EXAMTOPICS

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



CERTIFICATION TEST

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

Question #1 *Topic 1*

An administrator has a vSphere 8.0 environment that is not currently running NSX.

How can the administrator converge this vSphere 8 environment into a VMware Cloud Foundation (VCF) management domain?

A. Manually upgrade the vSphere 8.0 environment to version 9.0 and use the VCF installer to converge the vSphere 9.0 environment into a new VCF instance.

B. Manually upgrade the vSphere 8.0 environment to version 9.0 and manually install NSX 9.x and use the VCF installer to converge the vSphere 9.0 with NSX 9.0 environment into a new VCF instance.

C. Manually upgrade the vSphere 8.0 environment to version 9.0 and use VCF Operations to converge the vSphere 9.0 environment into a new VCF instance.

D. Manually install NSX 9 into the vSphere 8.0 environment and use the VCF installer to converge the vSphere 8.0 with NSX 9.0 environment into a new VCF instance.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

A cloud service provider runs VPCs with differing traffic patterns:

Some VPCs are generating high large North/South flows.

Most of the VPCs generate very little traffic.

The architect needs to optimize Edge dataplane resource consumption while ensuring that noisy VPCs do not impact others.

Which optimization satisfies the requirement?

A. Use multiple Edge clusters and distribute VRF-backed VPCs based on traffic profiles.

B. Convert high-traffic VPCs into VLAN-backed segments attached directly to Tier-0 gateways.

C. Reduce the number of VPCs by consolidating VPCs into shared namespaces.

D. Assign one dedicated Edge node per high-traffic VPC.

**Suggested Answer:** *A*

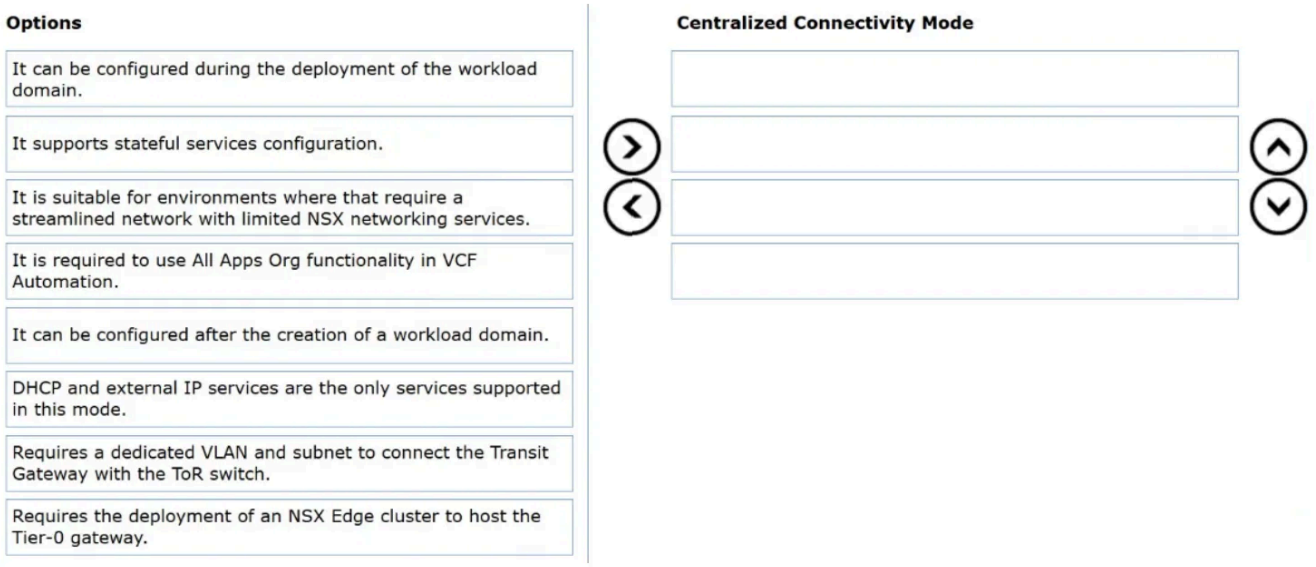
Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

DRAG DROP

An administrator was asked to explain the characteristic and requirements of Centralized Connectivity Mode which is planned to be configured in one of the workload domains in VMware Cloud Foundation (VCF) environment.

Drag and drop four options from the Options list on the left and place them into the Centralized Connectivity Mode on the right in any order.




**Suggested Answer:**
Select: It can be configured during workload-domain deployment; supports stateful services; suits streamlined networking with limited NSX services; requires an NSX Edge cluster to host the Tier-0 gateway.

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

To which component does the hyperbus interface (vmk50) provide network connectivity?

A. containers running on ESX transport nodes

B. virtual machines and containers running across transport nodes

C. virtual machines running on the same hypervisor

D. virtual machines running in the same segment

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

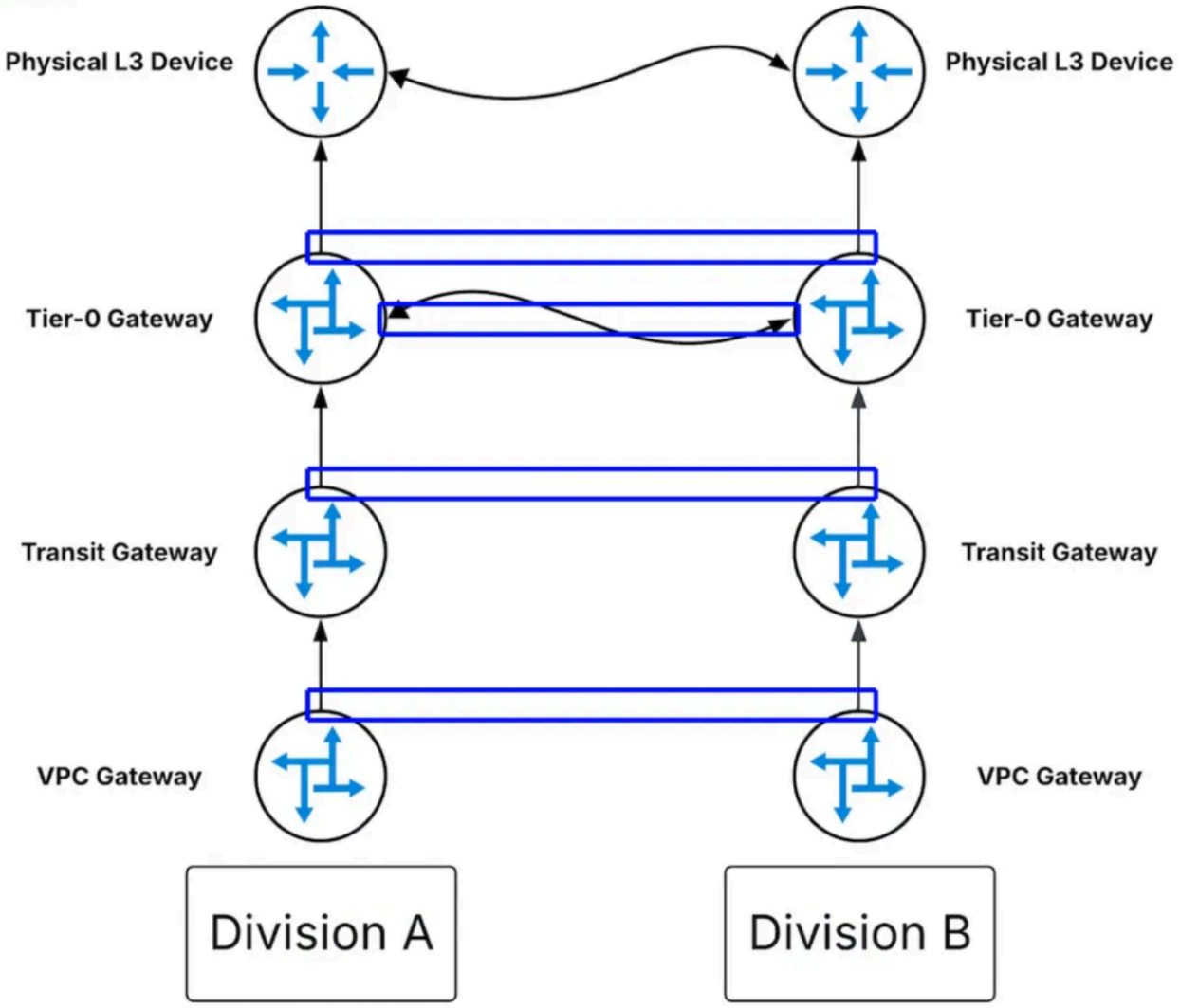
Question #5 *Topic 1*

HOTSPOT

An administrator implements route leaking between the Tier-0 gateways to enhance east/west communication because the physical L3 devices are oversubscribed.

Where should NAT be configured based on the architecture observed in the diagram to allow communication between overlapping IPs?

**Answer Area**




**Suggested Answer:**
Configure NAT on the Tier-0 Gateway where overlapping IP address spaces meet; the diagram does not specify a particular gateway or hotspot location.

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

An administrator is troubleshooting why workloads in NSX cannot reach the external network 10.100.0.0/16.

The Tier-0 Gateway is in Active/Active mode and has the following configuration:

Uplink-1 (VLAN 100): 192.168.100.0/24 → router R1 at 192.168.100.1

Uplink-2 (VLAN 101): 192.168.101.0/24 → router R2 at 192.168.101.1

A static route for 10.100.0.0/16 was added with both next-hops (192.168.100.1 and 192.168.101.1)

The Scope of this route is set to Uplink-1

Symptoms:

Virtual Machines (VMs) cannot reach 10.100.0.0/16

Traceroute from the VM stops at the Tier-0 gateway with "Destination Net Unreachable"

Pings from the Edge nodes to both 192.168.100.1 and 192.168.101.1 are success

What explains why workloads in NSX cannot reach the external network?

A. The physical routers are missing return routes.

B. The next-hops should have been configured as the Tier-0's own uplink IPs instead of the routers IPs.

C. Static routes do not support Equal Cost Multi-Pathing (ECMP) in NSX.

D. The static route Scope is set to only one uplink interface, but the next-hops are on two different VLANs.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

The NSX Manager is reporting the following open alarm:

Remote Logging Not Configured

The administrator has verified that remote logging is enabled for the NSX Manager and NSX Edge nodes. However, the alarm is still open in NSX Manager.

Which statement explains why the Remote Logging Not Configured alarm is still open?

A. The Remote Logging Not Configured alert has been suppressed in the NSX Manager.

B. Operations for Logs has not been enabled in VCF Operations Fleet Management.

C. One or more ESX nodes are not currently configured to forward log messages to a remote logging server.

D. The administrator needs to log out and log back in to the NSX Manager UI to refresh the alert status.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

How should the Global Managers (GMs) and Local Manager (LM)s be distributed to ensure high availability and optimal performance in a multisite NSX Federation deployment comprised of three sites? (Choose two.)

A. The GM should be a single appliance placed in a central cloud environment to simplify connectivity, relying on vSphere HA for availability.

B. The GM cluster should be deployed across three sites.

C. LMs are only needed on the primary site. Secondary sites can manage their local data plane directly via the GM.

D. Each NSX site must have its own LM cluster that reports to the GM.

E. LMs should only be deployed as single nodes to reduce overhead.

**Suggested Answer:** *B, D*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

An architect needs to allow users to deploy multiple copies of a test lab with public access to the internet.

The design requires the same machine IPs be used for each deployment.

What configuration will allow each lab to connect to the public internet?

A. Configure firewall rules to isolate the traffic going to the public internet.

B. Configure DNAT rules on the Tier-1 gateway.

C. Configure SNAT rules on the Tier-0 gateway.

D. Configure isolation on the NSX segment.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

An administrator created a new Tier-1 Gateway and is attempting to change the connected gateway for a deployed segment to use the new gateway.

In the UI, when the administrator clicks the Connected Gateway dropdown, the new Tier-1 gateway is not shown as an available gateway.

What would prevent the new Tier-1 gateway from showing in the list of available gateways?

A. The Tier-1 Gateway is not connected to an NSX Edge Cluster.

B. The Tier-1 Gateway and NSX Segment are connected to different Tier-0 Gateways.

C. The Tier-1 Gateway and NSX Segment are in different transport zones.

D. The Tier-1 Gateway connectivity policy is set to "None".

**Suggested Answer:** *A*

Currently there are no comments in this discussion, be the first to comment!

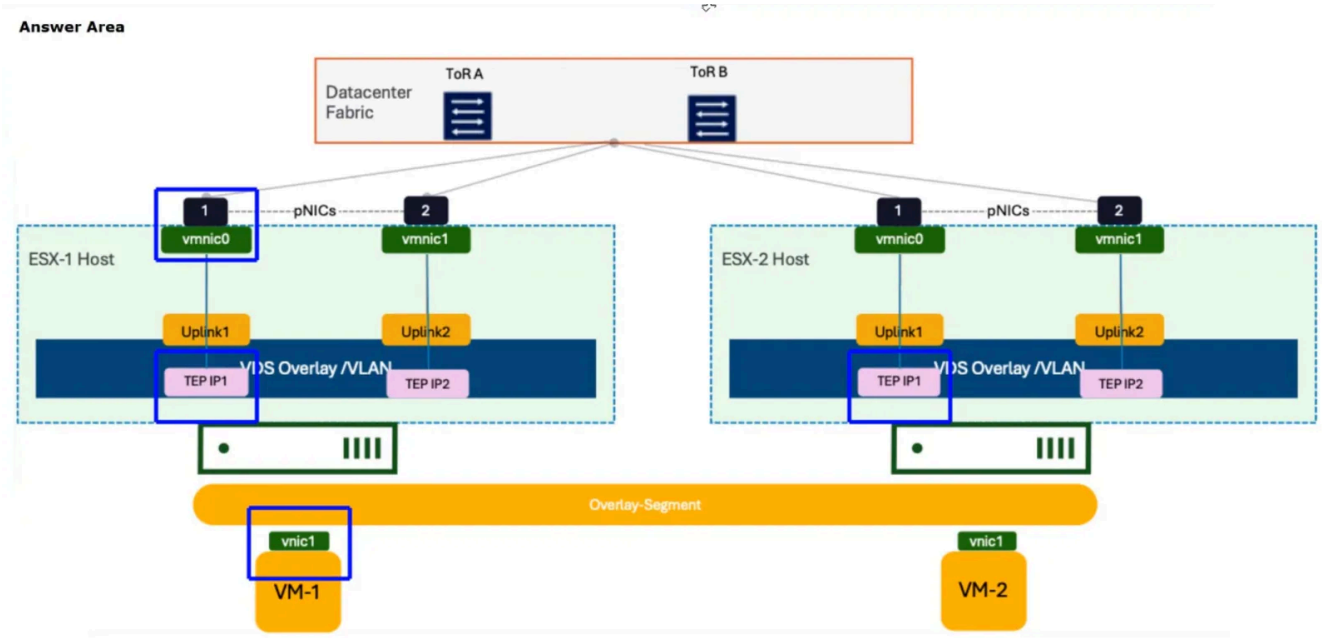
Question #11 *Topic 1*

HOTSPOT

The administrator is working to ascertain the encapsulation of GENEVE by reviewing the capture on Wireshark.

The administrator instructed VM-1 to send a continuous ICMP request directed at VM-2.

Click to highlight where the administrator should observe the GENEVE encapsulated packet.




**Suggested Answer:**
Highlight the VM-1 vNIC/overlay segment traffic and its host TEP encapsulation path.

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

During a design review, the administrator is asked to explain which underlying technology enables the NSX Edge to perform fast packet processing and achieve near line-rate performance for Virtual Network Functions (VNFs).

Which technology is leveraged in the NSX Edge for fast packet processing?

A. Data Plane Development Kit (DPDK)

B. AMD Power Now

C. Intel Speed Step

D. Non-Uniform Memory Access (NUMA)

**Suggested Answer:** *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

When using a DHCP Relay on a segment, which design restriction that must be considered?

A. DHCP settings, DHCP options, and static bindings can be configured on the segment.

B. DHCP Relay service is available to all the other segments in the network.

C. DHCP client requests cannot be relayed to the external DHCP servers.

D. DHCP settings, DHCP options, and static bindings cannot be configured on the segment.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

An administrator is registering secondary site Local Manager (LM) to the Global Manager (GM). The secondary site LM has three NSX Manager Virtual Machine (VMs). The administrator is preparing the connection details to provide during registration.

What must be provided during LM registration to the GM?

A. The external load balancer Virtual IP (VIP) without requiring API certificate updates on individual LM VMs.

B. The IP address of the primary NSX Manager VM in the cluster.

C. The LM Cluster Virtual IP (VIP) or FQDN of the LM Cluster VIP.

D. All three individual LM VM IP addresses in a comma-separated list for redundant connectivity.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

An administrator is enabling IPv6-to-IPv4 communication for workloads hosted in an NSX environment. The workloads use IPv6-only addressing, but the external systems they must reach are IPv4-only. To provide this translation service, the administrator decides to configure NAT64.

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

A. NAT64 is supported on Tier-1 gateways only.

B. NAT64 requires the Tier-1 gateway to be configured in active-active mode.

C. NAT64 is supported on Tier-0 and Tier-1 gateways.

D. NAT64 requires the Tier-1 gateway to be configured in active-standby mode.

E. NAT64 is stateless and requires gateways to be deployed in active-standby mode.

**Suggested Answer:** *C, D*

**BennyRamez88** Most Recent 1 month, 3 weeks ago

Selected Answer: CD

NAT is stateful service.

About NAT64:

- NAT64 is supported on Tier-0 and Tier-1 gateways.

- NAT64 is stateful and requires the Tier-0 gateway to be deployed in active-standby mode.

- NAT64 requires the Tier-1 gateway to be configured with an active-standby edge cluster.

upvoted 1 times

**AbleApe** 2 months ago

Selected Answer: CD

NAT64 supported on both Tier-0 and Tier-1 as long as deployed active-standby since it's a stateful service

upvoted 1 times

**03fastmach1** 2 months, 1 week ago

Selected Answer: BD

NAT64 is supported on a Tier-0 gateway in VMware NSX, provided the gateway is deployed in an active-standby high availability mode

upvoted 1 times

Question #16 *Topic 1*

An administrator is troubleshooting intermittent connectivity failures between two workloads connected to NSX VLAN segments using Traceflow. In-band Network Telemetry (INT) has been enabled in the NSX Global Configuration.

How does Traceflow identify issues in a VLAN network?

A. Injects ICMP traffic into the data plane and observes the results in the control plane.

B. Compares intended network state in the control plane with Tunnel End Point (TEP) keepalives in the data plane.

C. Traceflow cannot be enabled to analyze VLAN network segments in NSX.

D. Injects synthetic traffic into the data plane and observes the results in the control plane.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

An administrator is tasked to import an existing vSphere environment into VMware Cloud Foundation (VCF) as a new workload domain.

While importing the vSphere environment, the administrator must register the new workload domain with an NSX instance associated with an existing workload domain.

What tool should the administrator use to import the vSphere environment into VCF and register with the existing NSX instance?

A. vSphere Client.

B. SDDC Manager.

C. VCF Operations.

D. VCF Installer.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

An administrator is troubleshooting an issue where workloads connected to a Tier-1 Gateway named T1-App can no longer reach external North/South destinations.

The Tier-1 is connected to an Active/Standby Tier-0 Gateway named T0-Prod.

Symptoms observed:

VMs on segments attached to T1-App can ping each other.

VMs on T1-App cannot reach any external IP outside T0-Prod.

From a VM on the segment, ping to the T1-App Distributed Router (DR) IP succeeds.

Ping from the VM to the T1-App Service Router (SR) fails.

The Edge cluster hosting the T1-App SR shows both Edge nodes Up and Healthy.

No failover has occurred - the same Edge node is still shown as Active for T1-App.

What is the most likely cause of this issue?

A. The overlay network between DR and SR has an MTU mismatch.

B. Localized control plane is enabled on the Tier-1 causing the SR to remain admin-down.

C. Route advertisement from T1-App to T0-Prod for 100.64.x.x/31 is disabled.

D. Static default route is missing on the Tier-1 DR component.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Which two statements describe the recommended strategy for configuring and synchronizing security policies across Federated NSX sites? (Choose two.)

A. Security policies should be defined locally on each LM and only synchronized manually by an administrator to prevent accidental conflicts.

B. The Global Manager only synchronizes networking (L2/L3) configurations. Security rules must be configured separately on each site.

C. Consistency is achieved by ensuring all security groups have the exact same name on every Federated site's Local Manager (LM).

D. Security policies, such as Distributed Firewall rules and security groups, must be defined as global policies on the Global Manager (GM).

E. Local Manager (LM)s (LMs) can define local policies, but any global policies defined on the GM always take precedence over the local ones.

**Suggested Answer:** *D, E*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

In an NSX environment, an administrator is observing low throughput and intermittent congestion between the Tier-0 Gateway and the upstream physical routers. The environment was designed for high availability and load balancing, using two Edge Nodes deployed in Active/Active mode.

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

A. Enable ECMP on the Tier-0 gateway.

B. Convert Tier-1 gateways to be edgeless.

C. Add an additional vNIC to the NSX Edge node.

D. Deploy additional Edge nodes.

E. Disable NAT on the Tier-0 gateway.

**Suggested Answer:** *A, D*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

An administrator is onboarding a new research VPC under its R&D project.

Requirements include:

Application teams must be isolated while still consuming shared DNS.

The physical core network exposes BGP only on VLAN 300-dc-edge-uplink-pg that terminates on the Edge cluster.

Any north-south connectivity to the datacenter must traverse Edge.

East-west paths should remain on hosts where possible.

No direct Internet egress is allowed.

Which combination of Transit Gateway (TGW) mode, VPC subnet type and routing configuration meets the requirements?

A. Distributed TGW with Private-VPC subnet, policy-based routing to shared services; static routes for datacenter services on each segment.

B. Distributed TGW, external attachment for the datacenter core and Private-TGW Subnet to shared services; import datacenter routes via BGP on transport nodes and suppress export.

C. Centralized TGW with Private-TGW Subnet to datacenter core and external to shared services; advertise all VPC routes but rely on upstream ACLs to block.

D. Centralized TGW, external attachment on the Edge for datacenter core and Private-TGW Subnet to shared services; import only required datacenter prefixes and disable/filter export of VPC routes.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

The administrator has been tasked with differentiating the roles of Global Manager (GM) and Local Manager (LM) to determine where specific configurations should be performed.

Which statements describe the difference between Global Manager and Local Manager?

A. The Global Manager creates and manages global network objects, while Local Manager enforce them.

B. The Local Manager (LM) creates and manages local network objects, while Global Managers enforce them.

C. Policy creation must always be performed at each Local Manager and synchronized manually with the Global Manager.

D. The Global Manager only provides reporting functions.

**Suggested Answer:** *A*

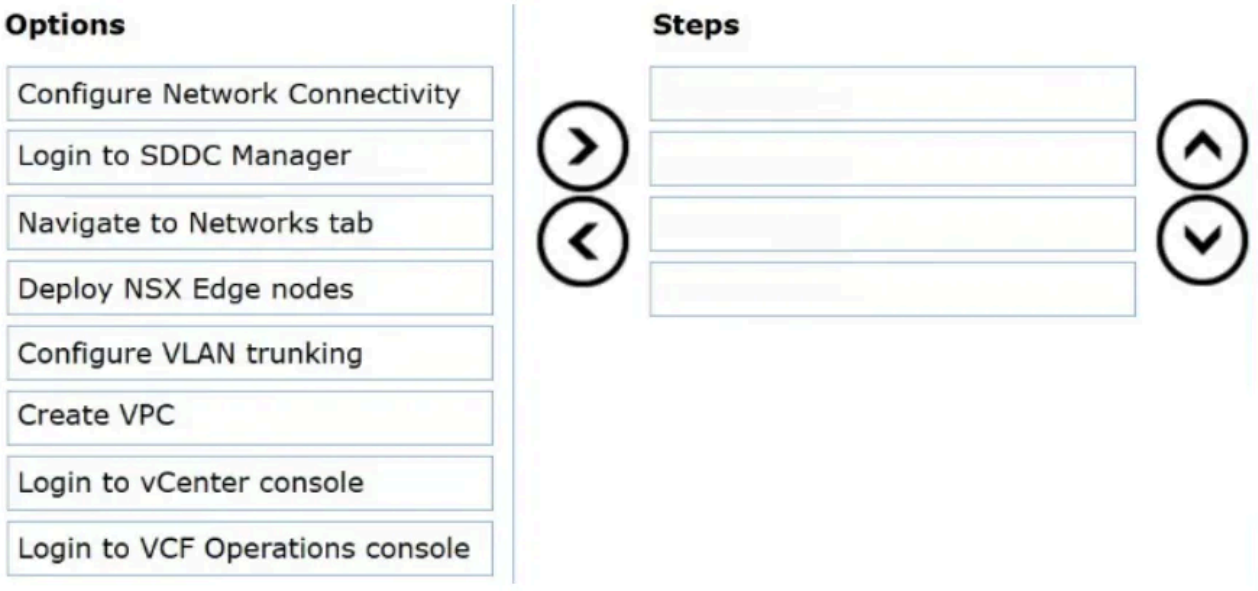
Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

DRAG DROP

An administrator was tasked to configure the Network Connectivity from in VMware Cloud Foundation (VCF) environment for the workload domain that will be used with vSphere Supervisor.

Drag and drop four options from the Options list on the left and place them into the Steps on the right in the correct order.




**Suggested Answer:**
Order: Login to SDDC Manager; navigate to Networks tab; configure Network Connectivity; deploy NSX Edge nodes. The remaining listed actions are not part of these steps.

**8db3afc** Most Recent 1 month, 2 weeks ago

Login to vCenter Console

Navigate to Networks tab

Configure Network Connectivity

Deploy NSX Edge nodes

upvoted 1 times