Free Questions for HPE7-A01 by certsdeals

Shared by Wheeler on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

your customer has asked you to assign a switch management role for a new user The customer requires the user role to View switch configuration information and have access to the PUT and POST meth0ds for REST API.

Which default AOS-CX user role meets these requirements?

Options:

A- administrators

B- auditors

C- sysops

D- helpdesk

Answer:

C

Explanation:

The correct answer is C. sysops.

The sysops user role is a predefined role that allows users to view switch configuration information and have access to the PUT and POST methods for REST API. The sysops user role can also use the PATCH and DELETE methods for REST API, but not for all resources. The sysops user role is suitable for users who need to perform system operations on the switch, such as backup, restore, upgrade, or reboot.

According to the AOS-CX REST API Reference basics1, one of the predefined user roles is:

sysops: Users with this role can view switch configuration information and have access to the PUT and POST methods for REST API. They can also use the PATCH and DELETE methods for REST API, but not for all resources. Users with this role can perform system operations on the switch, such as backup, restore, upgrade, or reboot.

The other options are incorrect because:

A) administrators: Users with this role have full access to all switch configuration information and all REST API methods. This role is more than what the customer requires.

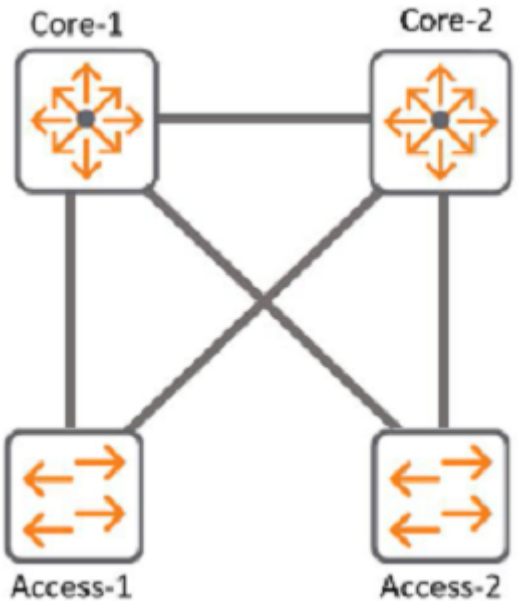
B) auditors: Users with this role can only view switch configuration information and have access to the GET method for REST API. They cannot use the PUT and POST methods for REST API.

D) helpdesk: Users with this role can view switch configuration information and have access to the GET method for REST API. They can also use the PATCH method for REST API, but only for a limited set of resources. They cannot use the PUT and POST methods for REST API.

Question 2

Question Type: MultipleChoice

Refer to Exhibit:



With Access-1, What needs to be identically configured With MSTP to load-balance VLANS?

Options:

A- Spanning-tree bpdu-guard setting

B- Spanning-tree instance vlan mapppjng

C- spanning-tree Cist mapping

D- Spanning-tree root-guard setting

Answer:

B

Explanation:

The correct answer is B. Spanning-tree instance VLAN mapping.

To load-balance VLANs with MSTP, you need to configure the same VLAN-to-instance mapping on all switches in the same MST region. This means that you need to assign different VLANs to different MST instances, and then adjust the spanning tree parameters (such as priority, cost, or port role) for each instance to achieve the desired load balancing. For example, you can make one switch the root for instance 1 and another switch the root for instance 2, and then map half of the VLANs to instance 1 and the other half to instance 2.

According to the Cisco document Understand the Multiple Spanning Tree Protocol (802.1s), one of the steps to configure MST is:

Split your set of VLANs into more instances and configure different MST settings for each of these instances. In order to easily achieve this, elect Bridge D1 to be the root for VLANs 501 through 1000, and Bridge D2 to be the root for VLANs 1 through 500. These statements are true for this configuration:

Switch D1(config)#spanning-tree mst configuration

Switch D1(config-mst)#instance 1 vlan 501-1000

Switch D1(config-mst)#exit

Switch D1(config)#spanning-tree mst 1 priority 0

Switch D2(config)#spanning-tree mst configuration

Switch D2(config-mst)#instance 2 vlan 1-500

Switch D2(config-mst)#exit

Switch D2(config)#spanning-tree mst 2 priority 0

The above commands create two MST instances, 1 and 2, and map VLANs 501-1000 to instance 1 and VLANs 1-500 to instance 2. Then, they make switch D1 the root for instance 1 and switch D2 the root for instance 2.

The other options are incorrect because:

A) Spanning-tree bpdu-guard setting is a security feature that disables a port if it receives a BPDU from an unauthorized device. It does not affect load balancing with MSTP.

C) Spanning-tree CIST mapping is not a valid command. CIST stands for Common and Internal Spanning Tree, which is the spanning tree instance that runs within an MST region and interacts with other regions or non-MST switches.

D) Spanning-tree root-guard setting is another security feature that prevents a port from becoming a root port if it receives superior BPDUs from another switch. It does not affect load balancing with MSTP.

Question 3

Question Type: MultipleChoice

you need to have different routing-table requirements With Aruba CX 6300 VSF configuration.

Assuming the correct layer-2 VLAN already exists, how would you create a new SVI for a separate routing table?

Options:

A- create a new VLAN, and attach the VRF to it.

B- Create a new routing table, and attach VLANS to it

C- Create a new SVI and use attach command.

D- Create a new VLAN. and attach the routing table to it

Answer:

C

Explanation:

The correct answer is C. Create a new SVI and use attach command.

To create a new SVI for a separate routing table, you need to use the attach command to associate the SVI with a VRF (Virtual Routing and Forwarding) instance. A VRF is a logical entity that allows multiple routing tables to coexist on the same switch. Each VRF has its own set of interfaces, routing protocols, and routes that are isolated from other VRFs.

According to the AOS-CX Virtual Switching Framework (VSF) Guide1, one of the steps to configure VRF-aware VSF is:

Configure the VRFs on each member switch and assign the SVIs to the respective VRFs using the attach command. For example:

switch(config)# vrf red

switch(config-vrf)# exit

switch(config)# interface vlan 10

switch(config-if-vlan)# ip address 10.1.1.1/24

switch(config-if-vlan)# attach vrf red

The above commands create a VRF named red and assign VLAN 10 SVI to it. The SVI has an IP address of 10.1.1.1/24.

The other options are incorrect because:

A) You cannot attach a VRF to a VLAN directly. You need to create an SVI for the VLAN and then attach the VRF to the SVI.

B) You cannot create a new routing table manually. You need to create a VRF and then use routing protocols or static routes to populate the routing table for the VRF.

D) You cannot attach a routing table to a VLAN directly. You need to create an SVI for the VLAN and then attach a VRF that has a routing table associated with it.

Question 4

Question Type: MultipleChoice

What is used to retrieve data stored in a Management Information Base (MIS)?

SNMPv3

DSCP

TLV

CDP

Options:

A- SNMPv3.

SNMPv3 is a protocol that is used to retrieve data stored in a Management Information Base (MIB), which is a database of managed objects in a network. SNMPv3 provides security and access control features that are not available in earlier versions of SNMP. SNMPv3 can also use encryption to protect the data from unauthorized access or modification.

According to the Aruba Certified Professional -- Campus Access document1, one of the skills that this certification validates is: Implement and Analyze the output from common network monitoring tools

Configure Port Mirroring to collect PCAPs
Configure NAE agents 9.4
Configure UXI sensors for internal and external tests
Describe how API scan be used to configure, manage, monitor, and troubleshoot your network
The document also mentions that the candidate should have a distinguished understanding of different protocols across vendors, which implies that they should be familiar with SNMPv3 and how it can be used to access MIB data.

Answer:

A

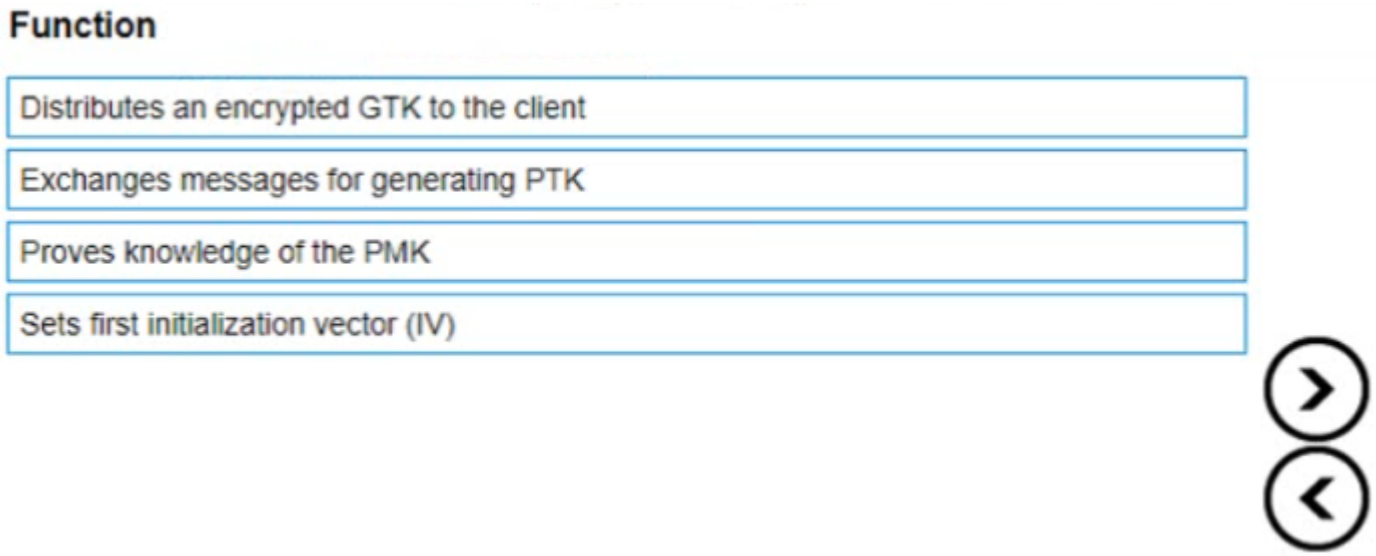
Explanation:

The correct answer is

Question 5

Question Type: **OrderList**

List the WPA 4-Way Handshake functions in the correct order.



Answer:

Exchanges messages for generating PTK Distrib

Question 6

Question Type: MultipleChoice

Due to a shipping error, five (5) Aruba AP-515S and one (1) Aruba CX 6300 were sent directly to your new branch office You have configured a new group persona for the new branch office devices in Central, but you do not know their MAC addresses or serial

numbers The office manager is instructed via text message on their smartphone to onboard all the new hardware into Aruba Central

What application must the office manager use on their phone to complete this task?

Options:

A- Aruba Onboard App

B- Aruba Central App

C- Aruba CX Mobile App

D- Aruba installer App

Answer:

D

Explanation:

Aruba Installer App is a mobile app that simplifies site installations and enables network connectivity for Aruba devices. The app allows the user to scan the barcode of the device and add it to the network using Aruba Central.The app also automates importing Aruba devices into Aruba NetEdit for intelligent configuration management and continuous conformance validation

Question 7

Question Type: DragDrop

Match the terms below to their characteristics (Options may be used more than once or not at all.)

Explanation:

The terms broadcast, IP directed broadcast, multicast, and unicast are different types of communication or data transmission over a network. They differ in how many devices are involved in the communication and how they address the messages.The following table summarizes the characteristics of each term1:

Question 8

Question Type: MultipleChoice

A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working across the campus which is connected via layer-3. The legacy devices are connected to Aruba CX 6300 switches throughout the campus.

Which technology minimizes flooding so the legacy application can work efficiently?

Options:

A- Generic Routing Encapsulation (GRE)

B- EVPN-VXLAN

C- Ethernet over IP (EolP)

D- Static VXLAN

Answer:

B

Explanation:

EVPN-VXLAN is a technology that allows layer-2 communication across layer-3 networks by using Ethernet VPN (EVPN) as a control plane and Virtual Extensible LAN (VXLAN) as a data plane3. EVPN-VXLAN can be used to support legacy applications that communicate at layer-2 across different campuses or data centers that are connected via layer-3.EVPN-VXLAN minimizes flooding by using BGP to distribute MAC addresses and IP addresses of hosts across different VXLAN segments3.EVPN-VXLAN also provides benefits such as loop prevention, load balancing, mobility, and scalability3.
Reference:3https://www.arubanetworks.com/assets/tg/TG_EVPN_VXLAN.pdf

Question 9

Question Type: MultipleChoice

A network engineer recently identified that a wired device connected to a CX Switch is misbehaving on the network To address this issue, a new ClearPass policy has been put in place to prevent this device from connecting to the network again.

Which steps need to be implemented to allow ClearPass to perform a CoA and change the access for this wired device? (Select two.)

Options:

A- Confirm that NTP is configured on the switch and ClearPass

B- Configure dynamic authorization on the switch.

C- Bounce the switchport

D- Use Dynamic Segmentation.

E- Configure dynamic authorization on the switchport

Answer:

B, C

Explanation:

CoA (Change of Authorization) is a feature that allows ClearPass to dynamically change the authorization and access privileges of a device after it has been authenticated1.CoA uses RADIUS messages to communicate with the network device and instruct it to perform an action, such as reauthenticating the device, applying a new VLAN or user role, or disconnecting the device2.

To enable CoA on a CX switch, the network engineer needs to configure dynamic authorization on the switch, which is a global command that allows the switch to accept RADIUS messages from ClearPass and execute the requested actions3.The network engineer also needs to specify the IP address and shared secret of ClearPass as a dynamic authorization client on the switch3.

To trigger CoA for a specific wired device, the network engineer needs to bounce the switchport, which is an action that temporarily disables and re-enables the port where the device is connected. This forces the device to reauthenticate and receive the new policy from

ClearPass. Bouncing the switchport can be done manually by using the interface shutdown and no shutdown commands, or automatically by using ClearPass as a CoA server and sending a RADIUS message with the Port-Bounce-Host AVP (Attribute-Value Pair).