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.passapply.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 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 tffp: 10.0.20.20 logs.tar
copy flash: logs.tar_md5sum.txt tffp: 10.0.20.20 logs.tar_md5sum.txt
```

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

D.
```
tar crash
copy flash: logs.tar tffp: 10.0.20.20 crash.tar
copy flash: logstarmd5sum.txt tffp: 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 2

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-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   -    204c0306e790000000170008
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
```

Based on the output shown in the exhibit, which wireless connection phase has just completed?

A. L3 authentication and encryption

B. MAC Authentication and 4-way handshake

C. 802.11 enhanced open association

D. L2 authentication and encryption

Correct Answer: A

QUESTION 3

A company plans to build a resort that includes a hotel with 1610 rooms, a casino, and a convention center. The company is interested in a mobility solution that provides scalability and a service-based approach, where they can rent the

WLAN infrastructure at the convention center to any customer (tenant) that hosts events at the resort.

The solution should provide:

Seamless roaming when users move from the hotel to the casino or the convention center

Simultaneous propagation of the resort and customer-owned SSIDs at the convention center

Null management access upon resort network infrastructure to the customers (tenants)

Configuration and monitor rights of rented SSIDs to the customers (tenants)

Which deployment meets the requirements?

A. Deploy an MM-MC infrastructure with multizone AP\\'s, with one zone for tenant SSIDs.

B. Deploy IAPs along with AirWave, and deploy role-based management access control.

C. Deploy IAPs with zone based SSIDs and manage them with different central accounts.

D. Deploy an MM-MC infrastructure, and create different hierarchy groups for MCs and APs.

E. Deploy IAPs, and manage them with different central accounts.

Correct Answer: E

QUESTION 4

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.

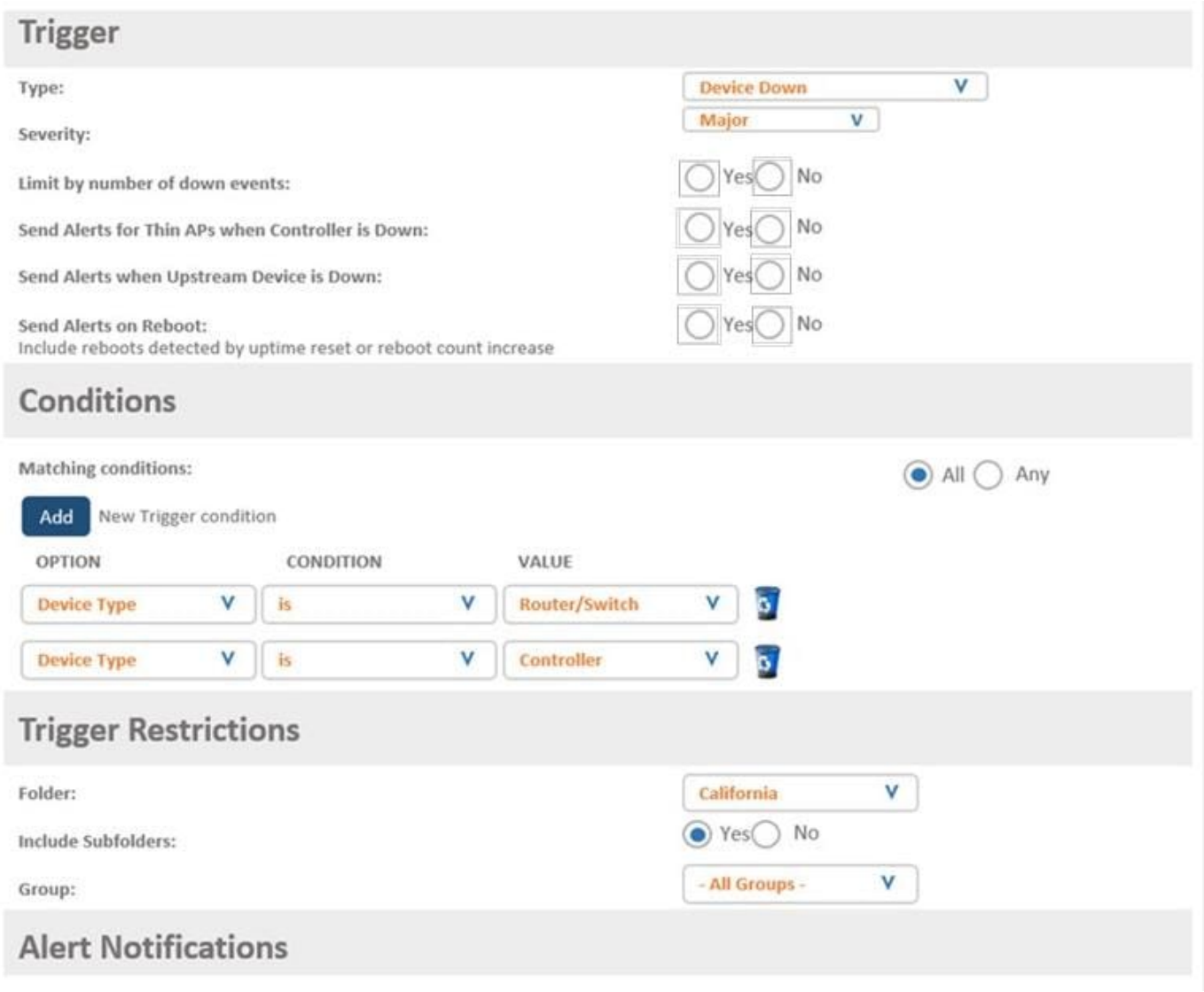
Correct Answer: C

QUESTION 5

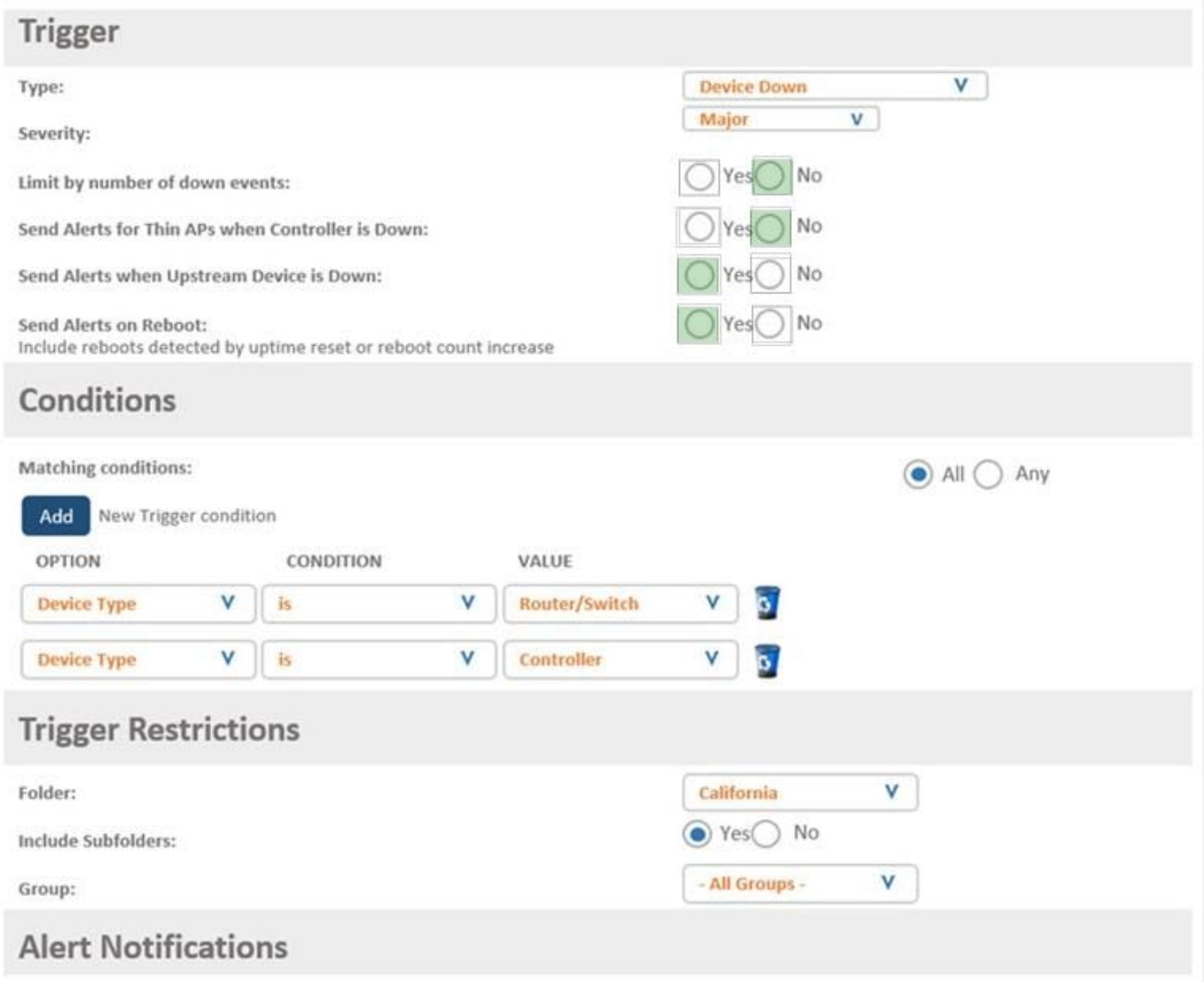
HOTSPOT

A network administrator wants to receive a major alarm every time a controller or an Aruba switch goes down for either a local or an upstream device failure. Which alarm definition must the network administrator create to accomplish this?

Hot Area:



Correct Answer:



[HPE6-A79 PDF Dumps](#) [HPE6-A79 Study Guide](#) [HPE6-A79 Braindumps](#)