HPE6-A79 Q&As

Aruba Certified Mobility Expert Written Exam

Pass HP HPE6-A79 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/hpe6-a79.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

A fully functional WLAN is deployed in a campus network using the following script.

```
aaa server-group group-corp
 auth-server radius1

aaa profile aaa-corp
   authentication-dot1x authenticated
   dot1x-server-group group-corp
!
wlan ssid-profile ssid-corp
   essid corp
   opmode wpa2-aes
!
wlan virtual-ap vap-corp
   aaa-profile aaa-corp
   vlan 20
   ssid-profile ssid-corp
!
ap-group building1
   virtual-ap vap-corp
```

Which part of the script can a network administrator re-use to assign a different default role to users when they connect to the same SSID in a second building?

A. server group and ssid profile

B. server group and VAP profile

C. server group, aaa profile, and ssid profile

D. server group and VAP

Correct Answer: A

QUESTION 2

A network administrator has updated the ArubaOS code of a standalone Mobility Controller (MC) that is used for User-Based Tunneling (UBT) to a newer early release. Ever since the MC seems to reject PAPI sessions from the switch with the 10.1.10.10 IP address. Also the controller\\'s prompt is now followed by a star mark: "(MC_VA) [mynode] *#"

When opening a support ticket, an Aruba TAC engineer asks the administrator to gather the crash logs and if possible replicate UBT connection attempts from the switch while running packet captures of PAPI traffic on the controller and obtain the PCAP files. The administrator has a PC with Wireshark and TFTP server using the 10.0.20.20 IP address.

What commands must the administrator issue to accomplish these requests? (Choose two.)

A.
```
packet-capture destination ip-address 10.0.20.20
packet-capture datapath ipsec 10.1.10.10
```

B.
```
show tech-support logs.tar
copy flash: logs.tar tftp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tftp: 10.0.20.20 logs.tar_md5sum.txt
```

C.
```
tar logs
copy flash: logs.tar tftp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tftp: 10.0.20.20 logs.tar_md5sum.txt
```

D.
```
tar crash
copy flash: logs.tar tftp: 10.0.20.20 crash.tar
copy flash: logstarmd5sum.txt tftp: 10.0.20.20 crash.tarmd5sum.txt
```

E.
```
packet-capture destination ip-address 10.0.20.20
packet-capture controlpath udp all
```

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Correct Answer: BE

QUESTION 3

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?

A. The administrator forgot to map a dot1x 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.

Correct Answer: C

QUESTION 4

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?

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.

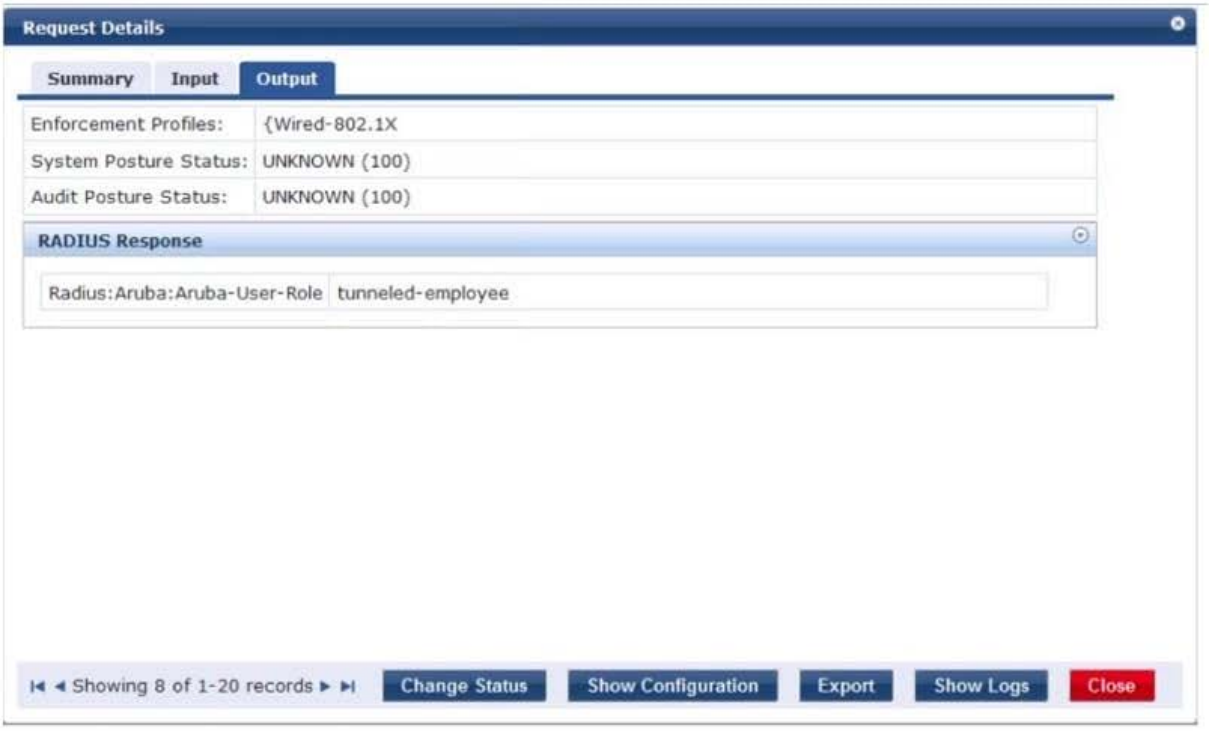
C. Confirm the MC is the Openflow controller of the MMs and Openflow is enabled in VAP and firewall roles. Enable Skype4Business ALG in UCC profiles.

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

Correct Answer: A

QUESTION 5

Refer to the exhibits.




```
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?

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.

Correct Answer: B