



Free Questions for HPE6-A79 by go4braindumps

Shared by Flowers on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

```
(MC11) [mynode] #show ap database | exclude =
```

AP Database

Name	Group	AP Type	IP Address	Status	Flags	Switch IP	Standby IP	Wired MAC Address	Serial #	Port	FQLN	Outer IP	User
AP21	CAMPUS	355	10.1.145.150	Up 3m:20s	UNI	10.254.13.14	0.0.0.0	xx:xx:xx:xx:xx:xx	CNBJ0Y301	N/A	N/A	N/A	
AP22	CAMPUS	355	10.1.146.150	Up 32m:23s		10.254.13.14	0.0.0.0	xx:xx:xx:xx:xx:xy	CNBJ0Y305	N/A	N/A	N/A	

Total Aps:2

```
(MC11) [mynode] #show ap active | exclude =
```

Active AP Table

Name	Group	IP Address	11g Clients	11g Ch/EIRP/MaxEIRP	11a Clients	11a Ch/EIRP/MaxEIRP	AP Type	Flags	Uptime	Outer IP
AP21	CAMPUS	10.1.146.150	0	AP:HT:11/9.0/24.0	0	AP:VHT:153E:/18.0/28.5	355	Aa	32m:30s	N/A

channel followed by "*" indicates channel selected due to unsupported configured channel.
"spectrum" followed by "^" indicates local spectrum override in effect.

Num Aps:1

A network administrator deploys a new Mobility Master (MM) - Mobility Controller (MC) network. To test the solution, the network administrator accesses the console of a pair of APs and statically provisions them. However, one of the APs does not propagate the configured SSIDs. The network administrator looks at the logs and sees the output shown in the exhibit.

Which actions must the network administrator take to solve the problem?

Options:

- A-** Create another AP group in the MC's configuration, and re-provision one AP with a different group.
- B-** Re-provision one of the APs with a different name, and add new entries with the proper group in the whitelist.
- C-** Re-provision the AP with a different group, and modify the name of one AP in the whitelist.
- D-** Re-provision one of the APs with a different name or modify the name in the whitelist.

Answer:

D

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

(MC14-1) #show aaa authentication dot1x Corp-Network

802.1X Authentication Profile "Corp-Network"

```
-----  
Parameter                                         Value  
-----  
Max authentication failures                       0  
Enforce Machine Authentication                   Enabled  
Machine Authentication: Default Machine Role     guest  
Machine Authentication Cache Timeout             24 hr(s)  
Blacklist on Machine Authentication Failure      Disabled  
Machine Authentication: Default User Role        guest  
Interval between Identity Requests               5 sec  
Quiet Period after Failed Authentication         30 sec  
Reauthentication Interval                        86400 sec  
Use Server provided Reauthentication Interval    Disabled  
Use the termination-action attribute from the Server Disabled  
Multicast Key Rotation Time Interval             1800 sec  
Unicast Key Rotation Time Interval               900 sec  
Authentication Server Retry Interval             5 sec  
Authentication Server Retry Count                3  
Framed MTU                                       1100 bytes  
Max number of requests sent during an Auth attempt 5  
Max Number of Reauthentication Attempts          3  
Maximum number of times Held State can be bypassed 0  
Dynamic WEP Key Message Retry Count              1  
Dynamic WEP Key Size                             128 bits  
Interval between WPA/WPA2 Key Messages          1000 msec  
Delay between EAP-Success and WPA2 Unicast Key Exchange 0 msec  
Delay between WPA/WPA2 Unicast Key and Group Key Exchange 0 msec  
Time interval after which the PMKSA will be deleted 8 hr(s)  
Delete Keycache upon user deletion              Disabled  
WPA/WPA2 Key Messages Retry Count                3  
Multicast Key Rotation                           Disabled  
Unicast Key Rotation                             Disabled  
Reauthentication                                 Disabled  
Opportunistic Key Caching                        Enabled
```

The network administrator must ensure that the configuration will force users to authenticate periodically every eight hours. Which configuration is required to effect this change?

Options:

- A-** Set the reauth-period to 28800 enable reauthentication in the dot1x profile.
- B-** Set the reauth-period to 28800 enable reauthentication in the AAA profile.
- C-** Set the reauth-period to 28800 enable reauthentication in both dot1x and AAA profile.
- D-** Set the reauth-period to 28800 in the dot1x profile and enable reauthentication in the AAA profile.

Answer:

A

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

```
(MC1) [mynode] #show ap database
```

AP Database

Name	Group	AP Type	IP Address	Status	Flags	Switch IP	Standby IP
AP1	Main-Campus-SC-B1	355	10.1.145.150	Up 1d:7h:21m:41s	2	10.1.140.100	0.0.0.0
AP2	Main-Campus-SC-B1	355	10.1.146.150	Up 1d:7h:21m:46s	2	10.1.140.100	0.0.0.0

Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- = 802.1x use factory cert; 2 = Using IKE version 2
B = Built-in AP; C = Cellular RAP; D = Dirty or no config
E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
G = no such group; I = Inactive; J = USB cert at AP; L = Unlicensed
M = Mesh node
N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
Y = Mesh Recovery
c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z = Datazone AP

Total APs:2

```
(MC1) [MDC] #
```

```
(MC1) [MDC] #show lc-cluster group-membership
```

Cluster Enabled, Profile Name = "Cluster1"

Redundancy Mode On

Active Client Rebalance Threshold = 50%

Standby Client Rebalance Threshold = 75%

Unbalance Threshold = 5%

AP Load Balancing: Disabled

Cluster Info Table

Type	IPv4 Address	Priority	Connection-Type	STATUS
self	10.1.140.100	10	N/A	ISOLATED (Leader)
peer	10.1.140.101	101	N/A	INCOMPATIBLE (CLUSTER_NAME_MISMATCH)

After deploying several cluster pairs, the network administrator notices that all APs assigned to Cluster1 communicate with MC1 instead of being distributed between members of the cluster. Also, no IP addresses are shown under the Standby IP column.

What should the network administrator do to fix this situation?

Options:

- A- Apply the same cluster profile to both members.
- B- Enable Cluster AP load balancing.
- C- Rename the cluster profile as 'CLUSTER1'.
- D- Place MCs at the same hierarchical group level.

Answer:

C

Question 4

Question Type: MultipleChoice

Refer to the exhibits.

Request Details

Summary Input **Output**

Enforcement Profiles: {Wired-802.1X

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role tunneled-employee

◀ Showing 8 of 1-20 records ▶▶

Change Status

Show Configuration

Export

Show Logs

Close

Access-1# show ubt users all

Displaying All UBT Users for Zone: zone1
Downloaded user roles are preceded by *

Port	Mac-Address	Tunnel Status	Secondary-UserRole	Failure Reason
------	-------------	---------------	--------------------	----------------

Access-1#

Access-1# show ubt state

Local Master Server (LMS) State:

LMS Type	IP Address	State
Primary	: 10.1.224.100	ready_for_bootstrap
Secondary	: 10.1.140.100	ready_for_bootstrap

Switch Anchor Controller (SAC) State:

	IP Address	MAC Address	State
Active	: 10.1.224.100	xx:xx:xx:xx:xx:xx	Registered

Access-1#

Access-1# show aaa authentication port-access int 1/1/20 client-status

Port Access Client Status Details

Client xx:xx:xx:xx:yy:yy, philip.swift

=====
Session Details

Port : 1/1/20
Session Time : 378s

Authentication Details

Status : dot1x Authenticated
Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted

Authorization Details

Role :
Status : Invalid

Access-1# █

A network administrator deploys User Based Tunneling (UBT) in a corporate network to unify the security policies enforcement. When users authenticate with 802.1X, ClearPass shows Accept results, and sends the Aruba-User-Role attribute as expected. However, the AOS-CX based switch does not seem to build the tunnel to the Mobility Controller (MC) for this user.

Why does the switch fail to run UBT for the user?

Options:

- A- The switch has not fully associated to the MC.
- B- ClearPass is sending the wrong Vendor ID.
- C- The switch is not configured with the gateway-role.
- D- ClearPass is sending the wrong VSA type.
- E- The switch is not configured with the port-access role.

Answer:

B

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

```
(MC1) [MDC] #show ip access-list no-webapps
```

```
ip access-list session no-webapps
no-webapps
```

Priority	Source	Destination	Service	Application	Action	TimeRange	Log	Expired	Queue	TOS	8021P	Blacklist	Mirror	Di
1	user	any		app facebook	deny send-deny-response				Low					
2	user	any		app youtube	deny send-deny-response				Low					
3	user	any		app netflix	deny send-deny-response				Low					

A network administrator completes the initial configuration dialog of the Mobility Controllers (MCs) and they join the Mobility Master (MM) for the first time. After the MM-MC association process, network administrator only creates AP groups, VAPs, and roles. Next, the network administrator proceeds with the configuration of the policies and creates the policy shown in the exhibit.

Which additional steps must be done to make sure this configuration takes effect over the contractor users?

- A. Apply the policy in the contractors user role.
 - Enable deep packet inspection.
 - Reload the MCs.
- B. Enable firewall visibility.
 - Enable web-content classification.
 - Reload the MCs.
- C. Apply the policy in the contractors user role.
 - Enable deep packet inspection.
- D. Enable firewall visibility.
 - Enable web-content classification.
 - Reload the MMs.

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

C

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

```
(MC2) [MDC] #show user mac xx:xx:xx:xx:xx:xx
```

This operation can take a while depending on number of users. Please be patient

```
Name: contractor14, IP:10.1.141.150, MAC: xx:xx:xx:xx:xx:xx, Age: 00:00:00
Role: contractor (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 128/0
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: ClearPass.23
Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE_DERIVATION_DOT1X_VSA
```

A network administrator is evaluating a deployment to validate that a user is assigned the proper role and reviews the output in the exhibit. How is the role assigned to user?

Options:

- A- The MC assigned the role based on Aruba VSAs.
- B- The MC assigned the machine authentication default user role.
- C- The MC assigned the default role based on the authentication method.
- D- The MC assigned the role based on server derivation rules.

Answer:

C

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

0 AirGroup Servers

0 AirGroup Clients

6 Calls

Wireless calls 6

USERNAME	START TIME	STATE	TERMINATIO...	DIRECTION	AP NAME	ALG	WIRELESS ONLY CALL QUALITY
hector.barbosa	2020-06-26 18:2...	Success	Terminated	NA	AP1	Skype4B	Fair

CALLERS

From
Client

IP Address
10.1.141.150

MAC Address
xx:xx:xx:xx:xx:xx

Username
hector.barbosa

To

Destination IP
10.254.1.24

CALL INFORMATION

Start time
2020-06-26 18:24:56

Duration
1m 13s

AP Name
AP1

Client health
67%

In call roam
No

QoS correction
Yes

CDR
6

UCC call ID

State
Success

Termination reason
Terminated

ALG
Skype4B

Controller
10.1.140.101

CALL HEALTH

Wireless-only	Controller	End
Fair	Good	Unk
Score 60.88	Score 80.67	Scor
Delay 32.58 msec	Delay -	Del
Jitter 7.21 msec	Jitter 31.16 msec	Jitte
Packet loss 5.02%	Packet loss 0.3%	Pac

A network administrator has recently enabled WMM on the VAP's SSID profile and enabled UCC Skype4B ALG at the Mobility Master level. During testing, some voice and video conference calls were made, and it was concluded that the call quality has dramatically improved. However, end to end information isn't displayed in the call's details. Also, Skype4B app-sharing's performance is poor at times.

What must the administrator do next in order to enable end to end call visibility and QoS correction to app-sharing service?

Options:

- A-** Deploy the SDN API Software in the Skype4B Solution and point to the MM.
- B-** Increase the app-sharing DSCP value in the Skype4B ALG profile.
- C-** Enable UCC monitoring on the 'default-controller' mgmt.-server profile.
- D-** Enable the App-sharing ALG profile at both MM and MD hierarchy levels.

Answer:

D

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac xx:xx:xx:xx:xx:xx count 27
```

```
Warning: user-debug is enabled on one or more specific MAC addresses;  
only those MAC addresses appear in the trace buffer.
```

Auth Trace Buffer

```
Jun 29 20:56:51 station-up      * xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy - - wpa2 aes
Jun 29 20:56:51 eap-id-req      <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 1 5
Jun 29 20:56:51 eap-start       -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy - -
Jun 29 20:56:51 eap-id-req      <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 1 5
Jun 29 20:56:51 eap-id-req      <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 1 5
Jun 29 20:56:51 eap-id-resp     -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 1 7 it
Jun 29 20:56:51 rad-req         -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 42 174 10.1.140.101
Jun 29 20:56:51 eap-id-resp     -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 1 7 it
Jun 29 20:56:51 rad-resp        <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1 42 88
Jun 29 20:56:51 eap-req         <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 2 6
Jun 29 20:56:51 eap-resp        -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 2 214
Jun 29 20:56:51 rad-req         -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1 43 423 10.1.140.101
Jun 29 20:56:51 rad-resp        <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1 43 228
Jun 29 20:56:51 eap-req         <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 3 146
Jun 29 20:56:51 eap-resp        -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 3 61
Jun 29 20:56:51 rad-req         -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1 44 270 10.1.140.101
Jun 29 20:56:51 rad-resp        <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1 44 128
Jun 29 20:56:51 eap-req         <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 4 46
Jun 29 20:56:51 eap-resp        -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 4 46
Jun 29 20:56:51 rad-req         -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1 45 255 10.1.140.101
Jun 29 20:56:51 rad-accept      <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1 45 231
Jun 29 20:56:51 eap-success     <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 4 4
Jun 29 20:56:51 user repkey change * xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 65535 - 204c0306e79000000170008
Jun 29 20:56:51 macuser repkey change * xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy 65535 - xx:xx:xx:xx:xx:xx
Jun 29 20:56:51 wpa2-key1       <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy - 117
Jun 29 20:56:51 wpa2-key2       -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy - 117
Jun 29 20:56:51 wpa2-key3       <- xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy - 151
Jun 29 20:56:51 wpa2-key4       -> xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy - 95
```

A network administrator is validating client connectivity and executes the show command shown in the exhibit. Which authentication method was used by a wireless station?

Options:

- A- EAP authentication
- B- 802.1X machine authentication
- C- MAC authentication
- D- 802.1X user authentication

Answer:

D

To Get Premium Files for HPE6-A79 Visit

<https://www.p2pexams.com/products/hpe6-a79>

For More Free Questions Visit

<https://www.p2pexams.com/hp/pdf/hpe6-a79>

