[Full Version 100% Valid Lead2pass Cisco 642-997 New Questions Free Version (1-20)

2016 November Cisco Official New Released 642-997 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! I was recommended by one of my friend, he used the Lead2pass 642-997 dumps and said they are helpful. He was right! I passed my Cisco 642-997 exam yesterday. I was lucky, all my questions in the exams were from Lead2pass dumps. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/642-997.html QUESTION 1 Which statement about Cisco FabricPath is true? A. It is the best solution for interconnecting multiple data centers. B. It optimizes STP throughout the Layer 2 network. C. It is a simplified extension of Layer 3 networks across a single data center. D. The Cisco FabricPath domain appears as a single STP bridge, where each edge port uses the same MAC address.Answer: D Explanation: To have a loop-free topology for the CE/FabricPath hybrid network, the FabricPath network automatically displays as a single bridge to all connected CE devices. The STP domains do not cross into the FabricPath network. If multiple STP domains are defined, BPDUs and topology change notifications (TCNs) are localized to the domain. If a connected STP domain is multihomed to the FabricPath domain, a TCN must be able to reach to all devices in the STP domain through the FabricPath domain. As a result, the TCN is sent to the FabricPath domain through the IS-IS protocol data unit (PDU) by default. http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1/ n5k_ops_fabricpath.html QUESTION 2 Which statement about scalability in Cisco OTV is true? A. The control plane avoids flooding by exchanging MAC reachability. B. IP-based functionality provides Layer 3 extension over any transport. C. Any encapsulation overhead is avoided by using IS-IS. D. Unknown unicasts are handled by the authoritative edge device. Answer: A Explanation: Cisco calls the underlying concept of OTV traffic forwarding "MAC routing", since it behaves as if you are routing Ethernet frames over the DCI transport. OTV uses a control plane protocol to proactively propagate MAC address reachability before traffic is allowed to pass, which eliminates dependency on flooding mechanism to either learn MAC addresses or forward unknown unicasts. http://www.computerworld.com/article/2515468/data-center/layer-2-data-center-interconnect-options.html QUESTION 3 Which two statements about Cisco Nexus 7000 line cards are true? (Choose two.) A. M1, M2, and F1 cards are allowed in the same VDC. B. M line cards are service-oriented and likely face the access layer and provide Layer 2 connectivity. C. F line cards are performance-oriented and likely connect northbound to the core layer for Layer 3 connectivity. D. M line cards support Layer 2, Layer 3, and Layer 4 with large forwarding tables and a rich feature set. E. The F2 line card must reside in the admin VDC. Answer: AD Explanation: Cisco is introducing a new line card called as F3 Module which has rich feature set and offers high performance 40G/100G port density to the Nexus 7000 product family. Cisco also introduced a new feature in NX-OS 6.2(2) where the F2e line card can be in the same VDC as M1 or M2 Line Card. The objective of this session is to cover detailed steps and methodology of migrating Nexus 7000 with VDC types prior to NX-OS 6.2 to the newer F3 or M/F2e VDC types. The session also covers the effect of VDC migration with commonly used Network features, firewall and load balancer services. M-Series XL modules support larger forwarding tables. M-Series modules are frequently required at network core, peering, and aggregation points. When used with the F1-Series, the M-Series modules provide inter-VLAN services and form a pool of Layer 3 resources for the system. https://www.ciscolive2014.com/connect/sessionDetail.ww?SESSION_ID=2244 http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2-6/vmdctechwp.html QUESTION 4 Which statement about the Layer 3 card on the Cisco Nexus 5500 Series Switch is true? A. BGP support is not provided, but RIP, EIGRP, and OSPF support is provided. B. Up to two 4-port cards are supported with up to 160 Gb/s of Layer 3 forwarding capability. C. Up to 16 FEX connections are supported. D. Port channels cannot be configured as Layer 3 interfaces. Answer: C Explanation: From the Cisco NX-OS 5.1(3)N1(1) release and later releases, each Cisco Nexus 5500 Series device can manage and support up to 24 FEXs without Layer 3. With Layer 3, the number of FEXs supported per Cisco Nexus 5500 Series device is 8. With Enhanced vPC and a dual-homed FEX topology each FEX is managed by both Cisco Nexus 5000 Series devices. As a result, one pair of Cisco Nexus 5500 Series devices can support up to 24 FEXs and 16 FEXs for Layer 2 and Layer 3. http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1/ n5k_enhanced_vpc.html QUESTION 5 Which statement explains why a Cisco UCS 6200 Fabric Interconnect that is configured in end- host mode is beneficial to the unified fabric network? A. There is support for multiple (power of 2) uplinks. B. Upstream Layer 2 disjoint networks will remain separated. C. The 6200 can connect directly via vPC to a Layer 3 aggregation device. D. STP is not required on the uplink ports from the 6200. Answer: D Explanation: In Cisco Unified Computing System environments, two Ethernet switching modes determine the way that the fabric interconnects behave as switching devices between the servers and the network. In end-host mode, the fabric interconnects appear to the upstream devices as end hosts with multiple links. In end-host mode, the switch does not run Spanning Tree Protocol and avoids loops by following a set of rules for traffic forwarding. In switch mode, the switch runs Spanning Tree Protocol to avoid loops, and broadcast and multicast packets are handled in the traditional way. http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/whitepaper_c11-701962.html QUESTION 6 Which option is a restriction of the unified ports on the Cisco UCS 6200 Series Fabric Interconnect when connecting to the unified fabric network? A. Direct FC connections are not supported to Cisco MDS switches B. The FCoE or Fibre Channel port allocations must be contiguous on the 6200. C. 10-G Fibre Channel ports only use SFP+ interfaces. D. vPC is not supported on the Ethernet ports. Answer: B Explanation: When you configure the links between the Cisco UCS 2200 Series FEX and a Cisco UCS 6200 series fabric interconnect in fabric port channel mode, the available VIF namespace on the adapter varies depending on where the FEX uplinks are connected to the fabric interconnect ports. Inside the 6248 fabric interconnect there are six sets of eight contiguous ports, with each set of ports managed by a single chip. When uplinks are connected such that all of the uplinks from an Cisco 642-997 Exam FEX are connected to a set of ports managed by a single chip, Cisco UCS Manager maximizes the number of VIFs used in service profiles deployed on the blades in the chassis. If uplink connections from an IOM are distributed across ports managed by separate chips, the VIF count is decreased. http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/6200-install-guide/6200_HIG/6200_HIG_chapter_01.html QUESTION 7 Which statement about the implementation of Cisco TrustSec on Cisco Nexus 7000 Series Switches is true? A. While SGACL enforcement and SGT propagation are supported on the M and F modules, 802.1AE (MACsec) support is available only on the M module. B. SGT Exchange Protocol is required to propagate the SGTs across F modules that lack hardware support for Cisco TrustSec. C. AAA authentication and authorization is supported using TACACS or RADIUS to a Cisco Secure Access Control Server. D. Both Cisco TrustSec and 802.1X can be configured on an F or M module interface. Answer: A Explanation: The M-Series modules on the Nexus 7000 support 802.1AE MACSEC on all ports, including the new M2-series modules. The F2e modules will have this feature enabled in the future. It is important to note that because 802.1AE MACSEC is a link-level encryption, the two MACSEC-enabled endpoints, Nexus 7000 devices in our case, must be directly L2 adjacent. This means we direct fiber connection or one facilitated with optical gear is required. MACSEC has integrity checks for the frames and intermediate devices, like another switch, even at L2, will cause the integrity checks to fail. In most cases, this means metro-Ethernet services or carrier-provided label switched services will not work for a MACSEC connection. http://www.ciscopress.com/articles/article.asp?p=2065720 QUESTION 8 Which statement about implementation of Cisco TrustSec on Cisco Nexus 5546 or 5548 switches are true? A. Cisco TrustSec support varies depending on Cisco Nexus 5500 Series Switch model. B. The hardware is not able to support MACsec switch-port-level encryption based on IEEE 802.1AE. C. The maximum number of RBACL TCAM user configurable entries is 128k. D. The SGT Exchange Protocol must use the management (mgmt 0) interface. Answer: B Explanation: https://scadahacker.com/library/Documents/Manuals/Cisco%20-%20TrustSec%20Solution%20Overview.pdf QUESTION 9 Which two security features are only supported on the Cisco Nexus 7000 Series Switches? (Choose two.) A. IP source guard B. traffic storm control C. CoPP D. DHCP snooping E. Dynamic ARP Inspection F. NAC Answer: BF Explanation: A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces. Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 10-millisecond interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/dcnm/security/configuration/guide/b_Cisco_DCNM_Security_Configuration_Guide__Release_5-x/Cisco_DCNM_Security_Configuration_Guide__Release_5-x_chapter17.html http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/dcnm/security/configuration/guide/b_Cisco_DCNM_Security_Configuration_Guide__Release_5-x/Cisco_DCNM_Security_Configuration_Guide__Release_5-x_chapter1.html QUESTION 10 After enabling strong, reversible 128-bit Advanced Encryption Standard password type-6 encryption on a Cisco Nexus 7000, which command would convert existing plain or weakly encrypted passwords to type-6 encrypted passwords? A. switch# key config-key ascii B. switch(config)# feature password encryption aes C. switch# encryption re-encrypt obfuscated D. switch# encryption decrypt type6 Answer: C Explanation: This command converts existing plain or weakly encrypted passwords to type-6 encrypted passwords. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5-x/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5-x_chapt

er_010101.html QUESTION 11 By default it will take 10 seconds for authentication to fail due to an unresponsive RADIUS server before a Cisco Nexus series switch reverts to another RADIUS server or local authentication. What is one efficient way to improve the reaction time to a RADIUS server failure? A. Decrease the global RADIUS retransmission count to 1. B. Decrease the global RADIUS timeout interval to 5 seconds. C. Configure the RADIUS retransmission count and timeout interval per server, versus globally. D. Configure per server a test idle timer, along with a username and password. Answer: D Explanation: You can monitor the availability of RADIUS servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval during which a RADIUS server receives no requests before the Nexus 5000 Series switch sends out a test packet. You can configure this option to test servers periodically. The test idle timer specifies the interval during which a RADIUS server receives no requests before the Nexus 5000 Series switch sends out a test packet. The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the Nexus 5000 Series switch does not perform periodic RADIUS server monitoring.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/CLIConfigurationGuide/sec_radius.html QUESTION 12 Which statement about RADIUS configuration distribution using Cisco Fabric Services on a Cisco Nexus 7000 Series Switch is true? A. Cisco Fabric Services does not distribute the RADIUS server group configuration or server and global keys. B. Enabling Cisco Fabric Services causes the existing RADIUS configuration on your Cisco NX- OS device to be immediately distributed. C. When the RADIUS configuration is being simultaneously changed on more than one device in a Cisco Fabric Services region, the most recent changes will take precedence. D. Only the Cisco NX-OS device with the lowest IP address in the Cisco Fabric Services region can lock the RADIUS configuration. Answer: A Explanation: CFS does not distribute the RADIUS server group configuration or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_6-x/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_6-x_chapter_0101.html QUESTION 13 When a local RBAC user account has the same name as a remote user account on an AAA server, what happens when a user with that name logs into a Cisco Nexus switch? A. The user roles from the remote AAA user account are applied, not the configured local user roles. B. All the roles are merged (logical OR). C. The user roles from the local user account are applied, not the remote AAA user roles. D. Only the roles that are defined on both accounts are merged (logical AND). Answer: C Explanation: If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_rbac.html QUESTION 14 Which statement is true if password-strength checking is enabled? A. Short, easy-to-decipher passwords will be rejected. B. The strength of existing passwords will be checked. C. Special characters, such as the dollar sign ($) or the percent sign (%), will not be allowed. D. Passwords become case-sensitive. Answer: A Explanation: If a password is trivial (such as a short, easy-to-decipher password), the cisco NX_OS software will reject your password configuration if password-strength checking is enabled. Be sure to configure a strong password. Passwords are case sensitive.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x_chapter_01000.pdf QUESTION 15 Which statement about RBAC user roles on a Cisco Nexus switch is true? A. If you belong to multiple roles, you can execute only the commands that are permitted by both roles (logical AND). B. Access to a command takes priority over being denied access to a command. C. The predefined roles can only be changed by the network administrator (superuser). D. The default SAN administrator role restricts configuration to Fibre Channel interfaces. E. On a Cisco Nexus 7000 Series Switch, roles are shared between VDCs. Answer: B Explanation: If you belong to multiple roles, you can execute a combination of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose a user has RoleA, which denied access to the configuration commands. However, the users also have RoleB, which has access to the configuration commands. In this case, the users have access to the configuration commands.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/C
LIConfigurationGuide/sec_rbac.html QUESTION 16 Which two statements about SAN zoning on Cisco Nexus switches are true? (Choose two.) A. Unlike configured zones, default zone information is not distributed to the other switches in the fabric. B. Traffic can either be permitted or denied among members of the default zone. This information is not distributed to all switches. It must be configured in each switch. C. The settings for default zone configurations cannot be changed. D. To activate a zone set,

you must copy the running configuration to the startup configuration after the zone set is configured. E. Soft zoning restrictions will not prevent a source device from accessing a device outside its zone, if the source knows the Fibre Channel ID of the destination. F. Hard zoning is enforced by the hardware on each FLOGI sent by an N Port. Answer: BE Explanation: Each member of a fabric (in effect a device attached to an Nx port) can belong to any zone. If a member is not part of any active zone, it is considered to be part of the default zone. Therefore, if no zone set is active in the fabric, all devices are considered to be in the default zone. Even though a member can belong to multiple zones, a member that is part of the default zone cannot be part of any other zone. The switch determines whether a port is a member of the default zone when the attached port comes up. Unlike configured zones, default zone information is not distributed to the other switches in the fabric Traffic can either be permitted or denied among members of the default zone. This information is not distributed to all switches; it must be configured in each switch. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5_2/configuration/guides/f abric/DCNM-SAN/fm_fabric/zone.html QUESTION 17 Which two statements about SAN zoning on Cisco Nexus switches are true? (Choose two.) A. Zoning is enforced by examining the destination ID field. B. Devices can only belong to one zone. C. Only one zone set can be activated at any time. D. A zone can only be a member one zone set. E. Zoning must be administered from the primary SAN switch in the fabric. F. Zone configuration changes are nondisruptive. Answer: CF Explanation: A zone set can be activated or deactivated as a single entity across all switches in the fabric. Only one zone set can be activated at any time. If zoning is not activated, all devices are members of the default zone. If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone. Zoning can be administered from any switch in the fabric. When you activate a zone (from any switch), all switches in the fabric receive the active zone set. Additionally, full zone sets are distributed to all switches in the fabric, if this feature is enabled in the source switch. http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/san-os/quick/guide/qcg_zones.html QUESTION 18 The Connectivity Management Processor monitors the active supervisor module on a Cisco Nexus 7000 switch and will reboot the device in the event of a lights-out management issue. However, which option includes features that provide similar benefits in the absence of the Connectivity Management Processor? A. high-availability functionality from features such as vPC and NSF B. traditional system connectivity models like SNMP, GUI, or SSH C. Cisco FabricPath D. VDC failover Answer: A Explanation: vPC uses the vPC peer-keepalive link to run hello messages that are used to detect a dual-active scenario. A Gigabit Ethernet port can be used to carry the peer-keepalive messages. A dedicated VRF is recommended to isolate these control messages from common data packets. When an out-of-band network infrastructure is present, the management interfaces of the Cisco Nexus 7000 supervisor could be also used to carry keep-alive connectivity using the dedicated management VRF. When the vPC peer-link is no longer detected, a dual-active situation occurs, and the system disables all vPC port channel member on the "secondary" vPC peer (lower vPC role priority value). Also SVI interfaces associated to a vPC VLAN are suspended on the secondary switch. As a result, in this condition only the "primary" vPC peer actively forwards traffic on the vPC VLANs. Multiple peer-keepalive links can be used to increase resiliency of the dual-active detection mechanism. Both the Cisco Catalyst 6500 and the Cisco Nexus 7000 offer a variety of high-availability features. Some of the primary features to highlight are In Service Software Upgrade (ISSU), Stateful Switchover (SSO), and Nonstop Forwarding (NSF). The operation and the behavior of these features are unique to the respective platform and can be independently executed without affecting the interoperability between the two platforms. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_589890.html QUESTION 19 Which Cisco Nexus feature is best managed with DCNM-SAN? A. VSS B. domain parameters C. virtual switches D. AAA Answer: B Explanation: The Fibre Channel domain (fcdomain) feature performs principal switch selection, domain ID distribution, FC ID allocation, and fabric reconfiguration functions as described in the FC-SW-2 standards. The domains are configured on a per VSAN basis. If you do not configure a domain ID, the local switch uses a random ID. This section describes each fcdomain phase: Principal switch selection - This phase guarantees the selection of a unique principal switch across the fabric. Domain ID distribution - This phase guarantees each switch in the fabric obtains a unique domain ID. FC ID allocation - This phase guarantees a unique FC ID assignment to each device attached to the corresponding switch in the fabric. Fabric reconfiguration - This phase guarantees a resynchronization of all switches in the fabric to ensure they simultaneously restart a new principal switch selection phase. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5_2/configuration/guides/sysmgnt/DCNM-SAN/sysmgmt_dcnm/sysmgmt_overview.html#wp1051962 QUESTION 20 Which of the following Cisco Nexus features is best managed with DCNM-LAN? A. VSS B. Domain parameters C. Virtual switches D. AAA Answer: C I think Lead2pass dumps are very good for the people who do not have much time for their Cisco 642-997 exam preparation. You can easily pass the exam only by memorize Lead2pass exam questions. Believe or not, I did so and I passed my 642-997 exam. 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]