Free Questions for HPE6-A79 by braindumpscollection

Shared by Rich on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A network administrator is in charge of a Mobility Master (MM) -- Mobility Controller (MC) based network security. Recently the Air Monitors detected a Rogue AP in the network and the administrator wants to enable "Tarpit" based wireless containment.

What profile must the administrator enable "tarpit" wireless containment on?

Options:

A- IDS Unauthorized device profile

B- IDS profile

C- IDS General profile

D- IDS DOS profile

Answer:

A

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

```
(MC_VA) [mynode] #show aaa debug role user mac xx:xx:xx:xx:xx:xx


Role Derivation History
=======================
    0: l2 role->logon, mac user created
    1: l2 role->authenticated, station Authenticated with auth type: 802.1x
    2: l2 role->corp, RFC 3576 l3 role change COA
(MC_VA) [mynode] #
```

A network administrator has Mobility Master (MM) - Mobility Controller (MC) based network and has fully integrated the MCs with ClearPass for RADIUS-based AAA services. The administrator is testing different ways to run user role derivation.

Based on the show command output, what method has the administrator use for assigning the "corp" role to client with MAC xx:xx:xx:xx:xx:xx?

Options:

A- Dynamic Authorization using VSA attributes.

B- Dynamic Authorization using IETF attributes.

C- Server Derivation Rules using IETF attributes.

D- User Derivation Rules using the client's MAC.

Answer:

A

Question 3

Question Type: **MultipleChoice**

Refer to the exhibits.

```
(MM1) [md] #configure t
Enter Configuration commands, one per line. End with CNNL/Z

(MM1) [md] (config) #user-role corp-employee
(MM1) ^[md] (config-submode)#access-list session allowall
(MM1) ^[md] (config-submode)#exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #aaa profile corp-employee
(MM1) ^[md] (AAA Profile "corp-employee") #dot1x-default-role corp-employee
(MM1) ^[md] (AAA Profile "corp-employee") #dot1x-server-group Radius
(MM1) ^[md] (AAA Profile "corp-employee") #exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #write memory

Saving Configuration...

Configuration Saved.
```

```
(MM1) [md] (config) #cd MC1
(MM1) [20:4c:03:06:e5:c0] (config) #mdc
```

```
Redirecting to Managed Device Shell

(MC1)  [MDC] #show switches

All Switches
------------
IP Address    IPv6 Address  Name  Location          Type  Model      Version        Status  Configuration State  Config Sy
----------    ------------  ----  --------          ----  -----      -------        ------  -------------------  ---------
10.1.140.100  None          MC1   Building1.floor1  MD    Aruba7030  8.6.0.2_73853  up      UPDATE SUCCESSFUL    11

Total Switches:1
(MC1) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP              MAC             Name           Role    Age(d:h:m)  Auth     VPN link  AP name  Roaming   Essid/Bssid/Ph
----------    ------------       ------          ----    ----------  ----     --------  -------  -------
10.1.141.150  yy:yy:yy:yy:yy:yy  hector.barbosa  guest   00:00:23    802.1x             AP22     Wireless  corp-employee/

User Entries: 1/1
 Curr/Cum Alloc:3/18 Free:0/15 Dyn:3 AllocErr:0 FreeErr:0
(MC1) [MD] #show aaa profile corp-employee
```

```
AAA Profile “corp-employee”
---------------------------
Parameter                                                  Value
---------                                                  -----
Initial role                                               guest
MAC Authentication Profile                                 N/A
MAC Authentication Server Group                            default
802.1X Authentication Profile                              corp-employee_dot1_aut
802.1X Authentication Server Group                         Radius
Download Role from CPPM                                    Disabled
Set username from dhcp option 12                           Disabled
L2 Authentication Fail Through                             Disabled
Multiple Server Accounting                                 Disabled
User idle timeout                                          N/A
Max IPv4 for wireless user                                 2
RADIUS Accounting Server Group                             N/A
RADIUS Roaming Accounting                                  Disabled
RADIUS Interim Accounting                                  Disabled
RADIUS Acct-Session-Id In Access-Request                   Disabled
RFC 3576 server                                            N/A
User derivation rules                                      N/A
Wired to Wireless Roaming                                  Enabled
Reauthenticate wired user on VLAN change                   Disabled
Device Type Classification                                 Enabled
Enforce DHCP                                               Disabled
PAN Firewall Integration                                   Disabled
Open SSID radius accounting                                Disabled
Apply ageout mechanism on bridge mode wireless clients     Disabled
(MC1) [MDC] #
```

A network administrator has fully deployed a WPA3 based WLAN with 802.1X authentication. Later he defined corp-employee as the default user-role for the 802.1X authentication method in the aaa profile. When testing the setup he realizes the client gets the "guest" role.

What is the reason "corp-employee" user role was not assigned?

Options:

A- The administrator forgot to map a dotlx profile to the corp-employee aaa profile.

B- The administrator forgot to enable PEFNG feature set on the Mobility Master.

C- MC 1 has not received the configuration from the mobility master yet.

D- The Mobility Master lacks MM-VA licenses; therefore, it shares partial configuration only.

Answer:

C

Question 4

Question Type: **MultipleChoice**

A company with 535 users deploys an Aruba solution with more than 1000 Aruba APs, two 7220 Mobility Controllers, and a single Mobility Master (MM) virtual appliance at the campus server farm. The MCs run a HA Fast failover group in dual mode and operate at 50% AP capacity.

If there is an MM or MC failure, the network administrator must ensure that the network is fully manageable and the MC load does not exceed 80%.

What can the network administrator do to meet these requirements?

Options:

A- Place the APs in the same hierarchy level.

B- Create a cluster with AP load balancing.

C- Enable oversubscription in the HA group.

D- Add an MC and an MM in the server farm.

E- Add an MM and enable DC redundancy.

F- Place the APs in two different AP-Groups.

Answer:

E

Question 5

Question Type: MultipleChoice

Users run Skype for Business on wireless clients with no WMM support over an Aruba Mobility Master (MM) - Mobility Controller (MC) based network. When traffic arrives at the wired network, it does not include either L2 or L3 markings.

Which configuration steps should the network administrator take to classify and mark voice and video traffic with UCC heuristics mode?

Options:

A- Enable WMM in a VAP profile, and explicitly permit voice and video UDP ports in a firewall policy.

B- Confirm OpenFlow is enabled in the user role and VAP profile. Then enable WMM in a SSID profile, and explicitly permit voice and video UDP ports in a firewall policy.

C- Confirm the MC is the Openflow controller of the MMs and Openflow is enabled in VAP and firewall roles. Enable Skype4Business ALG in UCC profiles.

D- Confirm MM is the Openflow controller of MCs and Openflow is enabled in VAP and firewall roles. Enable Skype4Business ALG in UCC profiles.

Answer:

A

Question 6

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
----  -----    -------  ----------    ------   -----  ----------    ----------
AP21  CAMPUS   355      10.1.145.150  Down            10.254.13.14  0.0.0.0
AP22  CAMPUS   355      10.1.146.150  Up 7m:4s IL     10.254.13.14  0.0.0.0


Total Aps:2
(MC11) [mynode] #show version | include Aruba

Aruba Operating System Software.
Aruba05 (MODEL: ArubaMC-VA-US), Version 8/2/1/0
(MC11) [mynode] #
(MC11) [mynode] #show log system 5| include "license"
Jun 21 12:20:25 :399814: <5481> <DBUG> |cfgn| Config Manager is not ready to send the new license config to the applications yet
Jun 21 12:29:34 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP xx:xx:xx:xx:xx:xx
Jun 21 12:29:38 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP xx:xx:xx:xx:xx:xx
Jun 21 12:34:42 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP AP22
Jun 21 12:34:46 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP AP22
(MC11) [mynode] #
(MC11) [mynode] #show license aggregate

Aggregate License Table for pool /
----------------------------------
Hostname     IP Address   Mac addr           AP   REF  RF Protect  ACR  WebCC  MM  MC-VA-RW  MC-VA-EG  MC-VA-IL  MC-VA-JP  MC-VA-US  VIA
 Last update (secs. ago)
--------     ----------   --------           ---- ---- ----------  ---- -----  --- --------- --------  --------  --------  --------  ---
 ----------------------
From Server  10.254.13.14 yy:yy:yy:yy:yy:yy  16   0    0           0    0      0   0         0         0         0         0         0


Total no. of clients: 0
```

A network administrator deploys a standalone Mobility Controller (MC) and configures some VAPs within the CAMPUS AP group. The network administrator realizes that none of the VAPs are being broadcasted.

Based on the output shown in the exhibit, what should the network administrator do to solve this problem?

Options:

A- Install MC-VA licenses, then install PEF licenses and enabled the PEF feature.

B- Install MC-VA licenses, then reprovision the APs.

C- Install MM licenses, then install PEF licenses and enable the PEF feature.

D- Install MM licenses and install MC-VA licenses, then install RFP licenses.

Answer:

D

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

```
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


User Anchor Controller(UAC): 10.1.224.100

User                Port    State                              Bucket ID   Gre Key
-------------------------------------------------------------------------------
xx:xx:xx:xx:yy:yy   1/1/20 registered                          255         20
Access-1#
```

Based on the output shown in the exhibit, with which Aruba devices has Access-1 established tunnels?

Options:

A- a pair of standalone MCs

B- a pair of switches running VXLAN

C- a pair of MCs within a L3 cluster

D- a single standalone MC

Answer:

C

Question 8

Question Type: **MultipleChoice**

Refer to the exhibit.

```
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=
 fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass:10.254.1.23:1812 id:45, len:26
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  User-Name: contractor12
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-IP-Address: 10.254.13.14
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Id: 0
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Identifier: 10.254.13.14
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Type: Wireless-IEEE802.11
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Calling-Station-Id: 608E9A910FT8
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Called-Station-Id: 44646807DE4G
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Service-Type: Framed User
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Framed MTU: 1100
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  EAP-Message: \002\012
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  State: AGcATgBnAKj9IQQAkgYQj1ulavmnP5/OVna0PQ==
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Essid-Name: EmployeesNet
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Location-Id: AP22
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-AP-Group: CAMPUS
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2381]  Aruba-Device-Type: (VSA with invalid length - Don't send it)
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Message-Auth: \487e\326\445\540\318/f\789\416\110\874\4482\612
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:95]  Find Request: id=45, server=(null), IP=10.254.1.23, server-group=(n
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null),
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:48]  Del Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=
fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1228] Authentication Successful
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Aruba} Aruba-User-Role: contractor
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Microsoft} MS-MPPE-Recv-Key: \640\510\973>J\644\238n\421\789\252
\0551\898h\354\519\733Fe0\450\739(\456\152="c\217bR\794\777\649\147\682\400\118\493y\452\731(
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Microsoft} MS-MPPE-Send-Key: \641\486\489\011\605\784\064h\027\38
884 \375o\446 \398\453
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  EAP-Message: \003\012
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Message-Auth: z\498XS\330\480\512\383\498\711
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  User-Name: contractor12
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Class: \202\005\456)\123\789C\056\2578#\876\041\579"\656\741\081
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RADIUS_ID: -
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Rad-Length: 250
Jun 23 21:28:17 :124031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RADIUS_CODE: \002
Jun 23 21:28:17 :124031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RAD_AUTHENTICATOR: PN\495\591\685$\211\481\982G\363RD\261\696\
Jun 23 21:28:17 :124003:  <5533> <INFO> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass, user=
xx:xx:xx
```

A network administrator wants to allow contractors to access the WLAN named EmployeesNet. In order to restrict network access, the network administrator wants to assign this category of users to the contractor user role. To do this, the network administrator configures

ClearPass in a way that it returns the Aruba-User-Role with the contractor value.

When testing the solution, the network administrator receives the wrong role.

What should the network administrator do to assign the contractor role to contractor users without affecting any other role assignment?

Options:

A- Check the Download role from the CPPM option in the AAA profile.

B- Set contractor as the default role in the AAA profile.

C- Create Contractor firewall role in the M.

D- Create server deviation rules in the server group.

Answer:

A

Question 9

Question Type: **MultipleChoice**

A network administrator has deployed an Airwave Management Platform (AMP) server and integrated it with a Mobility Master (MM) -- Mobility Controller (MC) based WLAN. The AMP server already has all Aruba Mobility devices including Access Points (APs) in the "UP" devices list.

What are two actions the administrator can execute upon the APs under "Airwave>Devices>Monitor"? (Choose two.)

Options:

A- Open the WebUI of the MC where the AP terminates.

B- Re-provision the Access Point.

C- Disable and change the mode of the AP's radios.

D- Invoke MC's show commands for that Access Point.

E- Run Spectrum Analysis locally.

Answer:

D, E