

Szkolenie: HPE
VMware NSX: Install, Configure, Manage



Cel szkolenia:

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

- Configure and deploy NSX components for management and control
- Describe basic NSX layer 2 networking
- Configure, deploy, and use logical switch networks
- Configure and deploy NSX distributed router appliances to establish east-west connectivity
- Configure and deploy VMware NSX® Edge™ services gateway appliances to establish north-south connectivity
- Configure NSX L2 bridging
- Configure and use all main features of the NSX Edge services gateway
- Configure NSX Edge firewall rules to restrict network traffic
- Configure NSX distributed firewall rules to restrict network traffic
- Configure Service Composer policies
- Configure an identity-aware firewall
- Describe NSX data security
- Use the cross-vCenter NSX feature

Audience

Experienced system or network administrators

Plan szkolenia:

- Course Introduction
 - Introductions and course logistics
 - Review course objectives
- Introduction to vSphere Networking
 - Describe VMware vSphere® networking components
 - Describe vSphere standard switches
 - Describe vSphere distributed switches
- Introduction to NSX

- Describe the benefits of NSX
- Identify NSX key use cases
- NSX Architecture
 - Describe the NSX architecture
 - Describe the cloud management, management, control, and data planes of NSX
 - Identify the component interactions
 - Describe the VMware NSX® Controller™ cluster and its functions
 - Explain the NSX Controller workload distribution
- NSX Infrastructure Preparation
 - Explain the steps required for an NSX installation
 - Describe what is involved in planning an NSX deployment
 - Describe the NSX Controller cluster and deployment
 - Describe NSX Controller cluster high availability and load distribution
 - Explain how to deploy and configure the NSX Controller cluster
 - Explain the workflow involved in host preparation
- NSX Logical Switch Networks
 - Explain transport zones, VXLANs, and VXLAN tunnel End Points (VTEPs)
 - Describe the procedure for preparing the infrastructure for virtual networking
 - Describe the configuration of vSphere distributed switches for VXLAN
 - Identify the components involved in NSX logical switching
 - Define VLANs for VXLAN
- NSX Logical Routing
 - Explain the east-west and north-south routing concepts
 - Define the NSX distributed logical router
 - Explain the logical router, interfaces, and interface addresses
 - Describe the management and control plane interaction
 - Describe logical router deployment models and two-tier routing for east-west traffic
 - Explain the common topologies of an NSX Edge services gateway
- Advanced NSX Logical Routing
 - Describe how routers connect remote networks
 - Explain route redistribution methods
 - Describe less-than-or-equal (LE) and greater-than-or-equal (GE) configurations
 - Describe routing event notification enhancements
 - Configure equal-cost multipath (ECMP) routing
 - Describe high availability for NSX Edge service gateways
- NSX L2 Bridging

- Explain L2 bridging use cases
- Describe software and hardware L2 bridging between VXLAN and VLANs
- Discuss L2 bridging packet flows
- NSX Edge Services
 - Describe the NSX Edge services
 - Explain how Network Address Translation (NAT) works
 - Explain NAT64
 - Explain the function of load balancing
 - Explain one-armed and inline load-balancing architectures
 - Explain the DHCP and DNS services for NSX Edge
- NSX Edge VPN Services
 - Describe the NSX Edge VPN services
 - Describe the VPN use cases
 - Configure a L2 VPN on an NSX Edge instance
 - Configure an NSX Edge instance for IPsec VPN services
 - Explain NSX Edge SSL VPN-Plus services
 - Configure NSX Edge SSL VPN-Plus server settings
- NSX Security Services
 - Describe the policy enforcement of the distributed firewall
 - Describe virtualization context-awareness
 - Explain custom network and security containers
 - Describe the architecture of an NSX Edge firewall
 - Explain DHCP snooping
 - Explain ARP snooping
- NSX Advanced Security Services
 - Describe NSX SpoofGuard
 - Identify how tags enable dynamic security service chains
 - Explain Service Composer groups, policies, and tags
 - Describe the Identity Firewall architecture
 - Explain Application Rule Manager
 - Explain how to create a monitoring session
- NSX Introspection Services
 - Describe the types of introspection services
 - Describe the installation and configuration of Guest and Network Introspection
 - Summarize Guest and Network Introspection alarms, events, and audit messages
- Cross-vCenter NSX

- Describe cross-vCenter features and use cases
- Identify VMware NSX® Manager™ roles and NSX Controller cluster placement
- Deploy universal logical networks
- Explain the design considerations for cross-vCenter NSX

Wymagania:

This course requires completion of one of the following prerequisites:

- Understanding of enterprise switching and routing
- Knowledge of TCP/IP services
- Experience with firewalls and firewall rule sets
- Understanding of concepts presented in the VMware Data Center Virtualization Fundamentals course
- Understanding of the concepts presented in the VMware Introduction to Network Virtualization with NSX course

Poziom trudności



Certyfikaty:

After completing the course, participants receive a certificate of completion of course.

Prowadzący:

Authorized VMware Trainer.