ARROW

Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå os her

.

Email: training.ecs.dk@arrow.com
Phone: +45 7025 4500

VMware NSX-T Data Center for Intrinsic Security [V3.1]

CODE:	LENGTH:	PRICE:
VMW_NSXTIS31	40 Hours (5 dage)	kr 25,600.00

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-T™ Data Center for intrinsic security. In this course, you are introduced to all the security features in NSX-T Data Center, including distributed and gateway firewall, Intrusion Detection and Prevention (IDS/IPS), VMware NSX® Intelligence™, and Network Detection and Response (NDR).
In addition, you are presented with common configuration issues and given a methodology to resolve them.

Objectives

By the end of the course, you should be able to meet the following objectives:
• Define information security related concepts
• Explain different types of firewalls and their use cases
• Describe the operation of Intrusion Detection and Intrusion Prevention Systems
• 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™, VMware vRealize® Network Insight™, and NSX Intelligence to operate NSX firewalls and generate security recommendations
• Explain security best practices related to grouping, tagging, and rule configuration
• Describe North-South and East-West service insertion
• Describe Endpoint Protection
• Configure and troubleshoot Distributed IDS/IPS
• Describe the capabilities of Network Detection and Response

Audience

• Experienced security administrators

Prerequisites

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-L7 Firewalling
  • Intrusion Detection and Prevention Systems
• Knowledge and working experience of VMware vSphere® environments and KVM-based environments
The VMware Certified Technical Associate - Network Virtualization is recommended.

Programme

1 Course Introduction
• Introductions and course logistics
• Course objectives

2 Security Basics
• Define information security related concepts
• Explain different types of firewalls and their use cases
• Describe the operation of Intrusion Detection and Intrusion Prevention Systems

3 VMware Intrinsic Security
• Define VMware intrinsic security strategy
• Describe VMware intrinsic security portfolio
• Explain how NSX-T Data Center aligns in 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

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

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
7 Gateway Security
• Configure gateway firewall rules and policies
• Describe the architecture of the gateway firewall
• Identify and troubleshoot common gateway firewall issues
• Configure URL analysis and identify common configuration issues
8 Operating Internal Firewalls
• Use vRealize Log Insight, vRealize Network Insight, and NSX Intelligence to operate NSX firewalls
• Explain NSX Intelligence visualization and recommendation capabilities
• 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 Advanced Threat 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
• Describe the capabilities of Network Detection and Response

Session Dates

På anmodning. Kontakt os venligst

Yderligere Information

Denne træning er også tilgængelig som træning på stedet. Kontakt os for at finde ud af mere.