[Full Version 100% Pass Lead2pass 642-997 New Questions Free Version (21-40)

2016 November Cisco Official New Released 642-997 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! As a professional IT exam study material provider, Lead2pass gives you more than just 642-997 exam questions and answers. We provide our customers with the most accurate study material about the 642-997 exam and the guarantee of pass. We assist you to prepare for 642-997 certification which is regarded valuable the IT sector. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/642-997.html QUESTION 21 Which statement about electronic programmable logic device image upgrades is true? A. EPLD and ISSU image upgrades are nondisruptive. B. An EPLD upgrade must be performed during an ISSU system or kickstart upgrade. C. Whether the module being upgraded is online or offline, only the EPLD images that have different current and new versions are upgraded. D. You can execute an upgrade or downgrade only from the active supervisor module.Answer: D Explanation: You can upgrade (or downgrade) EPLDs using CLI commands on the Nexus 7000 Series device. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_0/epld/release/notes/epld_rn.html QUESTION 22 Which statement about SNMP support on Cisco Nexus switches is true? A. Cisco NX-OS only supports SNMP over IPv4. B. Cisco NX-OS supports one instance of the SNMP per VDC. C. SNMP is not VRF-aware. D. SNMP requires the LAN_ENTERPRISE_SERVICES_PKG license. E. Only users belonging to the network operator RBAC role can assign SNMP groups. Answer: B Explanation: Cisco NX-OS supports one instance of the SNMP per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC. SNMP supports multiple MIB module instances and maps them to logical network entities. SNMP is also VRF aware. You can configure SNMP to use a particular VRF to reach the SNMP notification host receiver. You can also configure SNMP to filter notifications to an SNMP host receiver based on the VRF where the notification occurred. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_nx_os_cg/sm_9snmp.html QUESTION 23 Which GLBP load-balancing algorithm ensures that a client is always mapped to the same VMAC address? A. vmac-weighted B. dedicated-vmac-mode C. shortest-path and weighting D. host-dependent Answer: D Explanation: Host dependent--GLBP uses the MAC address of the host to determine which virtual MAC address to direct the host to use. This algorithm guarantees that a host gets the same virtual MAC address if the number of virtual forwarders does not change. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_glbp.html QUESTION 24 What is the grace period in a graceful restart situation? A. how long the supervisor waits for NSF replies B. how often graceful restart messages are sent after a switchover C. how long NSF-aware neighbors should wait after a graceful restart has started before tearing down adjacencies D. how long the NSF-capable switches should wait after detecting that a graceful restart has started, before verifying that adjacencies are still valid Answer: C Explanation: Graceful restart (GR) refers to the capability of the control plane to delay advertising the absence of a peer (going through control-plane switchover) for a "grace period," and thus help minimize disruption during that time (assuming the standby control plane comes up). GR is based on extensions per routing protocol, which are interoperable across vendors. The downside of the grace period is huge when the peer completely fails and never comes up, because that slows down the overall network convergence, which brings us to the final concept: nonstop routing (NSR). NSR is an internal (vendor-specific) mechanism to extend the awareness of routing to the standby routing plane so that in case of failover, the newly active routing plane can take charge of the already established sessions. http://www.ciscopress.com/articles/article.asp?p=1395746&seqNum=2 QUESTION 25 Which two types of traffic are carried over a vPC peer link when no failure scenarios are present? (Choose two.) A. multicast data traffic B. unicast data traffic C. broadcast data traffic D. vPC keep-alive messages Answer: AC Explanation: The vPC peer link is the link used to synchronize states between the vPC peer devices. The vPC peer link carries control traffic between two vPC switches and also multicast, broadcast data traffic. In some link failure scenarios, it also carries unicast traffic. You should have at least two 10 Gigabit Ethernet interfaces for peer links.
http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/configuration_guide_c07-543563.html QUESTION 26 A Cisco Nexus 2000 Series Fabric Extender is connected to two Cisco Nexus 5000 Series switches via a vPC link. After both Cisco Nexus 5000 Series switches lose power, only one switch is able to power back up. At this time, the Cisco Nexus 2000 Series Fabric Extender is not active and the vPC ports are unavailable to the network. Which action will get the Cisco Nexus 2000 Series Fabric Extender active when only one Cisco Nexus 5000 Series switch is up and active? A. Move the line from the failed Cisco Nexus 5000 Series switch to the switch that is powered on, so the port channel forms automatically on the switch that is powered on. B. Shut down the peer link on the Cisco Nexus 5000 Series switch that is powered on. C. Configure reload restore or auto-recovery reload-delay on the Cisco Nexus 5000 Series switch that is powered on. D. Power off and on the Cisco Nexus 2000 Series Fabric Extender so that it can detect only one Cisco Nexus 5000 Series switch at power up. Answer: C Explanation: The

vPC consistency check message is sent by the vPC peer link. The vPC consistency check cannot be performed when the peer link is lost. When the vPC peer link is lost, the operational secondary switch suspends all of its vPC member ports while the vPC member ports remain on the operational primary switch. If the vPC member ports on the primary switch flaps afterwards (for example, when the switch or server that connects to the vPC primary switch is reloaded), the ports remain down due to the vPC consistency check and you cannot add or bring up more vPCs. Beginning with Cisco NX-OS Release 5.0(2)N2(1), the auto-recovery feature brings up the vPC links when one peer is down.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/operations/n5k_vpc_ops.html QUESTION 27 Which policy-map action performs congestion avoidance? A. priority B. bandwidth C. queue-limit D. random-detect Answer: D Explanation: Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Among the more commonly used congestion avoidance mechanisms is Random Early Detection (RED), which is optimum for high-speed transit networks. Cisco IOS QoS includes an implementation of RED that, when configured, controls when the router drops packets. If you do not configure Weighted Random Early Detection (WRED), the router uses the cruder default packet drop mechanism called tail drop.
http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfconav.html QUESTION 28 Refer to the exhibit. Which statement based on these two outputs that were collected 24 hours apart is true?

```
OTV_EDGE1_SITE#1 show otv route
 OTV Unicast MAC Routing Table For Overlay1

VLAN MAC-Address          Metric Uptime  La
   Next-Hop(s)
!100 MACs from SITE 1 - local
110 0000.6e01.010a 1      2d16h          2d
   port-channel1


!100 MACs from SITE 2
110 0000.6e02.020a 42  2d16h          2d16h
   Overlay1-10.3.8.2


OTV_EDGE1_SITE#1 show otv route
 OTV Unicast MAC Routing Table For Overlay1

VLAN MAC-Address          Metric Uptime  La
   Next-Hop(s)
!100 MACs from SITE 1 - local
110 0000.6e01.010a 1      3d16h          3d
   port-channel1
110 0000.6e02.020a 1      0d01h          0d
   port-channel2

!100 MACs from SITE 2
```


A. The Site 2 OTV edge device has gone down. B. The MAC address cannot be discovered on two separate port channel interfaces. C. The MAC address that ends in 020a moved to the local site 23 hours ago. D. The Overlay1 IP address should be a multicast IP address. Answer: C QUESTION 29 Which two reasons explain why a server on VLAN 10 is unable to join a multicast stream that originates on VLAN 20? (Choose two.) A. IGMP snooping and mrouter are not enabled on VLAN 10. B. VLAN 20 has no IGMP snooping querier defined and VLAN 10 has no mrouter. C. The mrouter on VLAN 20 does not see the PIM join. D. The mrouter must be on VLAN 10 and VLAN 20. Answer: AC Explanation: IGMP snooping is a mechanism to constrain multicast traffic to only the ports that have receivers attached. The mechanism adds efficiency because it enables a Layer 2 switch to selectively send out multicast packets on only the ports that need them. Without IGMP snooping, the switch floods the packets on every port. The switch "listens" for the exchange of IGMP messages by the router and the end hosts. In this way, the switch builds an IGMP snooping table that has a list of all the ports that have requested a particular multicast group. The mrouter port is simply the port from the switch point of view that connects to a multicast router. The presence of at least one mrouter port is absolutely essential for the IGMP snooping operation to work across switches. All Catalyst platforms have the ability to dynamically learn about the mrouter port. The switches passively listen to either the Protocol Independent Multicast (PIM) hellos or the IGMP query messages that a multicast router sends out periodically.
http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/68131-cat-multicast-prob.html QUESTION 30 Which two issues explain why a packet is not being routed as desired in a policy-based routing configuration? (Choose two.) A.

The route map is not applied to the egress interface. B. The route map is not applied to the ingress interface. C. The next hop that is configured in the route map is not in the global routing table. D. The next hop that is configured in the route map has a higher metric than the default next hop. Answer: CD Explanation: The next hop that is configured in the route map is not in the global routing table then the packet will not be forwarded as desired. The next hop that is configured in the route map has a higher metric than the default next hop. QUESTION 31 Which three VDC resources can be constrained with a resource template? (Choose three.) A. ACLs B. NAT entries C. IPv4 routes D. IPv6 routes E. SPAN sessions F. RBAC users Answer: CDE Explanation: VDC resource templates set the minimum and maximum limits for shared physical device resources when you create the VDC. The Cisco NX-OS software reserves the minimum limit for the resource to the VDC. Any resources allocated to the VDC beyond the minimum are based on the maximum limit and availability on the device. You can explicitly specify a VDC resource template, or you can use the default VDC template provided by the Cisco NX-OS software. VDC templates set limits on the following resources: IPv4 multicast route memory IPv6 multicast route memory IPv4 unicast route memory IPv6 unicast route memory Port channels Switch Port Analyzer (SPAN) sessions VLANs Virtual routing and forwarding instances (VRFs) http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device-Context-Configuration-Guide/vdc-res-template.html QUESTION 32 Which command sequence correctly enables Adapter FEX on Nexus 5000 Series Switches? A. switch(config)# install feature-set virtualization switch(config)# feature-set virtualization B. switch(config)# install feature-set adapter-fex switch(config)# feature-set adapter-fex C. switch(config)# install feature-set adapter-fex switch(config)# feature-set virtualization D. switch(config)# install feature-set virtualization switch(config)# feature-set adapter-fex Answer: A Explanation: install feature-set virtualization : installs the cisco virtual machine feature set on the switch. feature-set virtualization : enables the cisco virtual machine feature on the switch. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/adapter-fex/513_n1_1/b_Configuring_Cisco_Nexus_5000_Series_Adapter-FEX_rel_5_1_3_N1/b_Configuring_Cisco_Nexus_5000_Series_Adapter-FEX_rel_5_1_3_N1_chapter_010.pdf QUESTION 33 Which three Cisco UCS C-Series CNAs support Adapter FEX? (Choose three.) A. Qlogic QLE8152 B. Broadcom BCM57712 C. Cisco UCS P81E D. Cisco UCS VIC 1220 E. Emulex OCe10102-FX-C F. Intel X520 Answer: BCD Explanation: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c-series_integration/ucsm2-1/b_UCSM2-1_C-Integration/b_UCSM2-1_C-Integration_chapter_011.html#reference_D644111FC68046F0BEA49756A0834664 QUESTION 34 Which two Cisco Nexus platforms support Adapter FEX? (Choose two.) A. Cisco Nexus 7000 Series Switches B. Cisco Nexus 5000 Series Switches C. Cisco Nexus 5500 Series Switches D. Cisco Nexus 4000 Series Switches E. Cisco Nexus 2000 Series Fabric Extenders Answer: CE Explanation: At the access layer, the Adapter-FEX requires a FEX-enabled adapter on a server that connects to a parent device that supports virtualization of interfaces. The Adapter-FEX is supported on the following platforms: ? The Cisco Unified Computing System (UCS) platform supports Adapter-FEX between UCS servers and the UCS Fabric Interconnect. ? The Adapter-FEX is supported on the Cisco Nexus 5500 Series platform and on the Cisco Nexus 2200 Fabric Extender that is connected to a Cisco Nexus 5500 Series parent device. This implementation works on a variety of FEX-capable adapters, including the Cisco UCS P81E virtual interface card (VIC) adapter for the UCS C-Series platform and third party adapters such as the Broadcom BCM57712 Convergence Network Interface Card, that implement the virtual network tag (VNTag) technology. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/operations/adapter_fex/513_n1_1/ops_adapter_fex/ops_using_adapter_fex.html QUESTION 35 Which three items must be configured in the port profile client in Cisco UCS Manager? (Choose three.) A. port profile B. DVS C. data center D. folder E. vCenter IP address F. VM port group Answer: BCD Explanation: After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect. In Cisco UCS Manager, DVSes are organized in the following hierarchy: vCenter Folder (optional) Datacenter Folder (required) DVS At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSes. http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/1-3-1/b_UCSM_GUI_Configuration_Guide_1_3_1/UCSM_GUI_Configuration_Guide_1_3_1_chapter2 8.html QUESTION 36 In the dynamic vNIC creation wizard, why are choices for Protection important? A. They allow reserve vNICs to be allocated out of the spares pool. B. They enable hardware-based failover. C. They select the primary fabric association for dynamic vNICs. D. They allow dynamic vNICs to be reserved for fabric failover. Answer: C Explanation: Number of Dynamic vNICs - This is the number of vNICs that will be available

for dynamic assignment to VMs. Remember that the VIC has a limit to the number of vNICs that it can support and this is based on the number of uplinks between the IOM and the FI. At least this is the case with the 2104 IOM and the M81KR VIC, which supports ((# IOM Links * 15) ?2)). Also remember that your ESXi server will already have a number of vNICs used for other traffic such as Mgmt, vMotion, storage, etc, and that these count against the limit. Adapter Policy - This determines the vNIC adapter config (HW queue config, TCP offload, etc) and you must select VMWarePassThru to support VM-FEX in High Performance mode. Protection - This determines the initial placement of the vNICs, either all of them are placed on fabric A or Fabric B or they are alternated between the two fabrics if you just select the "Protected" option. Failover is always enabled on these vNICs and there is no way to disable the protection.
http://infrastructureadventures.com/2011/10/09/deploying-cisco-ucs-vm-fex-for-vsphere-%E2%80%93-part-2-ucsm-config-and-vmware-integration/ QUESTION 37 How is a dynamic vNIC allocated? A. Dynamic vNICs are assigned to VMs in vCenter. B. Dynamic vNICs can only be bound to the service profile through an updating template. C. Dynamic vNICs are bound directly to a service profile. D. Dynamic vNICs are assigned by binding a port profile to the service profile. Answer: C Explanation: The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs. Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy. For VM-FEX that has all ports on a blade in standard mode, you need to use the VMware adapter policy. For VM-FEX that has at least one port on a blade in high-performance mode, use the VMwarePassThrough adapter policy or create a custom policy. If you need to create a custom policy, the resources provisioned need to equal the resource requirements of the guest OS that needs the most resources and for which you will be using high-performance mode.
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vm_fex/vmware/gui/config_guide/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide_chapter_010.html QUESTION 38 Refer to the command below. When configuring an SVS connection on the Cisco Nexus 5000 Series Switch, which device is being referenced as the remote IP address? nexus5500-2(config-svs-conn)# remote ip address 10.10.1.15 port 80 vrf management A. ESX or ESXi host B. vCenter C. vPC peer switch D. Cisco IMC management Answer: B Explanation: This command specifies the hostname or IP address for the vCenter Server. Optionally, specifies the port number and VRF.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/layer2/6x/b_5500_Layer2_Config_6x/b_5500_Layer2_Config_602N12_chapter_010000.html QUESTION 39 When connecting Cisco Nexus 5000 Series Switches to the VMware vCenter Server, which item must be configured before installing the extension keys? A. configure vPC B. configure DirectPath I/O support in vCenter C. configure PTS on the VSM D. configure dynamic vNICs Answer: A QUESTION 40 Which feature enables NIV? A. EHV B. vPC C. Cisco FabricPath D. Cisco OTV E. VN-Tag Answer: A Explanation: EHV is the feature that enables NIV. Lead2pass.com has been the world leader in providing online training solutions for 642-997 Certification. You use our training materials that have been rigorously tested by international experts. 642-997 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDWnlXTnB1WEMzSjQ 2016 Cisco 642-997 exam dumps (All 137 Q&As) from Lead2pass: http://www.lead2pass.com/642-997.html [100% Exam Pass Guaranteed]