vmware LEARNING

VMware NSX-T Data Center: What's New

Course Overview

In this three-day, hands-on training course, you explore the new features and enhancements in VMware NSX-T™ Data Center 3.2. You will be introduced to all new security features in NSX-T Data Center 3.2, including NSX Application Platform, NSX Malware Prevention, NSX Intrusion Detection and Prevention, URL Filtering, VMware NSX® Intelligence™, and VMware NSX® Network Detection and Response™.

This course also discusses the architectural and operational changes introduced in version 3.2 and discusses the enhancements to OSPF, VMware NSX® Advanced Load Balancer™, and NSX Federation.

Course Objectives

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

- Describe the architectural and operations enhancements in NSX-T Data Center 3.2
- Configure OSPF in NSX-T Data Center 3.2
- Describe the NSX security architecture and features of NSX-T Data Center 3.2
- Configure Distributed Firewall on VDS for security use cases
- Configure URL Filtering and Identity Firewall on NSX Edge nodes
- Configure NSX Intrusion Detection and Prevention for east-west traffic
- Deploy NSX Application Platform
- Configure NSX Malware Prevention for east-west and north-south traffic
- Analyze the networking secure posture and threats with NSX Intelligence and NSX Network Detection and Response
- Deploy the NSX Advanced Load Balancer components
- Describe the NSX Federation enhancements in NSX-T Data Center 3.2

Target Audience

Network and security administrators, IT managers, VMware partners, and individuals responsible for implementing and managing the NSX-T Data Center deployments

Prerequisites

This course requires completion of the VMware NSX-T Data Center: Install, Configure, Manage course or equivalent knowledge and administration experience with NSX-T Data Center 3.0 or above.

Solid understanding of the concepts presented in the Kubernetes Fundamentals course is also required.

The following knowledge is beneficial:

- Understanding of TCP/IP services and protocols
- Knowledge and working experience of computer networking, including switching and routing technologies (L2-L3) and L2-L7 firewall

- Knowledge and working experience with VMware vSphere® environments
- Knowledge and working experience with Kubernetes or vSphere with Tanzu environments.

The VMware Certified Professional – Network Virtualization (2021) certification is recommended.

Course Delivery Options

- Classroom
- Live Online
- Private Training
- On Demand

Product Alignment

VMware NSX-T Data Center 3.2

Course Modules

1 Course Introduction
- Introduction and course logistics
- Course objectives

2 NSX Architecture and Operations
- Review key components of the NSX-T Data Center architecture
- Explain the Management Plane to Policy Promotion tool
- Compare Live Traffic Analysis with traditional network traffic analysis methods
- Identify how Fabric View helps visualize the underlying network fabric of a topology
- Recognize improvements in historical trending for network and system monitoring
- Explain how the fabric MTU health check can be used to identify an MTU mismatch

3 OSPF Routing Protocol
- Explain the core concepts of OSPF routing
- Define the OSPF use cases in NSX-T Data Center
- Explain the Tier-0 gateway topologies with OSPF
- Configure OSPF in NSX-T Data Center

4 NSX Security Overview
- Describe the NSX security architecture and main components
- Identify the use cases for NSX Distributed Security
- Identify the use cases for NSX Gateway Security
- Describe NSX Network Detection and Response

5 Distributed Firewall on VDS: Use Case for Security
- Identify the distributed firewall on VDS requirements
- Configure the distributed firewall on VDS
- Validate the distributed firewall on VDS configurations

6 Gateway Security
- Identify use cases for URL filtering
- Describe the URL filtering architecture
- Configure URL filtering
- Describe the uses cases, architecture, and components of Identity Firewall
- Configure Identity Firewall for north-south traffic

7 Intrusion Detection and Prevention
- Describe the MITRE ATT&CK framework
- Explain the phases of a cyberattack
- Describe features and methods used by intrusion detection and prevention systems
- Identify VMware NSX® Distributed IDS/IPS™ use cases
- Describe the NSX Distributed IDS/IPS terminology and architecture
- Configure NSX Distributed IDS/IPS

8 NSX Application Platform
- Describe NSX Application Platform and its use cases
- Define the core concepts of vSphere with Tanzu
- Deploy NSX Application Platform on vSphere with Tanzu
- Explain the NSX Application Platform architecture and services
- Scale out and scale up NSX Application Platform

9 Malware Prevention
- Describe techniques used in 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

10 NSX Intelligence and NSX Network Detection and Response
- Describe the NSX Intelligence architecture and core components
- Install NSX Intelligence
- Describe NSX Intelligence visualization, recommendation, and Suspicious Traffic Detection enhancements
- Describe NSX Network Detection and Response architecture and its use cases
- Activate NSX Network Detection and Response

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VMWARE SKU: EDU-NSXTWN32-OE REV. 1/2022

- Describe the visualization capabilities of NSX Network Detection and Response

11 NSX Advanced Load Balancer

- Describe NSX Advanced Load Balancer and its use cases
- Explain the NSX Advanced Load Balancer architecture
- Deploy NSX Advanced Load Balancer
- Explain the NSX Advanced Load Balancer components and how they manage traffic
- Configure virtual IP addresses, virtual services, and server pools
- Perform basic troubleshooting of virtual services, server pools, and service engines

12 NSX Federation Enhancements

- Recognize NSX Federation use cases
- Describe the main components of the NSX Federation architecture
- Explain LDAP support for the Global Manager
- Explain the purpose of firewall drafts on the NSX Global Manager
- Explain NSX Federation support for tag-based replication
- Describe ways to monitor NSX Federation components

Contact

If you have questions or need help registering for this course, click here.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com