HPE6-A48 Q&As

Aruba Certified Mobility Expert 8 Written Exam

Pass HP HPE6-A48 Exam with 100% Guarantee

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

https://www.pass4itsure.com/hpe6-a48.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibits. Exhibit 1

```
(MM1) [mynode] #show switches

All Switches
-----------------
IP Address  Ipv6 Address  Name  Location  Type  Model  Version  Status  Configuration State  Config  Sync  Time (sec)
Config ID
--------------  -----------------  ---------  ------------  ------  ---------  ----------  --------  ----------------------------  ----------------------------------------
--------------
10.254.10.14  None  MM1  Building1.floor1  master  ArubaMM-VA  8.2.1.0_64044  up  UPDATE SUCCESSFUL  0
53
10.254.10.14  None  MC1  Building1.floor1  MD  Aruba7030  8.2.1.0_64044  up  CONFIG ROLLBACK  0
0
10.254.10.114  None  MM2  Building1.floor1  standby  ArubaMM-VA  8.2.1.0_64044  up  UPDATE SUCCESSFUL  0
53
Total Switches:3
(MM1) [mynode] #
(MM1) [mynode] #show switches
All Switches
-----------------
IP Address  Ipv6 Address  Name  Location  Type  Model  Version  Status  Configuration State  Config  Sync  Time (sec)
Config ID
--------------  -----------------  ---------  ------------  ------  ---------  ----------  --------  ----------------------------  ----------------------------------------
--------------
10.254.10.14  None  MM1  Building1.floor1  master  ArubaMM-VA  8.2.1.0_64044  up  UPDATE SUCCESSFUL  0
53
10.1.140.100  None  MC1  Building1.floor1  MD  Aruba7030  8.2.1.0_64044  down  CONFIG ROLLBACK  0
0
10.254.10.114  None  MM2  Building1.floor1  standby  ArubaMM-VA  8.2.1.0_64044  up  UPDATE SUCCESSFUL  0
53
Total Switches: 3
(MM1) [mynode] #
(MM1) [mynode] #encrypt disable
(MM1) [mynode] #show running-config | include localip
Building Configuration...
localip 10.1.140.101 ipsec Aruba123
localip 10.1.140.100 ipsec Aruba 123
localip 10.200.0.20 ipsec 1234567890
localip 10.1.140.102 ipsec Aruba123
(MM1) [mynode] #
(MM1) [mynode] #cd MC1
(MM1) [20:4c:03:06:e5:c0] #show configuration effective | include masterip
masterip 10.254.10.214 ipsec aruba123
        controller-ip "masterip" 6633
```

Exhibit 2 Exhibit 3

```
(MM1) [20:4c:03:06:e5:c0] #show log system 15

Jun 26 13:51:40 :357002: <6573> <WARN> |cfgdist| freelc_node:355 (TID:6573) Status of 10.1.140.100
(20:4c:03:06:e5:c0) is now DOWN
Jun 26 13:51:50 :357002: <6574> <WARN> |cfgdist| handle_read:702 (TID:6574) Status of ::ffff:10.1.140
(20:4c:03:06:e5:c0) is now UP
Jun 26 13:51:50 :371012: <5733> <ERRS> |profmgr| |multiversion| |Adding device 20:4c:03:06:e5:c0 with version
8_2_1_0]
Jun 26 13:52:10 :357002: <6574> <ERRS> |cfgdist| handle_setupconfig:452 (TID:6574) Setup config not received
from device for 10.1.149.100 (20:
4c:03:06:e5:c0) fd(146)
Jun 26 13:52:10 :357002: <6574> <WARN> |cfgdist| freelc_node:355 (TID:6574) Status of 10.1.140.100
(20:4c:03:06:e5:c0) is now DOWN
Jun 26 13:52:20 :357002: <6575> <WARN> |cfgdist| handle_read:702 (TID:6575) Status of ::ffff:10.1.140.100
(20:4c:03:06:e5:c0) is now UP
Jun 26 13:52:20 :371012: <5733> <ERRS> |profmgr| |multiversion| |Adding device 20:4c:03:06:e5:c0 with version
8_2_1_0]
Jun 26 13:52:40 :357002: <6575> <ERRS> |cfgdist| handle_setupconfig:452 (TID:6575) Setup config not received
from device for 10.1.149.100 (20:
4c:03:06:e5:c0) fd(146)
Jun 26 13:52:40 :357002: <6575> <WARN> |cfgdist| freelc_node:355 (TID:6575) Status of 10.1.140.100
(20:4c:03:06:e5:c0) is now DOWN
Jun 26 13:52:50 :357002: <6576> <WARN> |cfgdist| handle_read:702 (TID:6576) Status of ::ffff:10.1.140.100
(20:4c:03:06:e5:c0) is now UP
Jun 26 13:52:50 :371012: <5733> <ERRS> |profmgr| |multiversion| |Adding device 20:4c:03:06:e5:c0 with version 8
_2_1_0]
Jun 26 13:53:10 :357002: <6576> <ERRS> |cfgdist| handle_setupconfig:452 (TID:6576) Setup config not received
from device for 10.1.140.100 (20:
4c:03:06:e5:c0) fd(146)
Jun 26 13:53:10 :357002: <6576> <WARN> |cfgdist| freelc_node:355 (TID:6576) Status of 10.1.140.100
(20:4c:03:06:e5:c0) is now DOWN
Jun 26 13:53:20 :357002: <6577> <WARN> |cfgdist| handle_read:702 (TID:6577) Status of ::ffff:10.1.140.100
(20:4c:03:06:e5:c0) is now UP
Jun 26 13:53:20 :371012: <5733> <ERRS> |profmgr| |multiversion| |Adding device 20:4c:03:06:e5:c0 with version 8
_2_1_0]

(MM1) [20:4c:03:06:e5:c0] #
```

```
(MC1) #show switches

All Switches
-----------------
IP Address    IPv6 Address  Name Location          Type      Model      Version        Status  Configuration State  Config  Sync  Time (sec)  Confi
g ID
--------------  ------------------  --------  -------------  ---------  -----------  -------------  ----------  ------------------------------  -----------  --------  --------------  ---------
-------
10.1.140.100  None          MC1   Building1.floor1  MD        Aruba7030  8.2.1.0_64044  up      CONFIG ROLLBACK  0                                0

Total Switches:1
(MC1) #
(MC1)encrypt disable
(MC1) #show running-config | include masterip
Building Configuration . . .
masterip 10.254.10.214 ipsec Aruba123
(MC1) #
(MC1) #ping 10.254.10.214

Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 10.254.10.214, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.829/1.3608/1.777 ms

(MC1) #show log errorlog 10

Jun 26 13:57:50 <cfgm 399816>  <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 13:58:00 <cfgm 399816>  <3458> <ERRS> |cfgm| Rollback config id 53 as bad
Jun 26 13:58:20 <cfgm 399816>  <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 13:58:30 <cfgm 399816>  <3458> <ERRS> |cfgm| Rollback config id 53 as bad
Jun 26 13:58:50 <cfgm 399816>  <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 13:59:00 <cfgm 399816>  <3458> <ERRS> |cfgm| Rollback config id 53 as bad
Jun 26 13:59:20 <cfgm 399816>  <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 13:59:30 <cfgm 399816>  <3458> <ERRS> |cfgm| Rollback config id 53 as bad
Jun 26 13:59:50 <cfgm 399816>  <3458> <ERRS> |cfgm| handle_read: State(READY: CONFIG ROLLBACK:CFGID-0: PEND-0:INITCFGID:0) FD=27:
Failure receiving heartbeat response header information Result=0 Err=Success
Jun 26 14:00:00 <cfgm 399816>  <3458> <ERRS> |cfgm| Rollback config id 53 as bad
```

A network administrator deploys a Mobility Master (MM) pair with the VRRP VIP equal to 10.254.10.214, and attempts to associate MC1 to it. At first, the integration appears to be successful. However after a few minutes the network administrator issues the show switches command and sees that the MC1 is down, even though the device is up and running.

Every time the network administrator reboots the Mobility Controller (MC), the MC shows as being up and then it shows as being down. The network administrator gathers the information shown in the exhibits.

What should the network administrator do to resolve this problem?

A. Change the localip ipsec key to Aruba123 in the mynode device level from the MM, save, and reboot.

B. Enable disaster recovery mode in MC1 and change the masterip ipsec key to Aruba 123, save, and reboot.

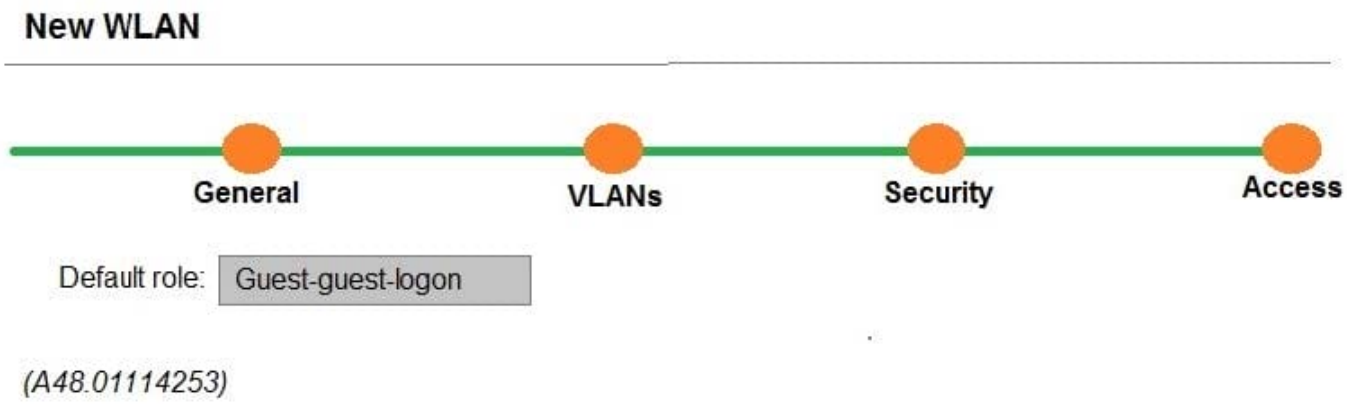
C. Change the masterip ipsec key to Aruba123 in the device level from the MM, save, then reboot MC1.

D. Wipe out the configuration in MC1 and reboot, then run the full-setup configuration dialog all over again.

Correct Answer: B

QUESTION 2

Refer to the exhibit.



A network administrator completes the task to cretae a WLAN, as shown in the exhibit. The network administrator selects the options to use guest as primary usage and Internal captive portal with authentication in the security step. Next, the network administrator creates a policy that denies access to the internal network.

Which additional step must the network administrator complete in order to prevent authenticated users from reaching internal corporate resources while allowing Internet access?

A. Apply the policy on the guest-guest-logon role.

B. Apply the policy on the authenticated role.

C. Apply the policy on the guest role.

D. Create a policy that permits dhcp, dns, and http access.

Correct Answer: D

QUESTION 3

A software development company has 700 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 months, brief failures have occurred in the 7240XM Mobility Controller (MC) that runs ArubaOS 8.3 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 redundancy while preventing failover events from disconnecting users?

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

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

C. Connect both controllers with different VLANs, and create an L2-connected cluster using private 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.

Correct Answer: A

QUESTION 4

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	DisScan	IPv4/6	Contract
1	user	any		app facebook	deny send-deny-response					Low						4
2	user	any		app youtube	deny send-deny-response					Low						4
1	user	any		app netflix	deny send-deny-response					Low						4

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, the 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 effecr over the contractor users?

A. Apply the policy in the contractors user role. Enable deep packet inspection.

B. Apply the policy in the contractors user role. Enable deep packet inspection. Reload the MCs.

C. Enable the firewall visibility. Enable web-content classification Reload the MCs.

D. Enable firewall visibility Enable web-content classification Reload the MMs.

Correct Answer: A

QUESTION 5

Refer to the exhibit.

```
(MM1) [md] #show switches

All Switches
---------------
```

IP Address	IPv6 Address	Name	Location	Type	Model	Version	Status	Configuration State	Config Sync Time (sec)	Config ID
10.254.10.14	None	MM1	Building1.floor1	master	ArubaMM-VA	8.2.1.0_64044	up	UPDATE SUCCESSFUL	0	415
10.254.10.114	None	MM2	Building1.floor1	standby	ArubaMM-VA	8.2.1.0_64044	up	UPDATE SUCCESSFUL	0	415
10.1.140.100	None	MC1	Building1.floor1	MD	Aruba7030	8.2.1.0_64044	up	UNK(20:4c:03:06:e5:c0)	N/A	N/A

```
Total Switches: 3
(MM1) [md] #
```

A network administrator adds a Mobility Controller (MC) in the /mm level and notices that the device does not show up in the managed networks hierarchy. The network administrator accesses the CLI, executes the show switches command, and obtains the output shown in the exhibit.

What is the reason that the MC does not appear as a managed device in the hierarchy?

A. The network administrator added the device using the wrong Pre=shared Key (PSK).

B. The digital certificate of the MC is not trusted by the MM.

C. The IP address of the MC does not match the one that was defined in the MM.

D. The network administrator has not moved the device into a group yet.

Correct Answer: B

QUESTION 6

A point venture between two companies results in a fully functional WLAN Aruba solution. The network administrator uses the following script to integrate the WLAN solution with two radius servers, radius1 and radius2.

```
aaa athentication-server radius radius1
  host 10.254.1.1
  key key111
!
aaa authentication-server radius radius2
  host 10.20.2.2
  key key222
!
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
ssid-profile ssid-corp
!
ap-group building1
virtual-ap vap-corp
```

While all users authenticate with username@doaminname.com type of credentials, radius1 has user accounts without the domain name portion.

Which additional configuration is required to authenticate corp1.com users with radius1 and corp2 users with radius2?

A. aaa authentication-server radius radius1 trim-fqdn ! aaa server-group-corp auth-server radius1 match-authstring corp1.com auth-server radius1 match-authstring corp2.com

B. aaa server-group-corp auth-server radius1 match-fqdn corp1.com auth-server radius1 trim-fqdn auth-server radius2 match-fqdn corp2.com

C. aaa authentication-server tadius radius1 ! aaa server-group-corp auth-server radius1 match-string corp1.com trim-fqdn auth-server radius1 match-string corp2.com

D. aaa authentication-server radius radius1 trim-fqdn ! aaa server-group-corp auth-server radius1 match-domain corp1.com auth-server radius1 match-domain corp2.com

Correct Answer: B

QUESTION 7

An airline wants to invest in an Aruba Mobility (MM)-Mobility Controller (MC) solution for the three hubs it has throughout the country. A single MM is located in the datacenter at one of the hubs. The MCs in the other two hubs reach the MM through a site-to-site IPSec VPN.

The operations team does not want to lose monitoring and configuration control of the MCs if something happens to the datacenter where the MM resides.

Which solution ensures that there is management access to the MCs in case of an MM failure due to a datacenter outage?

A. Deploy another MM in a different location, and enable L2 redundancy.

B. Install AirWave Management Platform, and enable Read and Write Management access on devices.

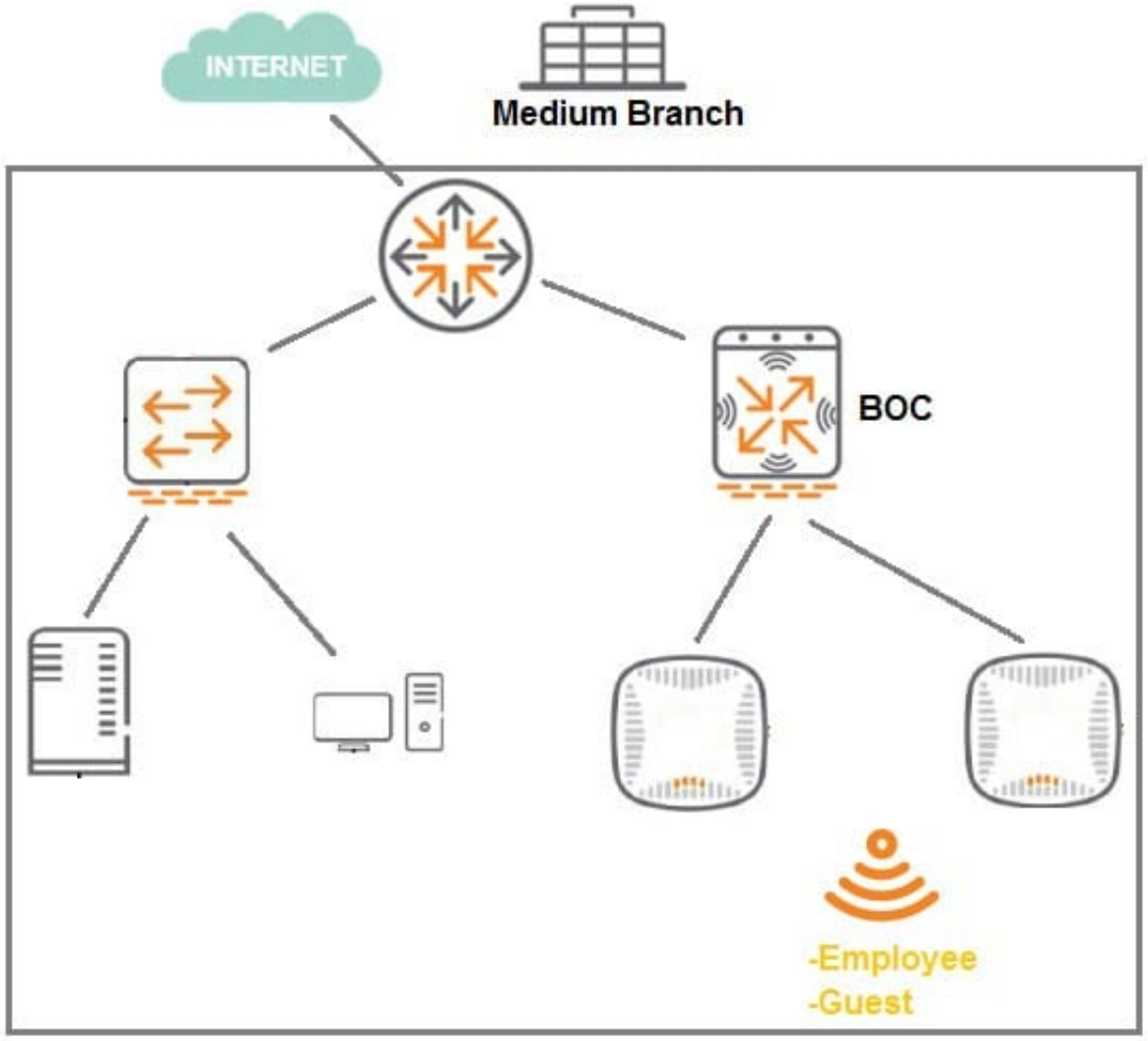
C. Deploy another MM in a different location, and enable L3 redundancy.

D. Deploy a local MM on each hub, and synchronize the configuration between all MMs.

Correct Answer: B

QUESTION 8

Refer to the exhibit.



A 7008 Branch Office Controller (BOC) is deployed in a remote office behind a core router. This core router does not support 802.1q encapsulation. The Mobility Controller (MC) is the gateway for two tunneling mode SSIDs, as shown in the exhibit.

Which two different configuration options ensure that wireless users are able to reach the branch network through the router? (Select two.)

A. Configure all ports of the BOC as access ports on the controller VLAN, and change the gateway of clients to the core router IP.

B. Configure the uplink of the BOC as an access port on the controller VLAN, and enable NAT for the SSID VLANs.

C. Configure the uplink of the BOC as a trunk port, tagging the controller and the SSID VLANs, and enable NAT for the SSID VLANs.

D. Configure the uplink of the BOC as an access port on the controller VLAN, and add static router in the router for the SSID VLAN subnets.

E. Configure the uplink of the BOC as a trunk port that permits the controller and the SSID VLANs. The controller VLAN must be native.

Correct Answer: BD

QUESTION 9

A company currently offers guest access with an open SSID and no authentication. A network administrator needs to integrate a web login page for visitors.

To accomplish this integration, the network administrator fully deploys a guest solution with self-registration in ClearPass, and defines the Mobility Controller (MC) as a RADIUS client. Then, the network administrator defines ClearPass as a RADIUS server and adds it into a server group in the MC.

Which two actions must the network administrator do next on the MC side to complete the deployment? (Select two.)

A. Associate the captive portal profile to the initial role

B. Define the web login URL and server group in a captive portal profile

C. Associate the captive portal profile to the VAP profile

D. Associate the captive portal to an AAA profile.

E. Define the web login URL in a captive portal profile and the server group in an AAA profile.

Correct Answer: BD

QUESTION 10

Refer to the exhibit.

```
(MM1) [mynode] #show airmatch debug history ap-name AP20

2 GHz radio mac 70:3a:0e:5b:0a:c0   ap name  AP20
```

Time of Change	Chan	Bandwidth	EIRP(dBm)	Mode	Source
2018-07-16 05:01:56	11->11	20-> 20	8.0-> 23.0	AP->AP	Solver
2018-07-16 05:01:48	6 ->11	20-> 20	8.0-> 8.0	AP ->AP	Solver
2018-07-15 13:26:13	11 -> 7	20-> 40	8.0-> 6.0	AP ->AP	Min Channel Bandwidth Change
2018-07-15 12:21:39	1 ->11	40-> 20	8.0-> 6.0	AP ->AP	Max Channel Bandwidth Change
2018-07-15 12:20:08	11 -> 1	20-> 40	8.0-> 6.0	AP ->AP	Min Channel Bandwidth Change
2018-07-15 12:18:47	7 ->11	40-> 20	8.0-> 6.0	AP ->AP	Max Channel Bandwidth Change
2018-07-15 11:47:26	11-> 7	20-> 40	8.0-> 6.0	AP ->AP	Min Channel Bandwidth Change

Help desk staff receive reports from users that there is inefficient wireless service in a location serviced by AP20, AP21, and AP22, and open a ticket. A few hours later, the users report that there is a drastic improvement in service. The staff still wants to determine the cause of the problem so the next day thay start monitoring the tasks.

They access the Mobility Master (MM), and obtain the output shown in the exhibit.

What could be the cause of the problem that the users reported?

A. AirMatch was running an initial incremental optimization.

B. An operator used AirMatch to manually freeze AP channel and power.

C. An operator manually assigned settings in the radio profile.

D. AirMatch was running a full on-demand optimization.

Correct Answer: B

QUESTION 11

A network administrator deploys APs with radios in Air Monitor mode and detects several APs and SSIDs that belong to stores next door. The Mobility Master (MM) classifies the APs and SSIDs as potential rogues. The network administrator wants to prevent the Air Monitor from applying countermeasures against these APs.

How can the network administrator accomplish this?

A. Select the BSSID and click reclassify, then select neighbor.

B. Run the Define WIP Policy task, and define the BSSIDs of the neighboring APs as interfering.

C. Select the BSSID and click reclassify, then select interfering.

D. Run the Define WIP Policy task, and define the BSSIDs of the neighboring APs as Authorized.

Correct Answer: A

QUESTION 12

Refer to the exhibit.

```
Access-1 (config) # show tunneled-node-server state

Local Master Server (LMS) State

LMS Type      IP Address      State      Capability   Role
Primary    :  10.1.140.100    Complete   Per User     Operational Primary
Secondary  :  10.1.140.101    Complete   Per User     Operational Secondary

Switch Anchor Controller (SAC) State
                IP Address     Mac Address      State
SAC          :  10.1.140.100   204c03-06e5c0    Registered
Standby-SAC  :  10.1.140.101   204c03-06e790    Registered

User Anchor Controller (UAC)  :  10.1.140.100
User            Port    VLAN    State       Bucket ID
005056-a5510b   20      143     Registered  255

User Anchor Controller (UAC) : 10.1.140.101
User            Port    VLAN    State       Backet ID
```

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

A. a pair of MCs within a cluster

B. a single standalone MC

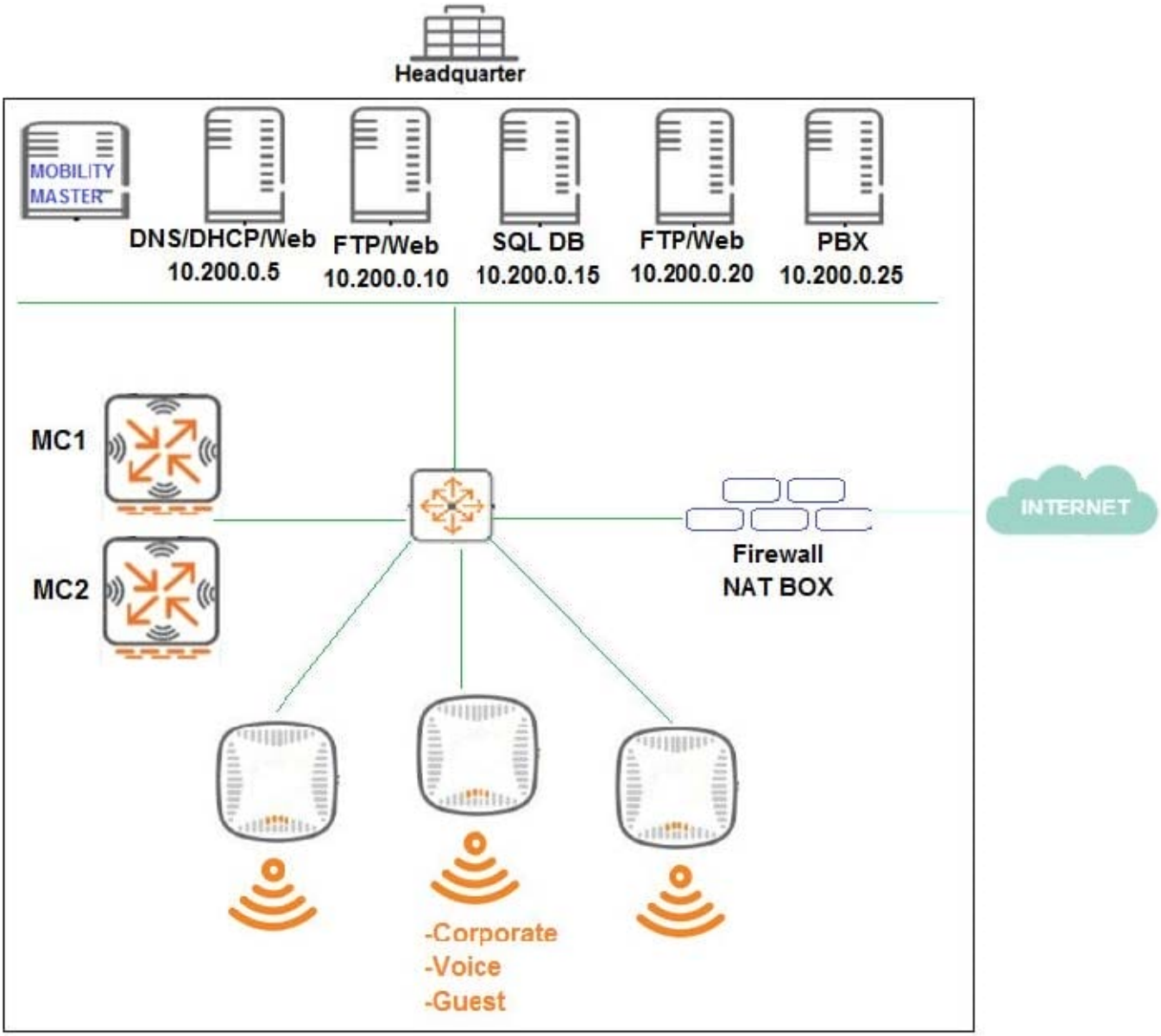
C. a pair of MCs with APFF enabled

D. a pair of switches

Correct Answer: B

QUESTION 13

Refer to the exhibit.



An organization provides WiFi access through a corporate SSID with an Aruba Mobility Master (MM)Mobility Controller (MC) network that includes PEF functions. The organization wants to have a single firewall policy configured and applied to the employee role.

This policy must allow users to reach Web, FTP, and DNS services, as shown in the exhibit. Other services should be exclusive to other roles. The client NICs should receive IP settings dynamically.

Which policy design meets the organization\\'s requirements while minimizing the number of policy rules?

A. netdestination alias1 host 10.200.0.10 host 10.200.0.20 ip access-list session policy1 user host 10.200.0.5 svc-dns permit user host 10.200.0.5 svc-http permit

user alias alias1 svc-http permit user alias alias1 svc-ftp permit

B. netdestination alias1 host 10.200.0.5 host 10.200.0.10 host 10.200.0.20 netdestination alias2 host 10.200.0.10 host 10.200.0.20 ip access-list session policy1 any any svc-dhcp permit user host 10.200.0.5 svc-dns permit user alias alias1 svc-http permit user alias alias2 svc-ftp permit

C. netdestination alias1 host 10.200.0.10 host 10.200.0.20 ip access-list session policy1 any any svc-dhcp permit user host 10.200.0.5 svc-dns permit user host 10.200.0.5 svc-http permit user alias alias1 svc-http permit user alias alias1 svc-ftp permit

D. netdestination alias1 host 10.200.0.5 host 10.200.0.10 host 10.200.0.20 netdestination alias2

Correct Answer: C

QUESTION 14

Refer to the exhibit.

```
(MC1) [MDC] #show ap debug multizone ap-name AP12

Multizone Table
---------------------
Zone  Configured IP     Serving IP      Max Vaps Allowed          Nodes   Flags
----- ----------------- --------------- ------------------------- ------- -----
0     10.1.140.100      10.1.140.100    4 (0-3)                   2       C2
1     10.254.10.114     10.254.10.114   2 (4-5)                   0
3     10.254.13.14      10.254.13.14    1 (6-6)                   1       2
4     10.2.100.25       10.2.100.25     4 (7-10)                  0

Flags: C = Cluster; L = Limited nodes; N = Nodes in other zones; 2 = Using IKE version 2; M = Image mismatch

Number of datazones:3
```

A network administrator deploys a multizone AP in the campus network in order to provide service for 11 SSIDs. After a few hours, the network administrator realizes that the AP is only broadcasting 5 out of the 11 SSIDs. The missing SSIDs belong to MC1 at IP address 10.254.10.114, and MC4 with IP address

10.2.100.25.

Based on the exhibit, what should the network administrator do next to fix this problem?

A. Confirm that AP12 is certified by the whitelist on MC1 and MC4, and confirm MC1 and MC4 are reachable by AP12.

B. Increase the number of nodes in zones 1 and 4, and confirm MC1 and MC4 are reachable by AP12.

C. Confirm that AP12 is certified by the whitelist on MC1 and MC4, and increase the number of nodes in zones 1 and 4.

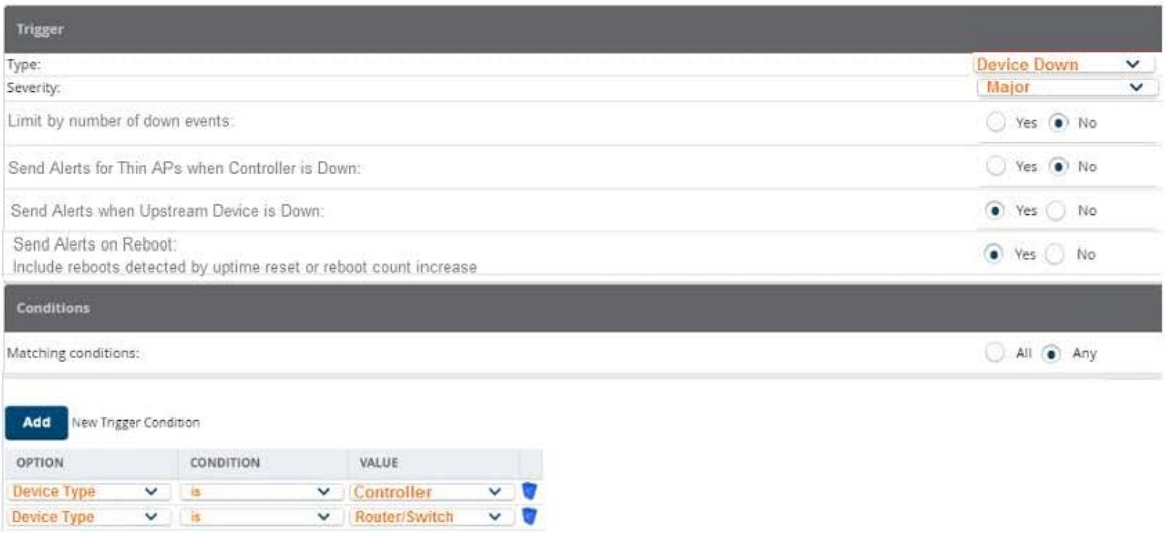
D. Reduce the number of nodes in zones 0 and 4, and disband the cluster in zone 0.

Correct Answer: D

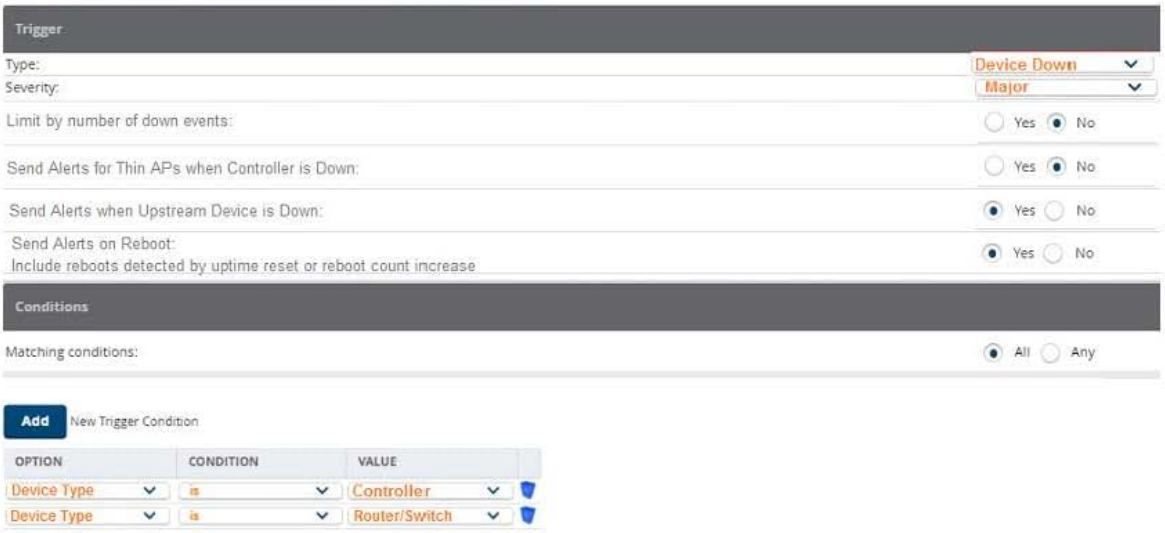
QUESTION 15

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?

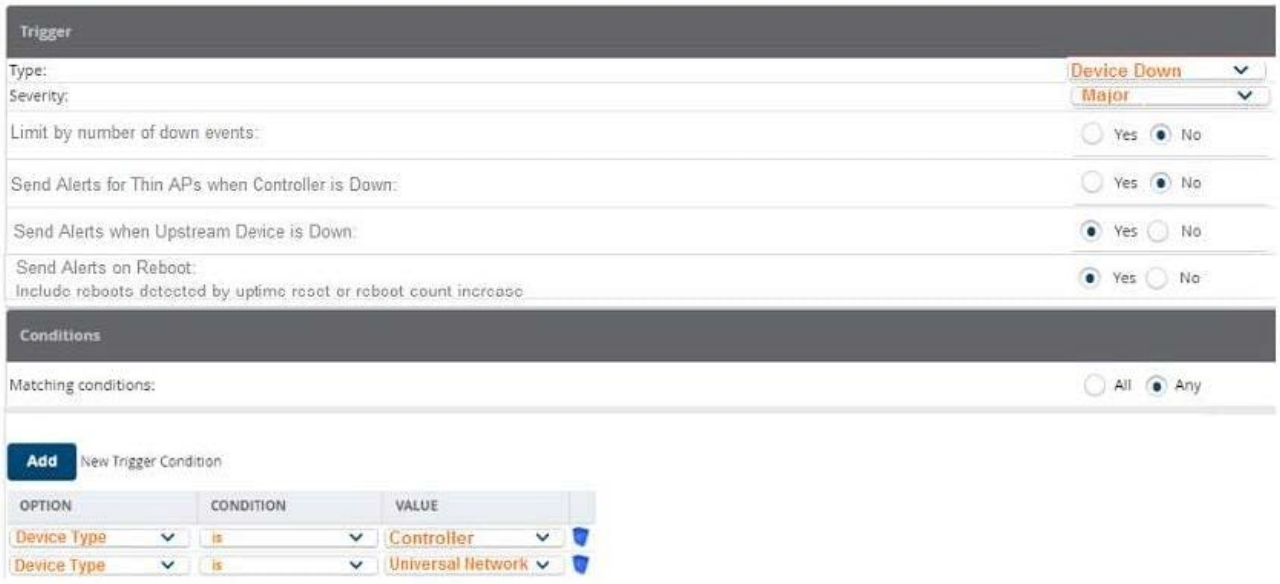
A.


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
Controller
Device Type
is
Router/Switch

B.


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
Controller
Device Type
is
Router/Switch

C.



A. Option A

B. Option B

C. Option C

Correct Answer: B