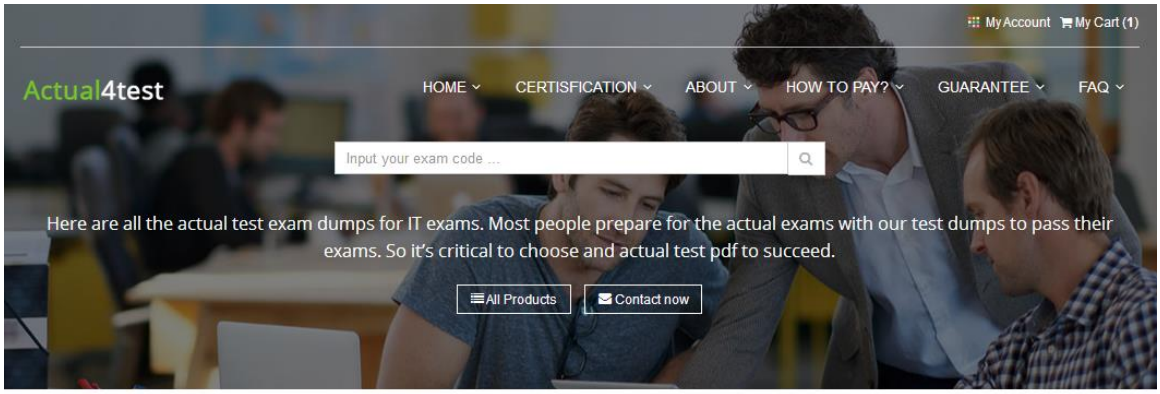
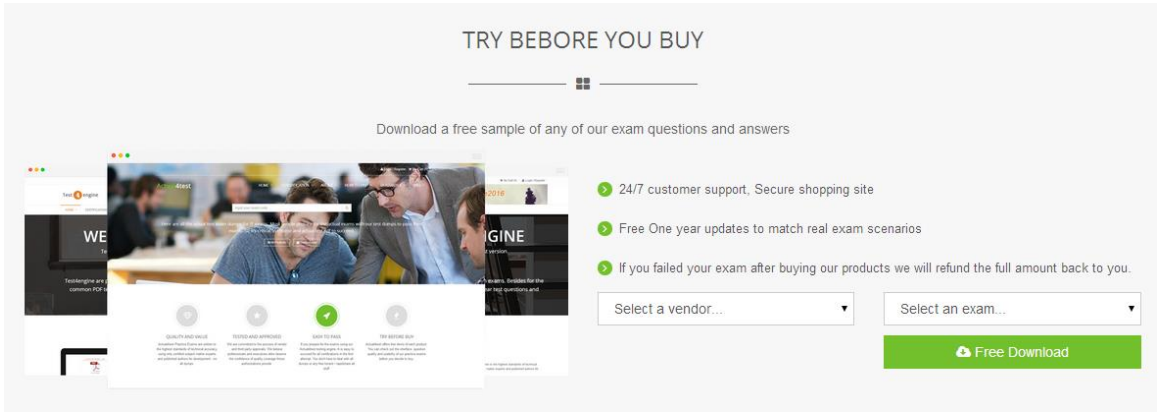
Actual4Test





http://www.actual4test.com

Actual4test - actual test exam dumps-pass for IT exams

Exam : **300-165**

Title : Implementing Cisco Data Center Infrastructure

Vendor : Cisco

Version : DEMO

NO.1 If vPC peer keepalives are used between vPC peers, which VRF is used by default?
A. management
B. default
C. The user must dedicate a VRF for keepalives.
D. system
Answer: A

NO.2 You have a Cisco Nexus 7700 Series switch on which the graceful which the graceful restart feature is disable, you are configuring BGP, which command should you run to enable the graceful restart feature?
A. Switch(config-router)# graceful-restart restart-time
B. Switch(config-router)** graceful-restart grace-period
C. Switch(config-router)ff graceful-restart-helper
D. Switch(config-router)> graceful-restart
Answer: B

NO.3 Refer to the exhibit.

```
N5K1(config)# svs connection 2VC
N5K1 (config-svs-conn)# protocol vmware-vim
N5K1 (config-svs-conn)# dvs-name  Pod1PTS port 80 vrf
management
N5K1 (config-svs-conn)# install certificate default
N5K1 (config-svs-conn)#  extension-key:
Cisco_Nexus_1000V_1543569268
```

Which two commands are missing from this configuration that an admin needs to integrate a Cisco Nexus 5000 switch with vCenter to leverage VM-FEX? (Choose two.)
A. vmware dvs datacenter-name <VMWare Datacenter name>
B. vmware dvs <DVS name>
C. remote ip address <vCenter IP> port 80 vrf <vrf>
D. connection-type vmware
E. installation-method auto
Answer: A,C

NO.4 Which command should you run to enforce SNMP message encryption for all SNMPv3 communications?
A. snmp-server globalEnforceAuth
B. snmp-server user Admin enforcePriv
C. snmp-server globalEnforcePriv
D. snmp-server user Admin enforceAuth
Answer: C

NO.5 What must be enabled on the interface of a multicast-enabled device to support the Source Specific Multicast feature?

A. IGMP version 3

B. IGMP version 2

C. IGMP version 1

D. PIM

Answer: A

Explanation:

IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. Version 3 of this protocol supports source filtering, which is required for SSM. To run SSM with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself.

IGMP v3lite and URD are two Cisco-developed transition solutions that enable the immediate development and deployment of SSM services, without the need to wait for the availability of full IGMPv3 support in host operating systems and SSM receiver applications. IGMP v3lite is a solution for application developers that allows immediate development of SSM receiver applications switching to IGMPv3 as soon as it becomes available. URD is a solution for content providers and content aggregators that enables them to deploy receiver applications that are not yet SSM enabled (through support for

IGMPv3). IGMPv3, IGMP v3lite, and URD interoperate with each other, so that both IGMP v3lite and URD can easily be used as transitional solutions toward full IGMPv3 support in hosts.

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfssm.html

NO.6 Which option shows how to configure an ERSPAN Type III source session in Cisco NX-OS 6.2?

A)

```
switch(config)# capture monitor erspan origin ip-address 10.10.10.10
global
switch(config)# capture monitor erspan granularity 100_ns
switch(config)# capture monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 2
switch(config-erspan-src)# source interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 192.168.0.1
switch(config-erspan-src)# no shut
```

B)

```
switch(config)# monitor erspan origin ip-address 10.10.10.10 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# destination interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 192.168.0.1
switch(config-erspan-src)# no shut
```

C)

```
switch(config)# monitor erspan origin ip-address 10.10.10.10 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# source interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 192.168.0.1
switch(config-erspan-src)# no shut
```

D)

```
switch(config)# capture monitor erspan origin ip-address 10.10.10.10
global
switch(config)# capture monitor erspan granularity 100_ns
switch(config)# capture monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 2
switch(config-erspan-src)# destination interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 192.168.0.1
switch(config-erspan-src)# no shut
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

NO.7 Between which two types of ports does FIP establish Fibre Channel virtual links? (Choose two.)

A. VE Ports and VE Ports

B. N Ports and F Ports

C. VN Ports and VF Ports

D. VP Ports and VE Ports

E. VE Ports and VF Ports

F. E Ports and E Ports

Answer: A,C

Explanation:

FIP aims to establish virtual FC links between VN_Ports and VF_Ports (ENode to FCF), as well as between pairs of VE_Ports (FCF to FCF), since these are the only legal combinations supported by native Fibre Channel fabrics. Standards-compliant implementations are not required to support both forms of virtual FC links, and Cisco has decided to focus initially on implementing FIP only between ENodes and FCFs. FCF-to-

FCF connectivity is considered a strategic direction for end-to-end FCoE deployments, but the short-term urgency is for FCoE adoption between CNAs and the Fibre Channel fabric perimeter, where unified fabric can offer the greatest capital expenditure (CapEx) savings today.

Reference: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white_paper_c11-560403.html

NO.8 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: B,C,D

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.

Reference:

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_chapter28.html

NO.9 When configure HSPR on IPv6 enabled interface, which two configuration is correct.

A. switchA{config-if)> standbyt 6 preempt

B. switchA(config-if)> hsrp <group-number>

C. switchA(config-if)ff key 6

D. switchA{config-if)> hsrp version 2

E. switchA{config-if)B priority <level>

Answer: B

NO.10 Which three options are CallHome predefined destination profiles that are supported on Cisco NX-OS? (Choose three.)

A. CiscoTAC-1

B. full-text-destination

C. pager-xml-destination

D. short-text-destination

E. xml-text-destination

F. pager-json-destination
Answer: A,B,D

NO.11 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.
Reference: 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

NO.12 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 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.
Reference: http://www.ciscopress.com/articles/article.asp?p=1395746&seqNum=2

NO.13 You have two Fibre Channel switches that are connected via EISL. You discover that the fabrics are isolated. What are two possible causes of the fabric isolation? (Choose two.)
A. mismatched SAN port channel group modes

B. mismatched VSANs on either switch
C. mismatched active zone set databases
D. mismatched line card types
E. mismatched switch series
Answer: B,C

NO.14 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. This feature performs two operations:
*
If both switches reload, and only one switch boots up, auto-recovery allows that switch to assume the role of the primary switch. The vPC links come up after a configurable period of time if the vPC peer-link and the peer-keepalive fail to become operational within that time.
If the peer-link comes up but the peer-keepalive does not come up, both peer switches keep the vPC links down. This feature is similar to the reload restore feature in Cisco NX-OS Release 5.0(2)N1(1) and earlier releases. The reload delay period can range from 240 to 3600 seconds.
*
When you disable vPCs on a secondary vPC switch because of a peer-link failure and then the primary vPC switch fails, the secondary switch reenables the vPCs. In this scenario, the vPC waits for three consecutive keepalive failures before recovering the vPC links.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/operations/n5k_vpc_ops.html

NO.15 Using the default VDC high-availability options in the Cisco Nexus 7010 switch, which event occurs after a VDC failure?
A. VDC restart occurs.
B. The VDC is deleted.
C. VDC bringdown occurs, and the VDC must be restarted manually.
D. VDC shutdown occurs, and the VDC must be restarted manually.
Answer: D

NO.16 What mode is required on a Cisco Nexus 7000 32-port 10-GB module port group to allow equal access to the 10-GB port controller?
A. dedicated
B. assigned
C. shared
D. community
Answer: C
Explanation:
You can share 10 Gb of bandwidth among a group of ports (four ports) on a 32-port 10-Gigabit Ethernet module. To share the bandwidth, you must bring the dedicated port administratively down, specify the ports that are to share the bandwidth, change the rate mode to shared, and then bring the ports administratively up.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/interfaces/configuration/guide/if_cli/if_basic.html#70242

NO.17 Which PIM configuration is supported in Cisco NX-OS?
A. Switch(config-if)tt ip pirn ssm default
B. switch(config-if)# ip pim sparse-mode
C. Switch(config-if)tf ip pim spase-mode
D. Switch(config-if)tf ip pim sparse-dense-mode
Answer: B

NO.18 Which two items are required components of VN-Link in software? (Choose two.)
A. VDC
B. VEM
C. vPC
D. VSM
E. VRRP
Answer: B,D
Explanation:
The Cisco Nexus 1000V Series consists of two main types of components that can virtually emulate a 66-slot modular Ethernet switch with redundant supervisor functions:
* Virtual Ethernet module (VEM)-data plane: This lightweight software component runs inside the hypervisor. It enables advanced networking and security features, performs switching between directly attached virtual machines, provides uplink capabilities to the rest of the network, and effectively replaces the vSwitch. Each hypervisor is embedded with one VEM.

* Virtual supervisor module (VSM)-control plane: This standalone, external, physical or virtual appliance is responsible for the configuration, management, monitoring, and diagnostics of the overall Cisco Nexus 1000V Series system (that is, the combination of the VSM itself and all the VEMs it controls) as well as the integration with VMware vCenter. A single VSM can manage up to 64 VEMs. VSMs can be deployed in an active-standby model, helping ensure high availability.
Reference: http://www.cisco.com/c/en/us/solutions/collateral/switches/nexus-1000v-switch-vmware-vsphere/white_paper_c11-525307.html

NO.19 When you configure LISP, which two components must be configured at the site edge? (Choose two.)
A. AED
B. ELAN
C. ITR
D. EOBC
E. ETR
Answer: C,E

NO.20 Which two RFCs are supported by Cisco NX-OS devices for OSPFv2? (Choose two.)
A. RFC 2238
B. RFC 1918
C. RFC 1583
D. RFC 2453
E. RFC 2740
Answer: A,C

NO.21 Which situation must you consider when you add a remote RADIUS server to a Cisco Nexus device?
A. If RADIUS authentication fails, the device falls back to local authentication automatically.
B. If RADIUS authentication fails, the user is denied access with no further authentication checks.
C. If the RADIUS server is unreachable, users are unable to log in.
D. If the RADIUS server is unreachable, all users are given access with the default role.
Answer: B

NO.22 Which Cisco MDS feature needs to be enabled for Cisco TrustSec FC Link Encryption to work?
A. feature Trust-Sec
B. feature ESP
C. feature FC-TSLE
D. feature FC-SP
Answer: D

NO.23 Which protocol is used to exchange MAC address reachability between OTV-enabled switches?
A. EIGRP

B. IS-IS
C. iBGP
D. RIPv2
Answer: B

NO.24 Refer to the exhibit.

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

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


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


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

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

!100 MACs from SITE 2
```

Which statement based on these two outputs that were collected 24 hours apart is true?
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

NO.25 Which implicit rules are applied to all IPv6 ACLs?
A. deny icmp any any nd-nadeny icmp any any nd-nspermit icmp any any router-advertisementpermit icmp any any router-solicitationdeny ipv6 any any
B. deny icmp any any router-advertisement logdeny icmp any a ny router-solicitation logdeny ipv6 any any log
C. deny icmp any any nd-na logdeny icmp any any nd-ns logdeny ipv6 any any log
D. permit icmp any any nd-napermit icmp any any nd-nspermit icmp any any router-

advertisementpermit icmp any any router- solicitationdeny ipv6 any any
Answer: D

NO.26 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: A,C
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.
Reference: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/configuration_guide_c07-543563.html