Free Questions for 300-430 by actualtestdumps

Shared by Sanders on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Refer to the exhibit.

```
aaa new-model
aaa local authentication default authorization default
aaa group server radius rad-group
 server name ise-lab272
aaa authentication login default local
┌─────────────────────────────────────────────────────┐
│                                                     │
└─────────────────────────────────────────────────────┘
wireless profile policy test profiling
   accounting-list acct method
   radius-profiling
```

A network architect configured the Cisco Catalyst 9800 Series Controller to find out information on client types in the wireless network. RADIUS profiling is enabled so that the controller forwards the information about clients to a Cisco ISE server through vendor-specific RADIUS attributes. The ISE server is not profiling any data from the controller. Which configuration must be added in the blank in the code to accomplish the profiling on the Cisco 9800 Series controller?

Options:
A- aaa accounting identity acct_method start-stop group rad-group

B- aaa accounting network acct_method start-stop group rad-group

C- aaa accounting exec acct_method start-stop group rad-group

D- aaa accounting commands acct_method start-stop group rad-group
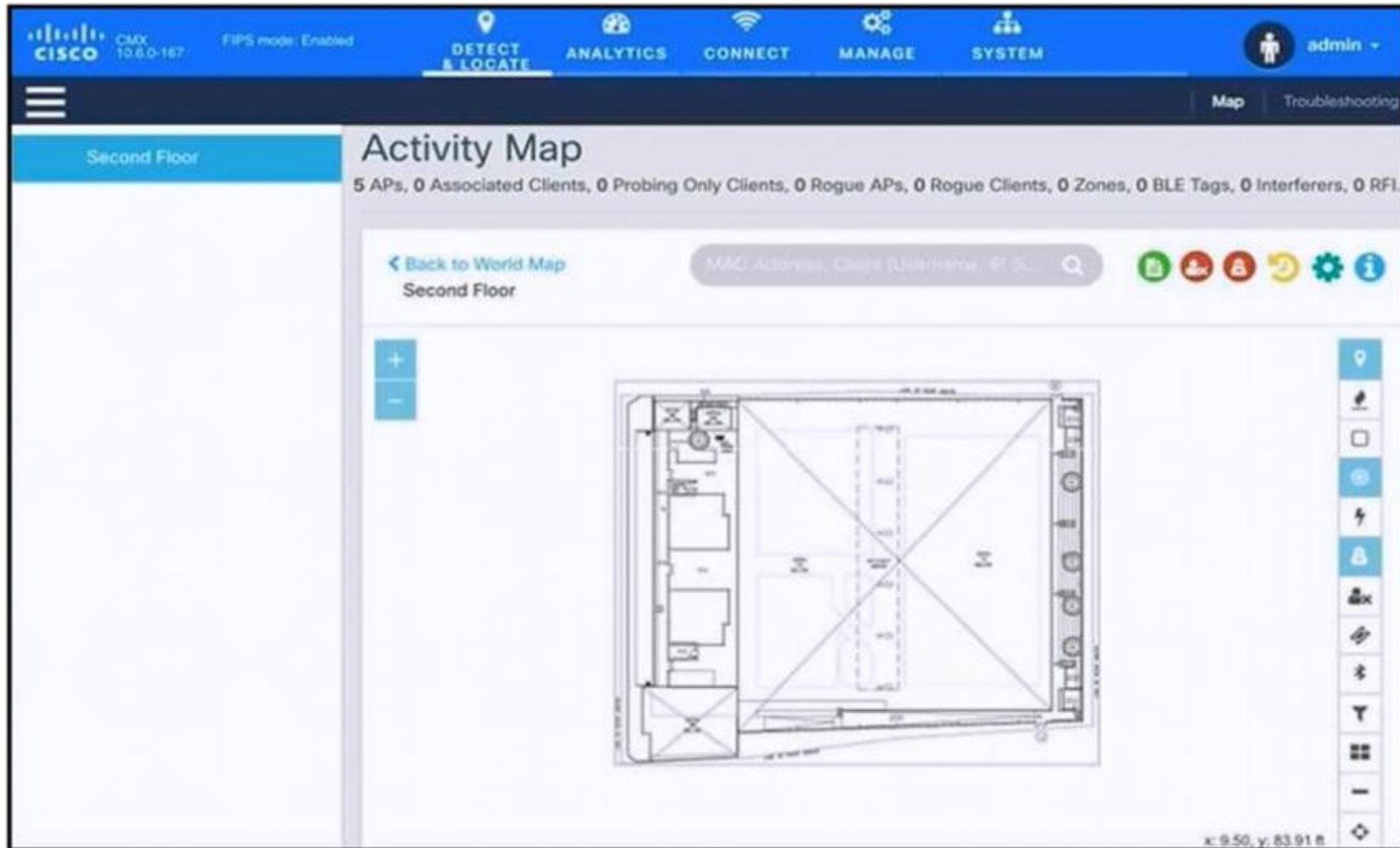
Answer:

B

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

An engineer has deployed the Cisco CMX solution to track and detect the number of users who visit the office each day. The CMX dashboard is not showing any dat

a. Which action resolves this issue?

Options:

A- Configure Single Sign-On authentication.

B- Add the WLCs to CMX.

C- Copy the exported Maps from CMX server to PI using SCP.

D- Install an evaluation license to CMX server.

Answer:

B

Question 3

Question Type: **MultipleChoice**

A wireless engineer deployed all remote sites as FlexConnect. The client VLAN assignment on these sites is configured manually mapped by WLAN and using local switching. Dynamic VLAN assignment is provided by the newly deployed Cisco ISE. Which IETF attribute must be configured on the AAA server to send that VLAN ID?

Options:

A- Tunnel-Medium-Type

B- Tunnel-Client-Endpoint

C- Tunnel-Assignment-ID

D- Tunnel-Private-Group-ID

Answer:

D

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

General		Session		Security		Mobility	
User Name	Unknown	SSID	Test	802.11 Authentication	Open System	Mobility Status	Local
MAC Address	40:83:1d:33:6a:dd	Protocol	802.11ac	Security Policy Type	WPA2	Mobility Controller	Data Not Available
IP Address	fe80:486:14bc:44aa:1428	802.11 State	Associated	EAP Type	Unknown	Anchor Mobility Controller	Data Not Available
Vendor	Unknown	Management VLAN ID	292	Policy Manager State	DHCP_REQD	Anchor Controller	N/A
Endpoint Type	none	Interface	management	On Network	No	Mobility Oracle	Data Not Available
Hostname	Data Not Available	Location	Root Area	Radius NAC State	DHCP_REQD	Mobility Group	Data Not Available
Client Type	Regular	Controller Name	WLC1_CX	Encryption Cipher	CCMP (AES)	Switch Peer Group	Data Not Available
Media Type	Lightweight	Controller IP Address/DNS Name	10.88.255.137	Reason Code	Unspecified	Anchor Switch Peer Group	Data Not Available
E2E	Not Supported	AP Name	AP3702e	SNMP NAC State	Access		
802.11u Capable	false	AP IP Address	10.99.22.178	AAA Override ACL Name			
Power Save	OFF	AP Type	Cisco AP	AAA Override ACL Applied Status	N/A		
CCX	Not Supported	AP Base Radio MAC	80:e0:1d:ac:87:80	Redirect URL			
Local Policy Name	none	Association ID	1	ACL Name			
Policy AAA Role	none	Port	8	ACL Applied Status	N/A		
		Profile Name	Test	FlexConnect Local Authentication	No		
		Data Switching	Central	Authenticating ISE	Data Not Available		

What is the reason that the wireless client cannot get the RUN state?

Options:

A- It has no communication with Cisco ISE.

B- An authentication error has occurred.

C- It is not getting the IP address.

D- Because of central switching, the AP must reach the Cisco ISE directly.

Answer:

C

Question 5

Question Type: **MultipleChoice**

WPA2 Enterprise with 802.1X is being used for clients to authenticate to a wireless network through a Cisco ISE server. For security reasons, the network engineer wants to ensure that only PEAP authentication is used. The engineer sent instructions to clients on how to configure the supplicants, but the ISE logs still show users authenticating using EAP-FAST. Which action ensures that access to the network is restricted for these users unless the correct authentication mechanism is configured?

Options:

A- Enable AAA override on the SSID, gather the usernames of these users, and disable the RADIUS accounts until the devices are correctly configured.

B- Enable AAA override on the SSID and configure an ACL on the WLC that allows access to users with IP addresses from a specific subnet.

C- Enable AAA override on the SSID and configure an access policy in Cisco ISE that denies access to the list of MACs that have used EAP-FAST.

D- Enable AAA override on the SSID and configure an access policy in Cisco ISE that allows access only when the EAP authentication

method is PEAP.

Answer:

D

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.

Maps Tree View

Floor Settings

- ☑ Access Points ›
- ☐ AP Heatmaps ›
- ☐ Coverage Areas
- ☐ Location Regions
- ☐ Obstacles
- ☐ Rails
- ☐ Markers
- ☐ Chokepoints
- ☐ Wifi TDOA Receivers
- ☐ GPS Markers
- ☐ Services

An engineer must provide a position of rogue APs on a floor map using Cisco PI 3.0, but no rogue AP options are showing on the left-hand navigation menu under Maps. What is the reason for this omission?

Options:

A- An assurance license is not installed.

B- The controller operational status background task is disabled.

C- The Show Detected Interferers feature under the AP option is disabled.

D- Cisco MSE has not been added to Cisco PI.

Answer:

A

Question 7

Question Type: **MultipleChoice**

A network administrator just completed the basic implementation of Cisco CMX and tries to implement location tracking. The administrator is having trouble establishing connectivity between one of the WLCs through NMSP. What must be configured to establish this connectivity? (Choose two.)

Options:

A- Add permanent licenses on the Cisco CMX server.

B- Allow on the firewall port 16113 between Cisco CMX and the WLC.

C- Enable NMSP on the WLC.

D- Reboot Cisco CMX after adding the WLC for the first time.

E- Add to the WLC the MAC address and SSC key for the Cisco CMX server.

Answer:

B, C

Question 8

Question Type: **MultipleChoice**

Refer to the exhibit.

```
(Test-1) >show network summary
RF-Network Name.............................. Test-1
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Web Mode Cipher-Option High........... Disable
Secure Web Mode Cipher-Option SSLv2.......... Disable
Secure Web Mode RC4 Cipher Preference........ Disable
OCSP......................................... Disabled
OCSP responder URL...........................
Secure Shell (ssh)........................... Enable
Telnet....................................... Disable
Ethernet Multicast Forwarding................ Disable
Ethernet Broadcast Forwarding................ Disable
IPv4 AP Multicast/Broadcast Mode............. Unicast
IGMP snooping................................ Disabled
IGMP timeout................................. 60 seconds
IGMP Query Interval.......................... 20 seconds
MLD snooping................................. Disabled
MLD timeout.................................. 60 seconds
MLD query interval........................... 20 seconds
User Idle Timeout............................ 3600 seconds
ARP Idle Timeout............................. 3600 seconds
Cisco AP Default Master...................... Disable
AP Join Priority............................. Disable

WebPortal Online Client ..................... 0
mDNS snooping................................ Disabled
mDNS Query Interval.......................... 15 minutes

(Test-1) >show mdns service summary
Number of Services............................... 5

Service-Name                        LSS   Origin     No SP    Service-string
----------------------------------- ----  ---------- -----    ---------------
AirPrint                            No    All           0     _ipp._tcp.local.
AppleTV                             No    All           0     _airplay._tcp.local.
HP_Photosmart_Printer_1             No    All           0     _universal._sub._ipp.
_tcp.local.
HP_Photosmart_Printer_2             No    All           0     _cups._sub._ipp._tcp.
local.
Printer                             No    All           0     _printer._tcp.local.
```

An engineer configured a BYOD policy that allows for printing on the WLAN using Bonjour services. However, the engineer cannot get printing to work. The WLC firmware is 8.x. What must be implemented on the controller?

Options:

A- Enable mDNS and IGMP snooping.

B- Activate location-specific services.

C- Configure Secure Web Mode Cipher-Option SSLv2.

D- Increase the IGMP Query Interval value

Answer:

B

Question 9

Question Type: **MultipleChoice**

An engineer is planning an image upgrade of the WLC, and hundreds of APs are spread across remote sites with limited WAN bandwidth. The engineer must minimize the WAN utilization for this upgrade. Which approach must be used for the AP image upgrade?

Options:

A- Predownload the new code to the APs.

B- Use the Smart AP image upgrade feature.

C- Allow the APs to download their code after WLC reboot.

D- Execute parallel TFTP code upgrade on the APs via SSH.

Answer:

B

Question 10

Question Type: **MultipleChoice**

A network administrator managing a Cisco Catalyst 9800 WLC must place all iOS connected devices to the guest SSID on VLAN 101. The rest of the clients must connect on VLAN 102 distribute load across subnets. To achieve this configuration, the administrator configures a local policy on the WLC. Which two configurations are required? (Choose two.)

Options:

A- Assign a policy map under global security policy settings.

B- Add local profiling policy under global security policy settings.

C- Create a service template.

D- Allow HTTP and DHCP profiling under policy map.

E- Enable device classification on global wireless settings.

Answer:

C, E

Question 11

A network engineer must get an autonomous AP to authenticate to the upstream switch via IEEE 802.1 X. Drag and drop the commands from the left onto the right to complete the configuration.

Answer Area

Answer:

ap(config-if)#dot1x credentials [PROFILE NAME]	step 1
ap(config-dot1x-creden)#password {0	7	LINE}	step 2
ap(config)#dot1x credentials [PROFILE NAME]	step 3
ap(config-dot1x-creden)#username username	step 4
ap(config)#interface gigabitethernet 0	step 5

To Get Premium Files for 300-430 Visit

https://www.p2pexams.com/products/300-430

For More Free Questions Visit

https://www.p2pexams.com/cisco/pdf/300-430

20% DISCOUNT