Download Huawei H12-893_V1.0 Exam Dumps Free

Shared by Solomon on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following operations need to be performed before deployment in Easy mode? (Choose All that Apply)

Options:

A- Disable data synchronization upon going online for the first time.
B- Load the license.
C- Pre-configure the access ports.
D- Configure an SSH fingerprint verification policy.

Answer:

B, C

Explanation:

The Easy mode in Huawei's iMaster NCE-Fabric simplifies VXLAN fabric deployment with automated configuration. Certain pre-deployment steps are required. Let's evaluate each option:

A . Disable data synchronization upon going online for the first time: This is false. Data synchronization is typically enabled by default to ensure consistency; disabling it is not a standard pre-deployment step and is optional based on specific needs. FALSE.

B . Load the license: This is true. A valid license must be loaded into iMaster NCE-Fabric before deployment to unlock features, including Easy mode functionality. TRUE.

C . Pre-configure the access ports: This is true. Access ports on devices (e.g., server leaf nodes) need to be pre-configured (e.g., with VLANs or basic settings) to ensure connectivity before Easy mode automation begins. TRUE.

D . Configure an SSH fingerprint verification policy: This is false. SSH fingerprint verification is part of security configuration but is not a mandatory pre-deployment step for Easy mode; it can be set post-deployment or is automated. FALSE.

Thus, B (Load the license) and C (Pre-configure the access ports) are required operations before deployment in Easy mode.

Question 2

Question Type: MultipleChoice

Which of the following technologies are Layer 4 load balancing technologies? (Select All that Apply)

Options:

A- Nginx
B- PPP
C- LVS
D- HAProxy

Answer:

A, C, D

Explanation:

Layer 4 load balancing operates at the transport layer (OSI Layer 4), using TCP/UDP protocols to distribute traffic based on information like IP addresses and port numbers, without inspecting the application-layer content (Layer 7). Let's evaluate each option:

A . Nginx: Nginx is a versatile web server and reverse proxy that supports both Layer 4 and Layer 7 load balancing. In its Layer 4 mode (e.g., with the stream module), it balances TCP/UDP traffic, making it a Layer 4 load balancing technology. This is widely used in Huawei's CloudFabric DCN solutions for traffic distribution. TRUE.

B . PPP (Point-to-Point Protocol): PPP is a Layer 2 protocol used for establishing direct connections between two nodes, typically in WAN scenarios (e.g., dial-up or VPNs). It does not perform load balancing at Layer 4 or any layer, as it's a point-to-point encapsulation protocol. FALSE.

C . LVS (Linux Virtual Server): LVS is a high-performance, open-source load balancing solution integrated into the Linux kernel. It operates at Layer 4, using techniques like NAT, IP tunneling, or direct routing to distribute TCP/UDP traffic across backend servers. It's a core Layer 4 technology in enterprise DCNs. TRUE.

D . HAProxy: HAProxy is a high-availability load balancer that supports both Layer 4 (TCP mode) and Layer 7 (HTTP mode). In TCP mode, it balances traffic based on Layer 4 attributes, making it a Layer 4 load balancing technology. It's commonly deployed in Huawei DCN environments. TRUE.

Thus, A (Nginx), C (LVS), and D (HAProxy) are Layer 4 load balancing technologies. PPP is not.

Question 3

Question Type: MultipleChoice

An enterprise builds a DC and deploys iMaster NCE-Fabric to automatically deliver network configurations. After the engineer manually deploys the underlay network and delivers overlay network configurations through iMaster NCE-Fabric, it is found that tenant hosts cannot access external networks. Which of the following is not a possible cause of this fault?

Options:

A- No return route is configured on the PE.
B- The engineer did not check whether the service loopback interface needs to be configured on the VXLAN network based on the switch model.
C- No firewall security policy is configured when host traffic passes through the firewall.
D- The MAC address of the NVE interface on the VXLAN network is not manually specified.

Answer:

D

Explanation:

In Huawei's CloudFabric Solution, iMaster NCE-Fabric automates overlay network (e.g., VXLAN) configuration, while the underlay network is manually deployed. Tenant hosts failing to access external networks indicate a connectivity issue, likely at the overlay-underlay boundary or security layer. Let's evaluate each option as a possible cause:

A . No return route is configured on the PE: This is a possible cause. The Provider Edge (PE) device (e.g., border leaf or router) must have a return route to the tenant's VXLAN network for external access. Without it, traffic from external networks cannot reach the DC. POSSIBLE CAUSE.

B . The engineer did not check whether the service loopback interface needs to be configured on the VXLAN network based on the switch model: This is a possible cause. Some Huawei switch models (e.g., CE series) require a service loopback interface as the VTEP source IP. If omitted or misconfigured based on the model, external connectivity fails. POSSIBLE CAUSE.

C . No firewall security policy is configured when host traffic passes through the firewall: This is a possible cause. If a firewall is in the path (e.g., between tenant VPC and external network), a missing security policy (e.g., allowing outbound traffic) blocks access. POSSIBLE CAUSE.

D . The MAC address of the NVE interface on the VXLAN network is not manually specified: This is not a possible cause. The Network Virtualization Edge (NVE) interface in VXLAN does not require

a manually specified MAC address; it uses the switch's system MAC or auto-generates one. iMaster NCE-Fabric typically handles this automatically, and manual specification is neither required nor a common fault point for external access issues. NOT A POSSIBLE CAUSE.

Thus, D is not a possible cause of the fault.

Question 4

Question Type: MultipleChoice

In an M-LAG, two CE series switches send M-LAG synchronization packets through the peer-link to synchronize information with each other in real time. Which option best entries need to be included in the M-LAG synchronization packets to ensure that traffic forwarding is not affected if either device fails? (Select All that Apply)

Options:

A- MAC address entries
B- Routing entries
C- IGMP entries
D- ARP entries

Answer:

A, D

Explanation:

Multi-Chassis Link Aggregation Group (M-LAG) is a high-availability technology on Huawei CloudEngine (CE) series switches, where two switches appear as a single logical device to downstream devices. The peer-link between the M-LAG peers synchronizes critical information to ensure seamless failover if one device fails. Let's evaluate the entries:

A . MAC Address Entries: MAC address tables map device MACs to ports. In M-LAG, synchronizing MAC entries ensures that both switches know the location of connected devices. If one switch fails, the surviving switch can forward Layer 2 traffic without relearning MAC addresses, preventing disruptions. Required.

B . Routing Entries: Routing entries (e.g., OSPF or BGP routes) are maintained at Layer 3 and typically synchronized via routing protocols, not M-LAG peer-link packets. M-LAG operates at Layer 2, and while Layer 3 can be overlaid (e.g., with VXLAN), routing table synchronization is not a standard M-LAG requirement. Not Required.

C . IGMP Entries: IGMP (Internet Group Management Protocol) entries track multicast group memberships. While useful for multicast traffic, they are not critical for basic unicast traffic forwarding in M-LAG failover scenarios. Huawei documentation indicates IGMP synchronization is optional and context-specific, not mandatory for general traffic continuity. Not Required.

D . ARP Entries: ARP (Address Resolution Protocol) entries map IP addresses to MAC addresses, crucial for Layer 2/Layer 3 communication. Synchronizing ARP entries ensures the surviving switch can resolve IP-to-MAC mappings post-failover, avoiding ARP flooding or traffic loss. Required.

Thus, A (MAC address entries) and D (ARP entries) are essential for M-LAG synchronization to maintain traffic forwarding during failover, per Huawei CE switch M-LAG design.

Question 5

Question Type: MultipleChoice

In Huawei CloudFabric Solution, iMaster NCE-Fabric uses SNMP to collect alarms and logs of physical devices and vSwitches.

Options:

A- TRUE
B- FALSE

Answer:

B

Explanation:

In Huawei's CloudFabric Solution, iMaster NCE-Fabric is the SDN controller responsible for managing physical devices and virtual switches (vSwitches). The method of data collection is critical for network monitoring.

SNMP Usage: Simple Network Management Protocol (SNMP) is a traditional method for collecting alarms and logs from network devices. However, Huawei's modern SDN controllers, including iMaster NCE-Fabric, primarily use telemetry (e.g., gRPC, NETCONF) for real-time data collection from physical devices and vSwitches. Telemetry provides higher efficiency and granularity compared to SNMP.

CloudFabric Approach: The solution leverages telemetry-based data collection, as documented in

FabricInsight and iMaster NCE-Fabric guides, to gather alarms, logs, and performance metrics. SNMP may be supported as a legacy option but is not the primary method in this context.

The statement is FALSE (B) because iMaster NCE-Fabric predominantly uses telemetry, not SNMP, for collecting alarms and logs.

Question 6

Question Type: MultipleChoice

Which option best statements is false about the routing design for the underlay network during DCN deployment?

Options:

A- OSPF is recommended for small and midsize DCNs, and EBGP is recommended for large and midsize networks.
B- When OSPF is used on the underlay network, only single-area OSPF can be deployed.
C- Compared with OSPF, EBGP involves fewer calculations and offers better scalability.
D- When EBGP is used on the underlay network, each group of active-active leaf nodes is deployed in an AS.

Answer:

B

Explanation:

The underlay network in Huawei's DCNs (e.g., CloudFabric) uses routing protocols like OSPF or BGP. Let's evaluate each statement:

A . OSPF is recommended for small and midsize DCNs, and EBGP is recommended for large and midsize networks: This is true. OSPF suits smaller networks (<300 switches), while EBGP is better for large networks (>300 switches) due to scalability. TRUE.

B . When OSPF is used on the underlay network, only single-area OSPF can be deployed: This is false. Multi-area OSPF can be deployed to manage larger networks, reducing routing table size and improving stability, a common practice in Huawei DCNs. FALSE.

C . Compared with OSPF, EBGP involves fewer calculations and offers better scalability: This is true. EBGP's path-vector nature requires fewer computational resources than OSPF's link-state calculations and scales better with large topologies. TRUE.

D . When EBGP is used on the underlay network, each group of active-active leaf nodes is deployed in an AS: This is true. In EBGP designs, active-active leaf nodes (e.g., M-LAG) are typically in the same Autonomous System (AS) to simplify routing, using iBGP or route reflectors. TRUE.

Thus, B is the false statement because multi-area OSPF is supported, not just single-area.

Question 7

Question Type: MultipleChoice

Assume that a VXLAN tunnel is monitored on a Huawei CE series switch and that the tunnel status is Down or the tunnel fails to be dynamically established. In this scenario, which of the following statements are true about how to check the cause of the fault? (Select All that Apply)

Options:

A- Run the display vxlan statistics command to check the cause of the fault.
B- Run the display vxlan peer command to check the cause of the fault on the peer device of the tunnel.
C- Run the display vxlan troubleshooting command to check the causes of at most the latest five failures to dynamically establish a VXLAN tunnel.
D- Run the display vxlan troubleshooting command to check at most the latest five reasons why a VXLAN tunnel goes Down.

Answer:

A, B, C, D

Explanation:

On Huawei CloudEngine (CE) series switches, VXLAN tunnel monitoring and troubleshooting involve specific commands to diagnose issues such as tunnel Down status or failed dynamic establishment. Let's evaluate each option:

A . Run the display vxlan statistics command to check the cause of the fault: This command provides statistics on VXLAN tunnel traffic, including packet drops, encapsulation/decapsulation counts, and errors. It helps identify issues like misconfiguration or network congestion, making it a valid troubleshooting tool. TRUE.

B . Run the display vxlan peer command to check the cause of the fault on the peer device of the tunnel: This command displays information about VXLAN peers, including their IP addresses,

VNIs, and reachability status. Checking the peer device's status can reveal connectivity or configuration mismatches, aiding fault diagnosis. TRUE.

C . Run the display vxlan troubleshooting command to check the causes of at most the latest five failures to dynamically establish a VXLAN tunnel: This command logs and displays troubleshooting details, including the latest five failure reasons for dynamic tunnel setup (e.g., BGP EVPN issues or reachability problems). This is a standard feature on Huawei CE switches. TRUE.

D . Run the display vxlan troubleshooting command to check at most the latest five reasons why a VXLAN tunnel goes Down: This command also tracks reasons for tunnel Down events (e.g., underlay failure, peer unreachability), limited to the latest five incidents. This is consistent with Huawei's troubleshooting capabilities. TRUE.

All options A, B, C, and D are true, as they represent valid commands and approaches to troubleshoot VXLAN tunnel issues on Huawei CE switches.

Question 8

Question Type: MultipleChoice

In EVPN Type 3 routes, the MPLS Label field carries a Layer 3 VNI.

Options:

A- TRUE
B- FALSE

Answer:

B

Explanation:

EVPN (Ethernet VPN) is a control plane technology used with VXLAN in Huawei's data center networks to provide Layer 2 and Layer 3 connectivity. EVPN routes are advertised using BGP, with different types serving specific purposes. Type 3 routes (Inclusive Multicast Ethernet Tag routes) are used for multicast or BUM (Broadcast, Unknown Unicast, Multicast) traffic handling in VXLAN networks.

MPLS Label Field: In MPLS (Multiprotocol Label Switching), the label field is used to identify the forwarding equivalence class (FEC) or virtual circuit. In EVPN with VXLAN, MPLS labels can be

used in underlay networks, but VXLAN itself relies on a VNI (VXLAN Network Identifier) in the VXLAN header for overlay segmentation.

Layer 3 VNI: A Layer 3 VNI is associated with inter-subnet routing in EVPN, typically carried in Type 5 routes (IP Prefix routes) for Layer 3 forwarding. Type 3 routes, however, focus on multicast distribution and carry a Layer 2 VNI or multicast group information, not a Layer 3 VNI.

MPLS Label in Type 3 Routes: The MPLS label in Type 3 routes, if used, identifies the VXLAN tunnel or multicast group, not a Layer 3 VNI. The Layer 3 VNI is specific to Type 5 routes for routing between subnets, not Type 3's multicast focus.

Thus, the statement is FALSE (B) because the MPLS Label field in EVPN Type 3 routes does not carry a Layer 3 VNI; it relates to Layer 2 multicast or tunnel identification.

P2P exams