DUMPSQUEEN

Aruba Certified Mobility Expert Written Exam

HP HPE6-A79

Version Demo

Total Demo Questions: 10

Total Premium Questions: 55

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

A network administrator assists with the migration of a WLAN from a third-party vendor to Aruba in different locations throughout the country. In order to manage the solution from a central point, the network administrator decides to deploy redundant Mobility Masters (MMs) in a datacenter that are reachable through the Internet.

Since not all locations own public IP addresses, the security team is not able to configure strict firewall polices at the datacenter without disrupting some MM to Mobility Controller (MC) communications.

They are also concerned about exposing the MMs to unauthorized inbound connection attempts.

What should the network administrator do to ensure the solution is functional and secure?

A. Deploy an MC at the datacenter as a VPN concentrator.

B. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.

C. Block all ports to the MMs except UDP 500 and 4500.

D. Install a PEFV license, and configure firewall policies that protect the MM.

ANSWER: C

QUESTION NO: 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 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

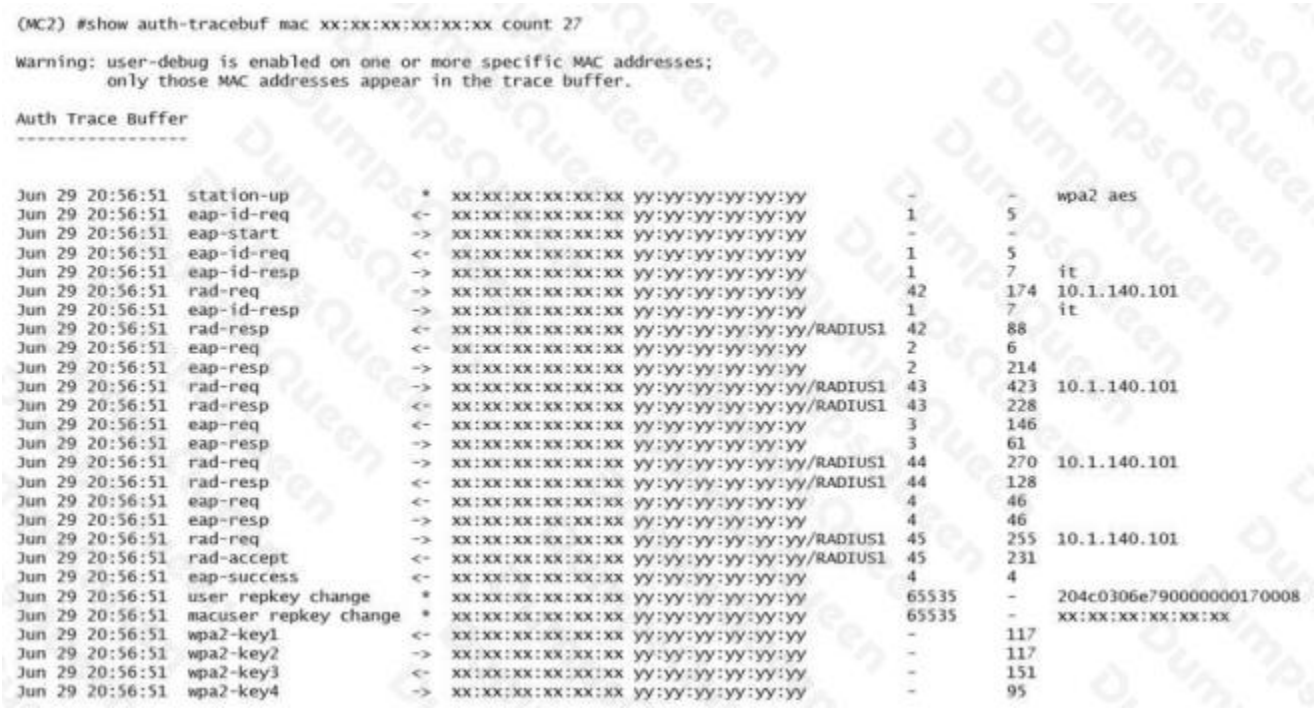
D. Option D

E. Option E

ANSWER: B E

QUESTION NO: 3

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

ANSWER: A

QUESTION NO: 4

An organization owns a fully functional multi-controller Aruba network with a Virtual Mobility Master (VMM) in VLAN20. They have asked a network consultant to deploy a redundant MM on a different server. The solution must offer the lowest convergence time and require no human interaction in case of failure.

The servers host other virtual machines and are connected to different switches that implement ACLs to protect them. The organization grants the network consultant access to the servers only, and appoints a network administrator to assist with the deployment.

What must the network administrator do so the network consultant can successfully deploy the solution? (Choose two.)

A. Allocate VLAN20 to the second server, and extend it throughout the switches, then reserve one IP address for the second MM and another IP address for its gateway.

B. Allocate VLAN20 to the second server, and permit routing between them, then reserve one IP address for the second MM and another IP address for its gateway.

C. Configure an ACL entry that permits IP protocol 50, UDP port 500, and multicast IP 224.0.0.18.

D. Allocate VLAN20 to the second server, and extend it throughout the switches, then reserve one IP address for the second MM and another for the VIP.

E. Configure an ACL entry that permits UDP 500, TCP 4500, and multicast IP 224.0.0.5.

ANSWER: A E

QUESTION NO: 5

Refer to the exhibits.

Exhibit 1

```
(MC2) [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/Phy
      Profile  Forward mode Type     Host Name   User Type
---------   ----------          -----   ----                 --------- ----   -------- -------- -------- ---------------
      -------      -------------      -----  --------   --------
192.168.14.101  xx:xx:xx:xx:xx:xx          guest-guest-logon     00:00:32                  AP1       Wireless  Guest/yy:yy:yy:yy:yy:yy/a-
VHT  Guest    tunnel        Win 10            WIRELESS

User Entries: 1/1
  Curr/Cum Alloc:2/5 Free:0/3 DVN:2 AllocErr:0 FreeErr:0
```

Exhibit 2

```
(MC2) [MDC] #show rights guest-guest-logon

Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'guest-guest-logon'
  Up BW:No Limit   Down BW:No Limit
  L2TP Pool = default-l2tp-pool
  PPTP Pool = default-pptp-pool
  Number of users referencing it = 2
  Periodic reauthentication: Disabled
  DPI Classification: Enabled
  Youtube education: Disabled
  Web Content Classification: Enabled
  IP-Classification Enforcement: Enabled
  ACL Number = 98/0
  Openflow: Enabled
  MaxSessions = 65535

  Check CP Profile for Accounting = TRUE
  Captive Portal profile = default
```

Exhibit 3

```
(MC2) [MDC] #show aaa authentication captive-portal Guest

Captive Portal Authentication Profile "Guest"
---------------------------------------------
Parameter                                   Value
---------                                   -----
Default Role                                guest
Default Guest Role                          guest
Server Group                                Guest
Redirect Pause                              10 sec
User Login                                  Enabled
Guest Login                                 Disabled
Logout popup window                         Enabled
Use HTTP for authentication                 Disabled
Logon wait minimum wait                     5 sec
Logon wait maximum wait                     10 sec
Logon wait CPU utilization threshold        60%
Max Authentication failures                 0
Show FQDN                                   Disabled
Authentication Protocol                     PAP
Login page                                  https://cp.mycompany.com/guest/web_login.php
Welcome page                                /auth/welcome.html
Show Welcome Page                           Yes
```

Exhibit 4

```
(MC2) [MDC] #show aaa authentication captive-portal default

Captive Portal Authentication Profile "default"
-----------------------------------------------
Parameter                                   Value
---------                                   -----
Default Role                                guest
Default Guest Role                          guest
Server Group                                Guest
Redirect Pause                              10 sec
User Login                                  Enabled
Guest Login                                 Disabled
Logout popup window                         Enabled
Use HTTP for authentication                 Disabled
Logon wait minimum wait                     5 sec
Logon wait maximum wait                     10 sec
Logon wait CPU utilization threshold        60%
Max Authentication failures                 0
Show FQDN                                   Disabled
Authentication Protocol                     PAP
Login page                                  /auth/index.html
Welcome page                                /auth/welcome.html
Show Welcome Page                           Yes
Add switch IP addresses in the redirection URL    Disabled

(MC2) [MDC] #show aaa server-group default

Fail Through: No
Load Balance: No

Auth Servers
------------
Name        Server-Type    trim-FQDN   Match-Type  Match-Op  Match-Str
----        -----------    ---------   ----------  --------  ---------
Internal    Internal       No

Role/VLAN derivation rules
--------------------------
Priority   Attribute   Operation   Operand   Type    Action    Value   Validated
--------   ---------   ---------   -------   ----    ------    -----   ---------
1          role        value-of              String  set role          No
```

A captive portal-based solution is deployed in a Mobility Master (MM) - Mobility Controller (MC) network. A wireless station connects to the network and attempts the authentication process. The outputs are shown in the exhibits.

Which names correlate with the authentication and captive portal servers?

A. ClearPass.23 is the authentication server, and cp.mycompany.com is the captive portal server.

B. ClearPass.23 is the authentication server, and MC2 is the captive portal server.

C. Internal database in MC2 is the authentication server, and cp.mycompany.com is the captive portal server.

D. cp.mycompany.com is the authentication server, and ClearPass.23 is the captive portal server.

ANSWER: A

QUESTION NO: 6

A software development company has 764 employees who work from home. The company also has small offices located in different cities throughout the world. During working hours, they use RAPs to connect to a datacenter to upload software code as well as interact with databases.

In the past two month, cabling issues have occurred connection to the 7240XM Mobility Controller (MC) that runs ArubaOS 8 and terminates the RAPs. These RAPs disconnect, affecting the users connected to the RAPs. This also causes problems with code uploads and database synchronizations. Therefore, the company decides to add a second 7240XM controller for redundancy.

How should the network administrator deploy both controllers in order to provide the redundancy while preventing failover events from disconnecting users?

A. Connect both controllers with common VLANs, and create an HA fast failover group with public addresses in the internet VLAN.

B. Connect both controllers with common VLANs, and create an L2-connected cluster using public addresses in the internet VLAN.

C. Connect both controllers with different VLANs, and create an L2-connected cluster using public addresses in the internet VLAN.

D. Connect both controllers with common VLANs, and configure LMS/BLMS values equal to public addresses in the internet VLAN.

ANSWER: A

QUESTION NO: 7

An organization has several RAPs at different locations that broadcast two SSIDs. The internet-only SSID is in bridge/always mode, and the corporate SSID is in split-tunneling/standard mode. The network administrator deploys 10 more RAPs in different locations.

Users can successfully connect to the corporate SSID that is propagated by a RAP at a remote location. However, they report that it takes too long to access public internet web sites.

What is one part of the configuration that should be checked by the network administrator to verify this RAP deployment?

A. User roles policies

B. IP pool

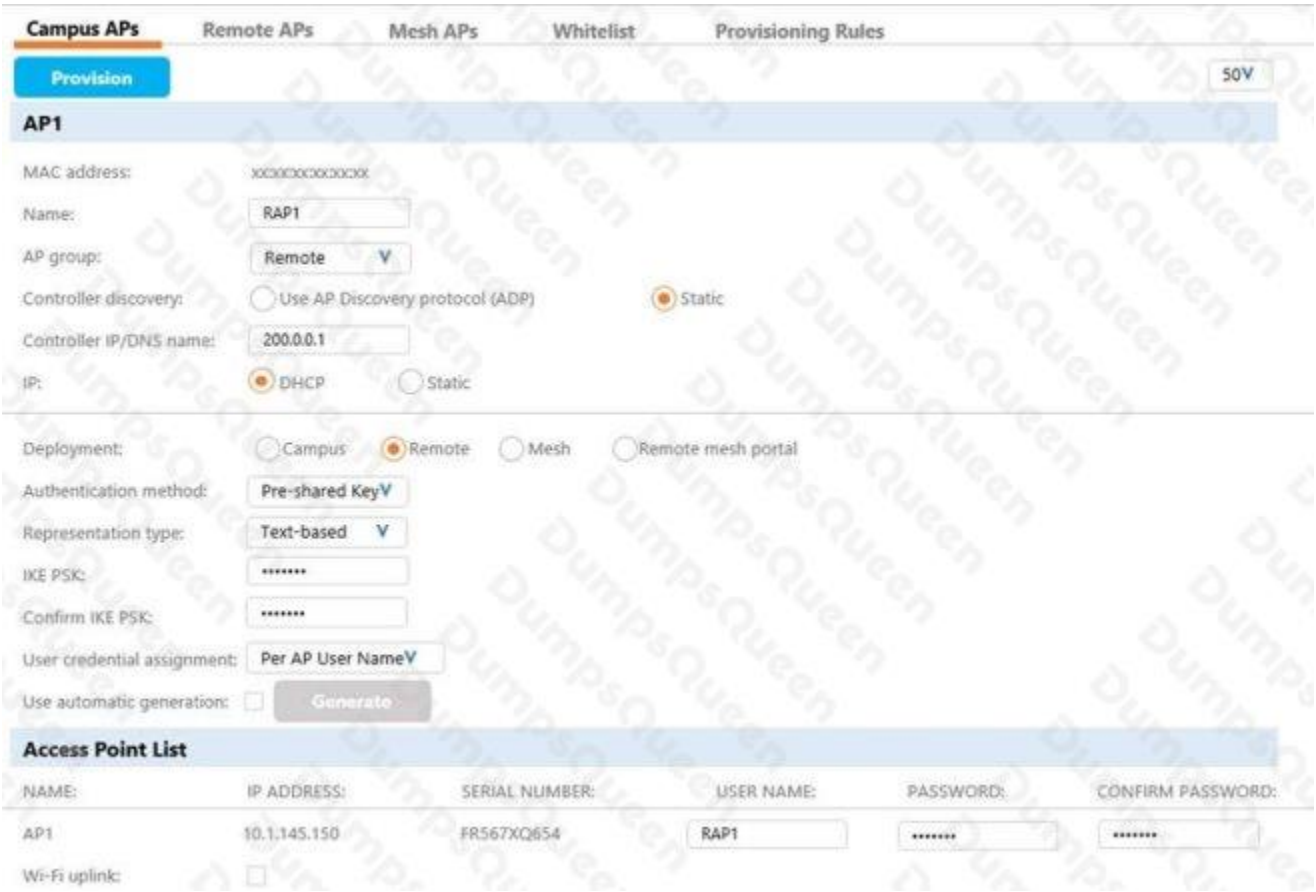
C. Operating mode

D. Assigned VLAN

ANSWER: A

QUESTION NO: 8

Refer to the exhibit.



A network administrator has a Mobility Master (MM) Mobility Controller (MC) architecture along with the MC in the DMZ for terminating RAPs. The network firewall has been provisioned to allow access to the MC in the DMZ for both UDP 500 and 4500. Then he proceeds to provision an AP as shown in the exhibit.

Which additional configuration steps must the administrator to assure RAPs successfully contact the MC? (Choose two.)

A. Create the RAP1 account in the InternalDB of the MC.

B. Create an IP local pool and PSK at the device node level.

C. Create the RAP1 account in the InternalDB of the MM.

D. Add the RAP1 entry in the CPsec whitelist at the MM level.

E. Create an IP local pool and PSK at the /mm/mynode level.

ANSWER: D E

QUESTION NO: 9

A network administrator is in charge of a Mobility Master (MM) – Mobility Controller (MC) based WLAN. The administrator has deployed an Airwave Management Platform (AMP) server in order to improve the monitoring capabilities and generate reports and alerts.

The administrator has configured SNMPv3 and Admin credentials on both the MMs and MCs and has created Groups and Folders in the AMP server. What two additional steps must the administrator do in order to let Airwave monitor the network devices? (Choose two.)

A. Manually add the Active MM and wait for automatic Discovery.

B. Map the AMP's IP address with a mgmt-config profile in the MM.

C. Set the AMP's IP address and Org string as DHCP option 43.

D. Manually add each MM, MC and Access Point in the AMP server.

E. Move "New" devices into a group and folder in Airwave.

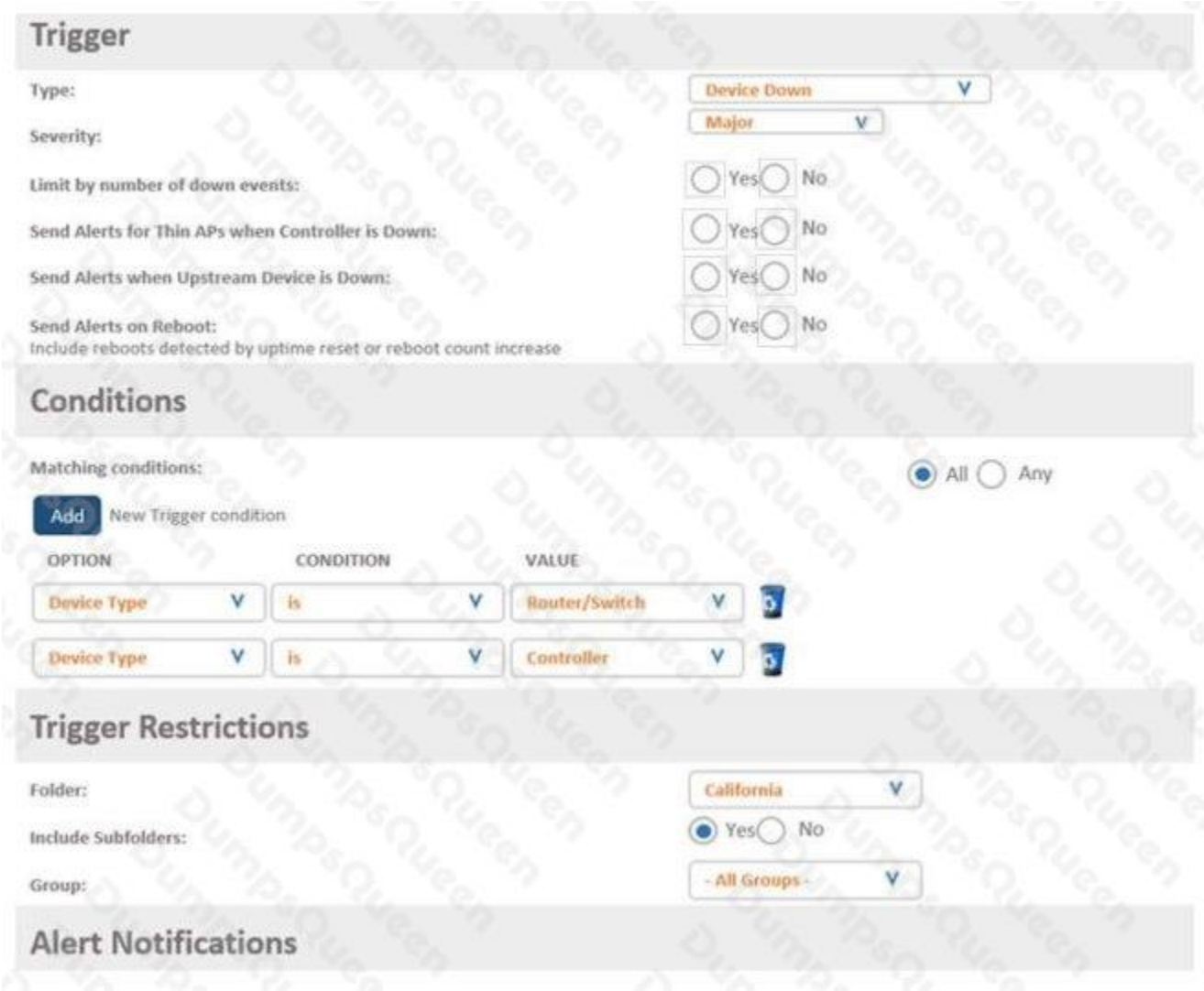
ANSWER: A B

QUESTION NO: 10 - (HOTSPOT)

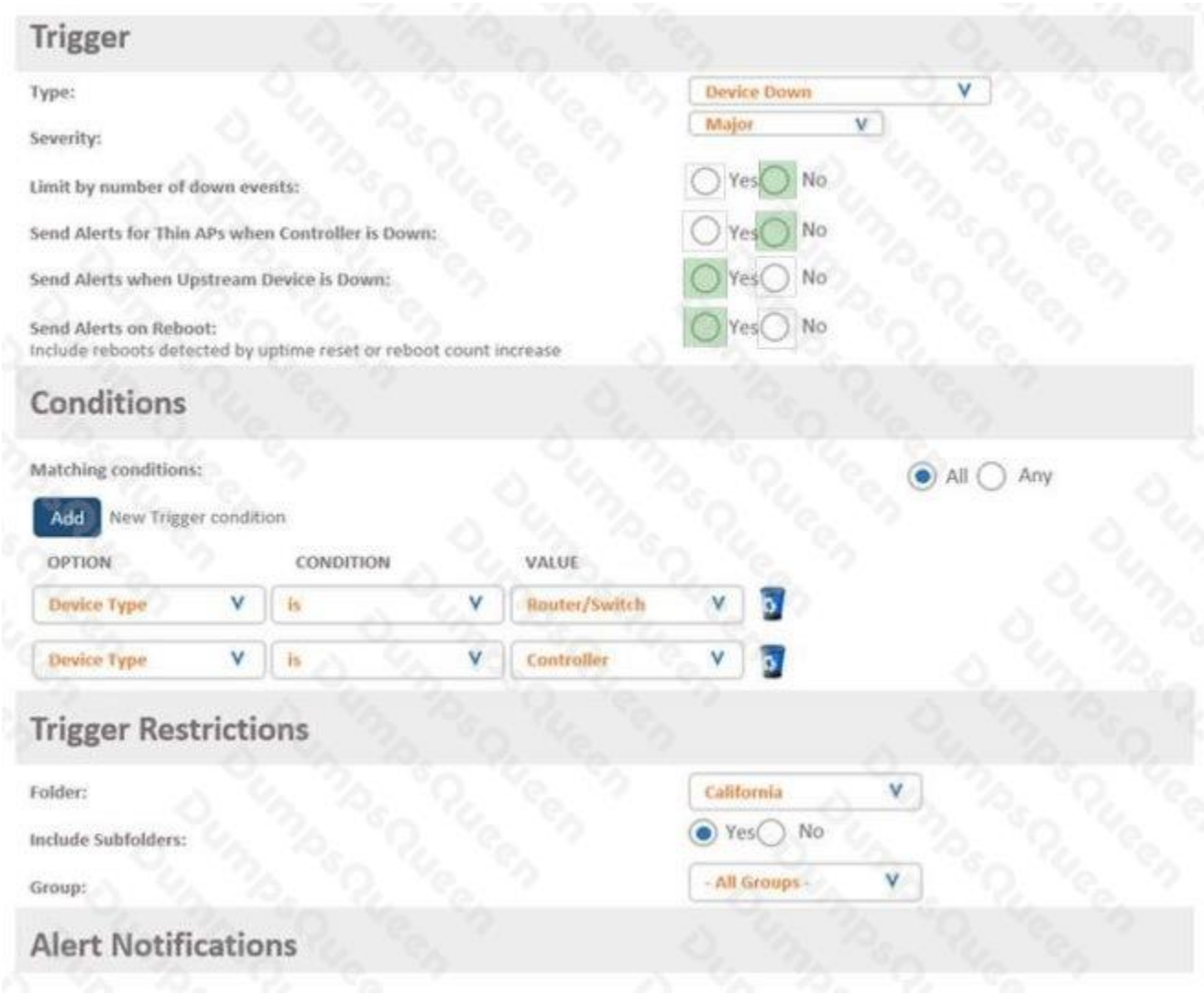
HOTSPOT

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:


Trigger
Type:
Device Down
Severity:
Major
Limit by number of down events:
Yes No
Send Alerts for Thin APs when Controller is Down:
Yes No
Send Alerts when Upstream Device is Down:
Yes No
Send Alerts on Reboot:
Include reboots detected by uptime reset or reboot count increase
Yes No
Conditions
Matching conditions:
All Any
Add
New Trigger condition
OPTION
CONDITION
VALUE
Device Type
is
Router/Switch
Device Type
is
Controller
Trigger Restrictions
Folder:
California
Include Subfolders:
Yes No
Group:
- All Groups -
Alert Notifications

ANSWER:



Explanation: