



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

What is the VMware recommended way to deploy a virtual NSX Edge Node?

- A. Through the NSX UI
- B. Through automated or interactive mode using an ISO
- C. Through the vSphere Web Client
- D. Through the OVF command line tool

Suggested Answer: A

Community vote distribution

A (100%)

🗉 👤 **General_HCCIE** 3 months, 3 weeks ago

Selected Answer: A

the recommended options is through NSX UI

upvoted 2 times

🗉 👤 **amorcle** 7 months, 4 weeks ago

Selected Answer: A

Install NSX Edge on an ESXi host using NSX Manager UI (recommended method),

<https://docs.vmware.com/en/VMware-NSX/4.1/installation/GUID-E9A01C68-93E7-4140-B306-19CD6806199F.html>

upvoted 3 times

🗉 👤 **yorchiluis** 7 months, 4 weeks ago

Selected Answer: A

<https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-E9A01C68-93E7-4140-B306-19CD6806199F.html>

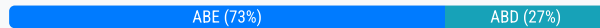
upvoted 2 times

Which three selections are capabilities of Network Topology? (Choose three.)

- A. Display how the different NSX components are interconnected.
- B. Display the VMs connected to Segments.
- C. Display how the Physical components are interconnected.
- D. Display the uplinks configured on the Tier-1 Gateways.
- E. Display the uplinks configured on the Tier-0 Gateways.

Suggested Answer: ABE

Community vote distribution



amorcle Highly Voted 5 months, 3 weeks ago

Selected Answer: ABE

In the official guide
upvoted 5 times

General_HCCIE Most Recent 3 months, 3 weeks ago

Selected Answer: ABE

ABE is the right answer
upvoted 3 times

Arslan7 7 months ago

Selected Answer: ABD

Explanation

According to the VMware NSX Documentation, these are three of the capabilities of Network Topology, which is a graphical representation of your network infrastructure in NSX:

- * Display how the different NSX components are interconnected: You can use Network Topology to view how your segments, gateways, routers, firewalls, load balancers, VPNs, and other NSX components are connected and configured in your network.
- * Display the uplink configured on the Tier-0 Gateways: You can use Network Topology to view the uplink interface and segment that connect your tier-0 gateways to your physical network. You can also view the VLAN ID and IP address of the uplink interface.
- * Display the VMs connected to Segments: You can use Network Topology to view the VMs that are attached to your segments. You can also view the IP address and MAC address of each VM.

upvoted 3 times

aothman 3 months ago

you mean ABE ?

upvoted 2 times



An NSX administrator has deployed a single NSX Manager node and will be adding two additional nodes to form a 3-node NSX Management Cluster for a production environment. The administrator will deploy these two additional nodes and Cluster VIP using the NSX UI. What two are the prerequisites for this configuration? (Choose two.)

- A. The cluster configuration must be completed using API.
- B. All nodes must be in the same subnet.
- C. All nodes must be in separate subnets.
- D. A compute manager must be configured.
- E. NSX Manager must reside on a Windows Server.

Suggested Answer: BD

Community vote distribution

BD (100%)

  **amorcle** 5 months, 3 weeks ago

Selected Answer: BD

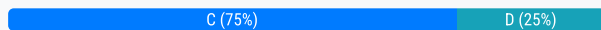
As in the official guide
upvoted 2 times

Which two commands does an NSX administrator use to check the IP address of the VMkernel port for the Geneve protocol on the ESXi transport node? (Choose two.)

- A. net-dvs
- B. esxcfg-nics -l
- C. esxcli network ip interface ipv4 get
- D. esxcfg-vmknics -l
- E. esxcli network nic list

Suggested Answer: C

Community vote distribution



🗲️ 👤 **wako565** 1 month, 2 weeks ago

Selected Answer: C

C & D the question say "chose two"
upvoted 1 times

🗲️ 👤 **Relbert** 1 month, 3 weeks ago

Selected Answer: C

C & D : both are correcl, this is a multiple choice question
upvoted 1 times

🗲️ 👤 **_danielgurgel** 2 months, 3 weeks ago

Selected Answer: C

Are the correct commands
upvoted 1 times

🗲️ 👤 **General_HCCIE** 3 months, 3 weeks ago

Selected Answer: D

C & D : both are correcl, this is a multiple choice question
upvoted 2 times

🗲️ 👤 **amorcle** 5 months, 3 weeks ago

Selected Answer: C

C and D
Like in the official guide. There are two choices not one
upvoted 3 times


Which two are supported by L2 VPN clients? (Choose two.)

- A. NSX Autonomous Edge
- B. NSX Edge
- C. NSX for vSphere Edge
- D. 3rd party Hardware VPN Device

Suggested Answer: AB

Community vote distribution

AB (100%)

 **Ssilva521** 4 weeks ago

Selected Answer: AB

The following L2 VPN clients are recommended:

1. NSX Managed NSX Edge in a separate NSX Managed environment.
 - Overlay and VLAN segments can be extended.
2. Autonomous Edge:
 - Enables L2 VPN access from a non-NSX environment to NSX environments.
 - Deployed by using an OVF file on a host that is not managed by NSX.
 - Only VLAN segments can be extended.


upvoted 1 times

 **General_HCCIE** 3 months, 3 weeks ago

Selected Answer: AB

the correct answer is AB

upvoted 1 times

 **amorcle** 5 months, 3 weeks ago

Selected Answer: AB

Correct, as in the official guide

upvoted 1 times

 **Salanazi** 6 months ago

Selected Answer: AB

This correct

upvoted 1 times

 **Arslan7** 7 months ago

Selected Answer: AB

Saw in the ICM 4.0 p.595.

The following L2 VPN clients are recommended:

1. NSX Managed NSX Edge in a separate NSX Managed environment.
 - Overlay and VLAN segments can be extended.
2. Autonomous Edge:
 - Enables L2 VPN access from a non-a NSX environment to NSX environments.
 - Deployed by using an OVF file on a host that is not managed by NSX.
 - Only VLAN segments can be extended.

upvoted 1 times

As part of an organization's IT security compliance requirement, NSX Manager must be configured for 2FA (two-factor authentication). What should an NSX administrator have ready before the integration can be configured?

- A. Active Directory LDAP integration with ADFS
- B. VMware Identity Manager with NSX added as a Web Application
- C. VMware Identity Manager with an OAuth Client added
- D. Active Directory LDAP integration with OAuth Client added

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **General_HCCIE** 3 months, 3 weeks ago

Selected Answer: C

C is the correct answer
upvoted 2 times

🗨️ 👤 **amorcle** 5 months, 3 weeks ago

Selected Answer: C

Correct. It's in the official guide.
upvoted 2 times



What should an NSX administrator check to verify that VMware Identity Manager integration is successful?

- A. From the NSX UI the status of the VMware Identity Manager Integration must be "Enabled".
- B. From the NSX CLI the status of the VMware Identity Manager Integration must be "Configured".
- C. From VMware Identity Manager the status of the remote access application must be green.
- D. From the NSX UI the URI in the address bar must have "local=false" part of it.

Suggested Answer: A

Community vote distribution

A (100%)

  **Ssilva521** 4 weeks ago



Selected Answer: A

You can validate the successful communication between NSX and VMware Identity Manager from the NSX UI.

Navigate to System > Settings > User Management > Authentication Providers > VMware Identity Manager to validate the VMware Identity Manager integration.

If the integration is successful, the VMware Identity Manager integration appears as Enabled.

upvoted 1 times

  **amorcle** 5 months, 3 weeks ago

Selected Answer: A

As in the official guide.

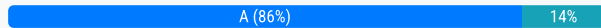
upvoted 3 times

An administrator has been tasked with implementing the SSL certificates for the NSX Manager Cluster VIP.
Which is the correct way to implement this change?

- A. Send an API call to `https://<nsx-mgr>/api/v1/cluster/api-certificate?action=set_cluster_certificate&certificate_id=<certificate_id>`
- B. Send an API call to `https://<nsx-mgr>/api/v1/node/services/http?action=apply_certificate&certificate_id=<certificate_id>`
- C. SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate node install <certificate_id>`
- D. SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate vip install <certificate_id>`

Suggested Answer: A

Community vote distribution



🗳️ 👤 **Ssilva521** 4 weeks ago

Selected Answer: A

You can replace the certificate for a manager node or the manager cluster virtual IP (VIP) by making an API call:

- To replace the certificate of a manager node, use the POST API call:

`https://<nsx-mgr>/api/v1/node/services/http?action=apply_certificate&certificate_id=<certificate_id>`

- To replace the certificate of the manager cluster VIP, use the POST API call:

`https://<nsx-mgr>/api/v1/cluster/api-certificate?action=set_cluster_certificate&certificate_id=<certificate_id>`

upvoted 1 times

🗳️ 👤 **General_HCCIE** 3 months, 3 weeks ago

Selected Answer: A

A is the correct, importing via UI and attached via API

upvoted 2 times

🗳️ 👤 **visse** 3 months, 3 weeks ago

Selected Answer: A

<https://techdocs.broadcom.com/us/en/vmware-tanzu/standalone-components/tanzu-kubernetes-grid-integrated-edition/1-19/tkgi/nsxt-install-tls-certs.html>

upvoted 1 times

🗳️ 👤 **visse** 3 months, 2 weeks ago

<https://techdocs.broadcom.com/us/en/vmware-cis/nsx/vmware-nsx/4-1/administration-guide/certificates/importing-certificates/replace-certificates-through-api.html>

upvoted 2 times

🗳️ 👤 **electro165** 5 months, 2 weeks ago

Selected Answer: D

o implement SSL certificates for the NSX Manager Cluster VIP, you need to install the certificate specifically for the VIP. This is done by accessing the NSX Manager node via SSH and using the `nsxcli` command.

The correct command to install a certificate for the Cluster VIP is:

`nsxcli cluster certificate vip install <certificate_id>`

This command is used to apply the certificate to the VIP, ensuring secure connections to the NSX Manager Cluster.

upvoted 1 times

🗳️ 👤 **amorcle** 5 months, 3 weeks ago

Selected Answer: A

A as says in the official doc.

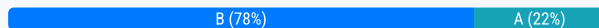
upvoted 2 times

An administrator wants to validate the BGP connection status between the Tier-0 Gateway and the upstream physical router. What sequence of commands could be used to check this status on NSX Edge node?

- A. - enable <LR-D>
- get vrf <ID>
- show bgp neighbor
- B. - get gateways
- vrf <number>
- get bgp neighbor
- C. - set vrf <ID>
- show logical-routers
- show <LR-D> bgp
- D. - show logical-routers
- get vrf
- show ip route bgp

Suggested Answer: B

Community vote distribution



General_HCCIE 3 months, 3 weeks ago

Selected Answer: B

there is no enable in the NSX Edge shell, the correct order is get gateways to see all the available gateways, then select by using the vrf and id of the logical gateway in this case the logical gateway need to be SR, then sget bgp neighbor
upvoted 1 times

putifarri 3 months, 3 weeks ago

Selected Answer: B

there isn't a command in NSX that starts with show, so for me that discard all the others
upvoted 3 times

electro165 5 months, 2 weeks ago

Selected Answer: A

To validate the BGP connection status between the Tier-0 Gateway and the upstream physical router, the following steps are typically used on an NSX Edge node:

Enable the Logical Router (LR-D): This step activates the specific logical router in which the BGP configuration is applied.

Get the VRF (Virtual Routing and Forwarding) ID: This command retrieves the VRF information to ensure that BGP is configured in the correct VRF.

Show BGP neighbor: This command displays the status of the BGP neighbor connection, showing if the BGP session is up or down and other related details.

B, C, and D are not correct because they do not provide the correct sequence or relevant commands for directly checking the BGP status from the NSX Edge node.

upvoted 2 times

amorcle 5 months, 3 weeks ago

Selected Answer: B

As in the official guide.
upvoted 3 times


What is VMware's recommendation for the minimum MTU requirements when planning an NSX deployment?

- A. MTU should be set to 1700 or greater across the data center network including inter-data center connections.
- B. MTU should be set to 1500 or less only on inter-data center connections.
- C. Configure Path MTU Discovery and rely on fragmentation.
- D. MTU should be set to 1550 or less across the data center network including inter-data center connections.

Suggested Answer: A

Community vote distribution

A (100%)

 **amorcle** 5 months, 3 weeks ago

Selected Answer: A

VMware recommends setting the MTU to at least 1700 bytes to ensure optimal performance and to future-proof the environment. This helps accommodate various functions and potential expansions

upvoted 1 times


In which VPN type are the Virtual Tunnel interfaces (VTI) used?

- A. SSL-based VPN
- B. Route & SSL based VPNs
- C. Policy & Route based VPNs
- D. Route-based VPN

Suggested Answer: D

Community vote distribution

D (100%)

 **amorcle** 5 months, 3 weeks ago

Selected Answer: D

As the official documentation

upvoted 3 times

In an NSX environment, an administrator is observing low throughput and congestion between the Tier-0 Gateway and the upstream physical routers.


Which two actions could address low throughput and congestion? (Choose two.)

- A. Configure ECMP on the Tier-0 gateway.
- B. Configure a Tier-1 gateway and connect it directly to the physical routers.
- C. Deploy Large size Edge node/s.
- D. Configure NAT on the Tier-0 gateway.
- E. Add an additional vNIC to the NSX Edge node.

Suggested Answer: AC

Community vote distribution

AC (100%)

 **amorcle** 5 months, 3 weeks ago

Selected Answer: AC

A C As in the official vmware guide.

upvoted 2 times

A company security policy requires all users to log into applications using a centralized authentication system.



Which two authentication, authorization, and accounting (AAA) systems are available when integrating NSX with VMware Identity Manager? (Choose two.)

- A. RSA SecureID
- B. SecureDAP
- C. RADIUS 2.0
- D. LDAP and OpenLDAP based on Active Directory (AD)
- E. Keygen Enterprise

Suggested Answer: AD

Community vote distribution

AD (100%)

  **amorcle** 5 months, 3 weeks ago

Selected Answer: AD

RADIUS 2.0 doesn't exist. RADIUS, but if it was radius?

upvoted 2 times

  **shell_terminator** 1 month, 3 weeks ago

I think the same, RADIUS is compatible with AAA

upvoted 1 times


An NSX administrator would like to export syslog events that capture messages related to NSX host preparation events. Which message ID (msgid) should be used in the syslog export configuration command as a filter?

- A. FABRIC
- B. SYSTEM
- C. GROUPING
- D. MONITORING

Suggested Answer: A

Community vote distribution

A (100%)

🗉  **amorcle** 5 months, 3 weeks ago

Selected Answer: A

As in the official vmware guide
upvoted 2 times

An NSX administrator wants to create a Tier-0 Gateway to support equal cost multi-path (ECMP) routing. Which failover detection protocol must be used to meet this requirement?

- A. Host Standby Router Protocol (HSRP)
- B. Beacon Probing (BP)
- C. Virtual Router Redundancy Protocol (VRRP)
- D. Bidirectional Forwarding Detection (BFD)

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **Ssilva521** 3 weeks, 6 days ago

Selected Answer: D

Failover Detection Mechanisms

The failover process uses the following mechanisms to check the connectivity between tiers:

- Bidirectional Forwarding Detection (BFD): On the management and overlay network
 - Dynamic Routing Protocol (BGP or OSPF): On the uplinks
- upvoted 1 times

🗨️ 👤 **amorcle** 5 months, 3 weeks ago

Selected Answer: D

As in the official vmware guide.

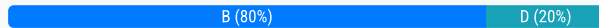
upvoted 2 times

An administrator has connected two virtual machines on the same overlay segment. Ping between both virtual machines is successful. What type of network boundary does this represent?

- A. Layer 2 bridge
- B. Layer 2 broadcast domain
- C. Layer 2 VPN
- D. Layer 3 route

Suggested Answer: B

Community vote distribution



electro165 5 months, 2 weeks ago

Selected Answer: B

In this scenario, both virtual machines are on the same overlay segment, meaning they are part of the same Layer 2 network. In a Layer 2 broadcast domain, devices can communicate with each other at the Ethernet level, meaning they are in the same broadcast domain, and broadcast traffic can reach all devices in the same domain.

Layer 2 bridge (A): This refers to connecting two different Layer 2 segments together, but in the case described, the VMs are already on the same segment, so this does not apply.

Layer 2 VPN (C): This would typically be used to extend a Layer 2 network over a Layer 3 infrastructure, not applicable in this scenario where the VMs are already on the same segment.

Layer 3 route (D): A Layer 3 boundary implies routing between different subnets or networks, which is not the case here, as the VMs are in the same network.

So, the scenario describes a Layer 2 broadcast domain where both VMs can communicate.

upvoted 4 times

amorcle 5 months, 3 weeks ago

Selected Answer: D

As in the official vmware guide

upvoted 1 times

amorcle 5 months, 3 weeks ago

I'm sorry, the correct choice is B

upvoted 4 times

What are two supported host switch modes? (Choose two.)

- A. Overlay Datapath
- B. Secure Datapath
- C. Standard Datapath
- D. Enhanced Datapath
- E. DPDK Datapath

Suggested Answer: CD

Community vote distribution

CD (100%)

  **Ssilva521** 3 weeks, 6 days ago



Selected Answer: CD

VDS Operational Modes

VDS switches can be configured in one of three modes based on performance requirements:

- Standard datapath: Configured for regular workloads, where normal workload traffic throughput is expected.
- Enhanced Datapath - Performance: Configured for telecom workloads, where high traffic throughput is expected on the workloads.
- Enhanced Datapath - Standard: An interrupt-driven version of Enhanced datapath.

upvoted 1 times

  **amorcle** 5 months, 3 weeks ago

Selected Answer: CD

Ok, as in the vmware guide

upvoted 1 times



Which is an advantage of an L2 VPN in an NSX 4.x environment?

- A. Achieve better performance
- B. Use the same broadcast domain
- C. Enables Multi-Cloud solutions
- D. Enables VM mobility with re-IP

Suggested Answer: B

Community vote distribution

B (100%)

  **amorcle** 5 months, 3 weeks ago

Selected Answer: B

As in the official vmware guide.

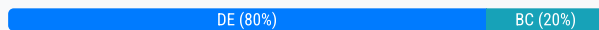
upvoted 1 times

Which two steps must an NSX administrator take to integrate VMware Identity Manager in NSX to support role-based access control? (Choose two.)

- A. Create a SAML authentication in VMware Identity Manager using the NSX Manager FQDN.
- B. Add NSX Manager as a Service Provider (SP) in VMware Identity Manager.
- C. Enter the Identity Provider (IdP) metadata URL in NSX Manager.
- D. Enter the service URL, Client Secret, and SSL thumbprint in NSX Manager.
- E. Create an OAuth 2.0 client in VMware Identity Manager.

Suggested Answer: DE

Community vote distribution



electro165 5 months, 2 weeks ago

Selected Answer: BC

To integrate VMware Identity Manager (vIDM) with NSX for role-based access control (RBAC), the administrator needs to set up the communication between the two systems using SAML or OAuth protocols.

B. Add NSX Manager as a Service Provider (SP) in VMware Identity Manager: In order to integrate NSX with VMware Identity Manager, NSX Manager must be added as a Service Provider (SP) in vIDM. This allows NSX to recognize the identity source managed by vIDM.

C. Enter the Identity Provider (IdP) metadata URL in NSX Manager: NSX Manager needs to be configured with the Identity Provider (IdP) metadata URL from VMware Identity Manager. This URL helps NSX to authenticate and interact with VMware Identity Manager.

upvoted 1 times

TheNorthernGeek 8 months ago

Selected Answer: DE

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-EAAD1FBE-F750-4A5A-A3BF-92B1E7D016FE.html>

upvoted 2 times

wako565 1 month, 2 weeks ago

Hey the exam is version 4 not 3.2.

upvoted 1 times

sajiby3k 8 months ago

Selected Answer: DE

Correct is D, E

upvoted 2 times

Which of the two following characteristics about NAT64 are true? (Choose two.)

- A. NAT64 requires the Tier-1 gateway to be configured in active-active mode.
- B. NAT64 is stateless and requires gateways to be deployed in active-standby mode.
- C. NAT64 is supported on Tier-0 and Tier-1 gateways.
- D. NAT64 is supported on Tier-1 gateways only.
- E. NAT64 requires the Tier-1 gateway to be configured in active-standby mode.

Suggested Answer: CE

Community vote distribution



Ssilva521 4 weeks ago

Selected Answer: CE

About NAT64

NAT64 is a mechanism for translating IPv6 packets into IPv4 packets:

- A. NAT64 allows IPv6-only clients to communicate with IPv4 servers.
 - B. Changes are not needed in the IPv6 or IPv4 nodes.
 - C. NAT64 is supported on Tier-0 and Tier-1 gateways.
 - D. NAT64 is stateful and requires the Tier-0 gateway to be deployed in active-standby mode.
 - E. NAT64 requires the Tier-1 gateway
- upvoted 1 times

kernelkraut 1 month, 3 weeks ago

Selected Answer: BC

This is directly from the training course - So I am going with B and C.

About NAT64

NAT64 is a mechanism for translating IPv6 packets into IPv4 packets:

1. NAT64 allows IPv6-only clients to communicate with IPv4 servers.
 2. Changes are not needed in the IPv6 or IPv4 nodes.
 3. NAT64 is supported on Tier-0 and Tier-1 gateways.
 4. NAT64 is stateful and requires the Tier-0 gateway to be deployed in active-standby mode.
 5. NAT64 requires the Tier-1 gateway to be configured with an active-standby edge cluster.
- upvoted 1 times

wako565 1 month, 2 weeks ago

For this reason B is not correct nat is statefull not stateless

upvoted 1 times

amorcle 5 months, 3 weeks ago

Selected Answer: CE

Correct, it's the same in the official guide.

upvoted 2 times

Which VMware GUI tool is used to identify problems in a physical network?

- A. VMware Aria Operations Networks
- B. VMware Aria Automation
- C. VMware Site Recovery Manager
- D. VMware Aria Orchestrator

Suggested Answer: A

Community vote distribution

A (100%)

🗉 👤 **CCT2023** 1 month, 2 weeks ago

As in the official guide.

upvoted 1 times

🗉 👤 **amorcle** 5 months, 3 weeks ago

Selected Answer: A

As in the official guide.

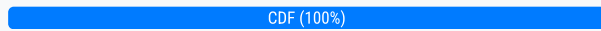
upvoted 1 times


Which three protocols could an NSX administrator use to transfer log messages to a remote log server? (Choose three.)

- A. HTTPS
- B. SSH
- C. TCP
- D. UDP
- E. SSL
- F. TLS

Suggested Answer: CDF

Community vote distribution



 **amorcle** 5 months, 3 weeks ago

Selected Answer: CDF

Correct, as in the official guide

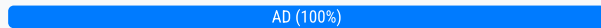
upvoted 1 times


Where does an administrator configure the VLANs used in VRF Lite? (Choose two.)

- A. uplink interface of the VRF gateway
- B. uplink interface of the default Tier-0 gateway
- C. downlink interface of the default Tier-0 gateway
- D. uplink trunk segment
- E. segment connected to the Tier-1 gateway

Suggested Answer: AD

Community vote distribution



 **amorcle** 5 months, 3 weeks ago

Selected Answer: AD

Correct, as in the official guide.

upvoted 1 times

Which two logical router components span across all transport nodes? (Choose two.)

- A. SERVICE_ROUTER_TIER0
- B. TIER0_DISTRIBUTED_ROUTER
- C. DISTRIBUTED_ROUTER_TIER0
- D. DISTRIBUTED_ROUTER_TIER1
- E. SERVICE_ROUTER_TIER1

Suggested Answer: CD

Community vote distribution



CD (100%)

  **_danielgurgel** 2 months, 3 weeks ago

Selected Answer: CD

C and D are correct.



upvoted 1 times

  **electro165** 5 months, 2 weeks ago

Selected Answer: CD

C and D are correct.

upvoted 1 times

  **amorcle** 5 months, 3 weeks ago

Selected Answer: CD

It's in the official book

upvoted 2 times


What must be configured on Transport Nodes for encapsulation and decapsulation of Geneve protocol?

- A. TEP
- B. STT
- C. VXLAN
- D. UDP

Suggested Answer: A

Community vote distribution

A (100%)

 **amorcle** 5 months, 3 weeks ago

Selected Answer: A

As in the official guide 4.X

upvoted 1 times

A customer is preparing to deploy a VMware Kubernetes solution in an NSX environment.


What is the minimum MTU size for the UPLINK profile?

- A. 1700
- B. 1500
- C. 1550
- D. 1650

Suggested Answer: A

Community vote distribution

A (100%)

🗨️  **amorcle** 5 months, 3 weeks ago

Selected Answer: A

The correct answer is A. 1700.

For VMware Tanzu (and related Kubernetes solutions deployed on NSX), the minimum MTU size for the Uplink profile is 1700 bytes. This is due to the overhead introduced by Geneve encapsulation used by NSX. While 1600 might work in some very limited cases, 1700 is the officially supported and recommended minimum to avoid potential issues. Using a smaller MTU can lead to fragmentation and performance problems.

upvoted 1 times

What are three NSX Manager roles? (Choose three.)

- A. master
- B. cloud
- C. policy
- D. zookeeper
- E. manager
- F. controller

Suggested Answer: CEF

Community vote distribution

CEF (100%)

  **_danielgurgel** 2 months, 3 weeks ago



Selected Answer: CEF

C. policy: Handles the configuration and management of network policies, firewall rules, and security settings.

E. manager: The core management component responsible for overall system configuration, monitoring, and APIs. It's the central point of interaction for administrators.

F. controller: Controls the distributed switching and routing functions within the NSX environment. It pushes configurations to the hypervisors.



upvoted 2 times

  **electro165** 5 months, 2 weeks ago

Selected Answer: CEF

C, E, F are correct.

upvoted 3 times

  **amorcle** 5 months, 3 weeks ago

Selected Answer: CEF

C. policy: Handles the configuration and management of network policies, firewall rules, and security settings.

E. manager: The core management component responsible for overall system configuration, monitoring, and APIs. It's the central point of interaction for administrators.

F. controller: Controls the distributed switching and routing functions within the NSX environment. It pushes configurations to the hypervisors.

upvoted 2 times


Which two CLI commands could be used to see if vmnic link status is down? (Choose two.)

- A. esxcfg-nics -l
- B. esxcli network nic list
- C. esxcfg-vmknics -l
- D. esxcfg-vmnic/get.networks
- E. esxcli network vswitch dvs vmware list

Suggested Answer: AB

Community vote distribution

AB (100%)

 **amorcle** 5 months, 3 weeks ago

Selected Answer: AB

As in the official guide

upvoted 1 times


Which VMware NSX Portfolio product can be described as a distributed analysis solution that provides visibility and dynamic security policy enforcement for NSX environments?

- A. NSX Manager
- B. NSX Distributed IDS/IPS
- C. NSX Intelligence
- D. NSX Cloud

Suggested Answer: C

Community vote distribution

C (100%)

 **amorcle** 5 months, 3 weeks ago

Selected Answer: C

The correct answer is C. NSX Intelligence.

NSX Intelligence is the product that provides advanced network traffic analysis, visibility, and dynamic security policy enforcement within NSX environments. 1 It uses distributed analysis to gain insights into application behavior and network flows, enabling automated threat detection and prevention

upvoted 1 times


An administrator has a requirement to have consistent policy configuration and enforcement across NSX instances.
What feature of NSX fulfills this requirement?

- A. Multi-hypervisor support
- B. Federation
- C. Load balancer
- D. Policy-driven configuration

Suggested Answer: B

Community vote distribution

B (100%)

🗨️  **amorcle** 5 months, 3 weeks ago

Selected Answer: B

Correct, as in the official guide 4.X
upvoted 2 times

When collecting support bundles through NSX Manager, which files should be excluded for potentially containing sensitive information?

- A. Core Files
- B. Controller Files
- C. Audit Files
- D. Management Files

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ **kernelkraut** 1 month, 3 weeks ago

Selected Answer: A

Definitely A, watch out for trick questions like this

upvoted 1 times

🗳️ **MSPB** 3 months ago

Selected Answer: A

A is correct, but if C had been "Audit Logs" then C would have been correct too.

- Core files and audit logs might contain sensitive information such as passwords or encryption keys.

<https://techdocs.broadcom.com/us/en/vmware-cis/nsx/vmware-nsx/4-1/administration-guide/operations-and-management/collect-support-bundles.html>

upvoted 1 times

🗳️ **amorcle** 5 months, 3 weeks ago

Selected Answer: A

Correct, as in the official 4.X guide

upvoted 1 times



What can the administrator use to identify overlay segments in an NSX environment if troubleshooting is required?

- A. Geneve ID
- B. VNI ID
- C. Segment ID
- D. VLAN ID

Suggested Answer: *B*

Community vote distribution

B (100%)

  **amorcle** 5 months, 3 weeks ago

Selected Answer: B

Correct, as in the official 4.X guide

upvoted 1 times



How does the Traceflow tool identify issues in a network?

- A. Compares intended network state in the control plane with Tunnel End Point (TEP) keepalives in the data plane.
- B. Compares the management plane configuration states containing control plane traffic and error reporting from transport node agents.
- C. Injects ICMP traffic into the data plane and observes the results in the control plane.
- D. Injects synthetic traffic into the data plane and observes the results in the control plane.

Suggested Answer: D

Community vote distribution

D (100%)

  **amorcle** 5 months, 3 weeks ago

Selected Answer: D

Correct, as in the official 4.X guide

upvoted 1 times



Where is the insertion point for East-West network introspection?

- A. Tier-0 router
- B. Guest VM vNIC
- C. Partner SVM
- D. Host Physical NIC

Suggested Answer: *B*



Community vote distribution

B (100%)

  **aothman** 2 months, 3 weeks ago

Selected Answer: B

Is the correct answer
upvoted 1 times

  **amorcle** 5 months, 3 weeks ago

Selected Answer: B

Correct, as in the official 4.X guide
upvoted 1 times


Which is the only supported mode in NSX Global Manager when using Federation?

- A. Proxy
- B. Policy
- C. Controller
- D. Proton

Suggested Answer: *B*

Community vote distribution

B (100%)

 **amorcle** 5 months, 3 weeks ago

Selected Answer: B

Correct, as in the official 4.X guide
upvoted 1 times



When a stateful service is enabled for the first time on a Tier-0 Gateway, what happens on the NSX Edge node?

- A. DR is instantiated and automatically connected with SR.
- B. SR is instantiated and automatically connected with DR.
- C. SR and DR doesn't need to be connected to provide any stateful services.
- D. SR and DR is instantiated but requires manual connection.

Suggested Answer: *B*

Community vote distribution

B (100%)

  **amorcle** 5 months, 3 weeks ago

Selected Answer: B

Correct, as in the official 4.X guide

upvoted 1 times

An NSX administrator is creating a Tier-1 Gateway configured in Active-Standby High Availability Mode. In the event of node failure, the failover policy should not allow the original failed node to become the Active node upon recovery. Which failover policy meets this requirement?

- A. Enable Preemptive
- B. Non-Preemptive
- C. Preemptive
- D. Disable Preemptive

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ **amorcle** 5 months, 2 weeks ago

Selected Answer: B

Correct.As in the official mware doc.
upvoted 1 times


Which CLI command is used for packet capture on the ESXi Node?

- A. tcpdump
- B. set capture
- C. pktcap-uw
- D. debug

Suggested Answer: C

Community vote distribution

C (100%)

 **amorcle** 5 months, 3 weeks ago

Selected Answer: C

As in the official guide.

upvoted 2 times

Which command on ESXi is used to verify the Local Control Plane connectivity with Central Control Plane?

- A. esxcli network ip connection list | grep netcpa
- B. esxcli network ip connection list | grep ccpd
- C. esxcli network ip connection list | grep 1234
- D. esxcli network ip connection list | grep 1235

Suggested Answer: D

Community vote distribution

D (100%)

🗲️ 👤 **Ssilva521** 3 weeks, 5 days ago

Selected Answer: D

<https://vdan.cz/vmware/nsx/nsx-installation-and-essential-commands-guide/>

upvoted 1 times

🗲️ 👤 **_danielgurgel** 2 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

🗲️ 👤 **amorcle** 5 months, 3 weeks ago

Selected Answer: D

In the new version 4.X.

The communication between CCP and LCP in on the port 1235.

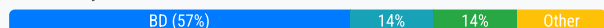
upvoted 3 times

Which two statements describe the characteristics of an Edge Cluster in NSX? (Choose two.)

- A. Must have only active-active edge nodes
- B. Can contain multiple types of edge nodes (VM or bare metal)
- C. Must contain only one type of edge nodes (VM or bare metal)
- D. Can have a maximum of 10 edge nodes
- E. Can have a maximum of 8 edge nodes

Suggested Answer: BD

Community vote distribution



Ssilva521 3 weeks, 6 days ago

Selected Answer: BD

- Supports up to 10 edge nodes, and a maximum of 160 clusters can be configured.
- An edge cluster can be formed with edge nodes of different form factor types.

The NSX Edge node supports the following form factors:

- VM on an ESXi host
 - Bare-metal node
- upvoted 1 times

aothman 2 months, 3 weeks ago

Selected Answer: BD

An NSX Edge cluster can contain a maximum of 10 NSX Edge nodes.

<https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-5-2-and-earlier/4-5/administering/deploying-nsx-edge-clusters-admin/add-edge-nodes-to-an-nsx-edge-cluster-admin.html>

upvoted 1 times

putifarri 3 months, 3 weeks ago

Selected Answer: CE

For standard NSX 4.x deployments (not tied to TKGI), the typical limit is still 8 edge nodes per cluster. NSX Edge Cluster cannot simultaneously contain multiple types of edge nodes (VM or bare metal).

upvoted 1 times

twohandz 4 months, 4 weeks ago

Selected Answer: BD

Support for NSX Edge VM and Bare-Metal to Co-Exist in the Same NSX Edge Cluster: NSX Edge nodes VM and bare-metal can now exist in the same NSX Edge cluster to simplify the scaling of services hosted on the NSX Edge node, such as load balancer.

NSX-T Reference Design Guide 3-0 also has a reference to this:

"NSX-T 2.3 introduced the support for heterogeneous Edge nodes which facilitates easy migration from Edge node VM to bare metal Edge node without reconfiguring the logical routers on bare metal Edge nodes."

upvoted 1 times

electro165 5 months, 2 weeks ago

Selected Answer: BE

Edge Cluster in NSX:

An Edge Cluster in NSX consists of multiple Edge Nodes that provide services such as routing, firewalling, NAT, VPN, and load balancing. Edge Clusters allow for scalability and redundancy by adding multiple edge nodes to the cluster.

Multiple Types of Edge Nodes (VM or Bare Metal):



An Edge Cluster can include both virtual machines (VMs) and bare-metal edge nodes.

This allows for flexibility in deployment and enables organizations to leverage existing infrastructure or scale with virtualized edge nodes.

Maximum of 8 Edge Nodes:

NSX supports up to 8 Edge Nodes per Edge Cluster. This number can vary depending on the version of NSX and the size of the deployment, but 8 is a common maximum.

upvoted 1 times

  **amorcle** 5 months, 3 weeks ago



Selected Answer: CD

I'm sorry, the correct answer to the question C and D

C: NSX Edge cluster: – Contains edge transport nodes (VM or bare-metal form factors) – Provides stateful and gateway services

D: Supports up to 10 edge nodes, and a maximum of 160 clusters can be configured

upvoted 1 times

  **amorcle** 5 months, 3 weeks ago

Selected Answer: BD

Supports up to 10 edge nodes, and a maximum of 160 clusters can be configured

upvoted 1 times

An NSX administrator is using ping to check connectivity between VM1 running on ESXi1 to VM2 running on ESXi2. The ping tests fail. The administrator knows the maximum transmission unit size on the physical switch is 1600. Which command does the administrator use to check the VMware kernel ports for tunnel end point communication?

- A. `vmkping ++netstack=geneve -d -s 1572 <destination IP address>`
- B. `vmkping ++netstack=vxlan -d -s 1572 <destination IP address>`
- C. `esxcli network diag ping -H <destination IP address>`
- D. `esxcli network diag ping -l vmk0 -H <destination IP address>`

Suggested Answer: B

Community vote distribution

B (67%)

A (33%)

🗳️ 👤 **Ssilva521** 3 weeks, 5 days ago

Selected Answer: B

<https://vdan.cz/vmware/nsx/nsx-installation-and-essential-commands-guide/>
upvoted 1 times

🗳️ 👤 **_danielgurgel** 2 months, 3 weeks ago

Selected Answer: B

Tested in NSX 4.2.1
upvoted 1 times

🗳️ 👤 **aothman** 2 months, 3 weeks ago

Selected Answer: B

`++netstack=geneve` is not a valid option.
upvoted 1 times

🗳️ 👤 **MSPB** 3 months ago

Selected Answer: B

`++netstack=geneve` is not a valid option.
upvoted 1 times

🗳️ 👤 **electro165** 5 months, 2 weeks ago

Selected Answer: A

`vmkping` is the command used to test network connectivity for VMware kernel ports (vmk interfaces).
The `++netstack=geneve` option specifies that the Geneve (Generic Network Virtualization Encapsulation) protocol is being used. Geneve is the protocol used in NSX-T for overlay tunneling between ESXi hosts.
`-d` enables the Don't Fragment (DF) bit, which ensures that the packet will not be fragmented. This is important because you're testing with a specific MTU size.
`-s 1572` sets the packet size to 1572 bytes. This accounts for the overhead of the encapsulation and leaves the packet size of 1600 bytes (the maximum allowed by the physical switch), considering the Geneve header.
upvoted 3 times

🗳️ 👤 **amorcle** 5 months, 2 weeks ago

Selected Answer: B

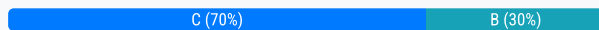
I tried in my personal lab and B works.
upvoted 2 times

An NSX administrator is creating a NAT rule on a Tier-0 Gateway configured in active-standby high availability mode. Which two NAT rule types are supported for this configuration? (Choose two.)

- A. Port NAT
- B. 1:1 NAT
- C. Destination NAT
- D. Reflexive NAT
- E. Source NAT

Suggested Answer: C

Community vote distribution



🗨️ 👤 **Ssilva521** 3 weeks, 6 days ago

Selected Answer: C

C & E.

Supported NAT Rules:

- SNAT / DNAT / NAT64

Gateway Type:

-Tier-0 and Tier-1

NSX Edge HA Mode :

-Active-Standby

upvoted 1 times

🗨️ 👤 **Relbert** 2 months, 1 week ago

Selected Answer: C

There are two choices C and E

upvoted 3 times

🗨️ 👤 **electro165** 5 months, 2 weeks ago

Selected Answer: B

Destination NAT is supported, but Tier-0 Gateways in active-standby HA mode have specific limitations regarding dynamic or stateful destination NAT configurations. Some more complex forms of DNAT may not work as expected in HA mode.

In active-standby HA mode on a Tier-0 Gateway, the supported NAT rule types are:

1:1 NAT

Source NAT (SNAT)

upvoted 3 times

🗨️ 👤 **amorcle** 5 months, 2 weeks ago

Selected Answer: C

There are two choices C and E

upvoted 3 times