grouping, tagging, and rule configuration

9 Network Introspection

- Explain network introspection
- Describe the architecture and workflows of north-south and east-west service insertion
- Troubleshoot north-south and east-west service insertion

10 Endpoint Protection

- Explain endpoint protection
- Describe the architecture and workflows of endpoint protection
- Troubleshoot endpoint protection

11 Intrusion Detection and Prevention

- Describe the MITRE ATT&CK framework
- Explain the different phases of a cyber attack
- Describe how NSX security solutions can be used to protect against cyber attacks
- Configure and troubleshoot Distributed IDS/IPS
- Configure and troubleshoot North-South IDS/IPS

12 NSX Application Platform

- Describe NSX Application Platform and its use cases
- Identify the topologies supported for the deployment of NSX Application Platform
- Deploy NSX Application Platform
- Explain the NSX Application Platform architecture and services
- Validate the NSX Application Platform deployment and troubleshoot common issues

13 NSX Malware Prevention

- Identify use cases for NSX Malware Prevention
- Identify the components in the NSX Malware Prevention architecture
- Describe the NSX Malware Prevention packet flows for known and unknown files
- Configure NSX Malware Prevention for east-west and north-south traffic

14 NSX Intelligence and NSX Network Detection and Response

- Describe NSX Intelligence and its use cases
- Explain NSX Intelligence visualization, recommendation, and network traffic analysis capabilities
- Describe NSX Network Detection and Response and its use cases
- Explain the architecture of NSX Network Detection and Response in NSX-T Data Center
- Describe the visualization capabilities of NSX Network Detection and Response

Fechas Programadas

A petición. Gracias por [contactarnos](#).

Información Adicional

[Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.](#)