HPE6-A48.VCEplus.premium.exam.61q

Number: HPE6-A48
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

HPE6-A48

Aruba Certified Mobility Expert 8 Written Exam

Version 1.0

Exam A

QUESTION 1
A bank deploys an Aruba Mobility Master (MM)-Mobility Controller (MC) solution to provide wireless access for users that run different applications on their laptops, including SIP-based IP telephony. When users only run the IP telephony software, call quality is high. However, if users also run email, web, or mission critical applications, then voice quality drops.

Which feature would help improve the quality of voice calls over the air when users run different applications?

A. DSCP for IPv4 traffic
B. WiFi Multi Media
C. Type of Service
D. High/Low Queue

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A network administrator implements a SIP-based IP telephone solution. The objective is to ensure that APs use 100% of their airtime for network access whenever a voice call is taking place, to minimize communication delays. The network administrator also wants to ensure that a log entry is generated when voice calls occur.

Which setup accomplishes these tasks?

A. ip access-list session voice user any svc-rtsp
permit log queue high user any svc-sip-udp permit
log queue high B. ip access-list session voice user
any-svc-rtsp permit disable-scanning log user any
svc-sip-udp permit disable-scanning log C. ip
access-list session voice user any svc-rtsp permit
log dot1p-priority 7 user any svc-sip-udp permit
log dot1p-priority 7 D. ip access-list session
voice user any svc-rtsp permit log tos 56 user any
svc-sip-udp permit log tos 56

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4 Refer
to the exhibits.

Exhibit1

```
(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
*********   ************      ******   ****      **********  ****        ********  *******  *******   ***************                      *******       ************  ****
    ---------  ---------
10.1.141.150  70:4d:7b:10:0e:c6  it       guest     00:00:48    8021x-User            AP22     Wireless  Corp-employee/70:3a:0e:5b:0a:d2/a-VHT  Corp-Network  tunnel        Win
10            WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:3/39 Free:0/36 Dyn:3 AllocErr:0 FreeErr:0
(MC2) [MDC] #
(MC2) [MDC] #show user ip 10.1.141.150 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: guest (how: ROLE_DERIVATION_DOT1X), ACL: 7/0
Role: Derivation: ROLE_DERIVATION_DOT1X
(MC2) [MDC] #
```

Exhibit2

```
(MC2) [MDC] #show log security
Jul 4 17: 32:15  :124004:  <3553>  <DBUG>  |authmgr|  Select server method=802.1x,
user=it, essid=Corp-employee, server-group=Corp-Network, last_srv <>
Jul 4 17: 32:15  :124004:  <3553>  <INFO>  |authmgr|  Reused server ClearPass. 23 for
method=802.1x; user=it, essid=Corp-employee, domain=<>, server-group=Corp-Network
Jul 4 17: 32:15  :124004:  <3553>  <DBUG>  |authmgr|  aal_auth_raw (1402) (INC) : os_reqs
1, s ClearPass.23 type 2 inservice 1 markedD 0
Jul 4 17: 32:15  :124004:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c:152] Radius
authenticate raw using server ClearPass.23
Jul 4 17: 32:15  :124004:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_request.c:67] Add
Request: id=22, server=ClearPass.23, IP=10.254.1.23, server-group=Corp.Network, fd=64
Jul 4 17: 32:15  :124004:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2367] Sending
radius request to ClearPass.23:10.254.1.23:1812 id:22, len:265
Jul 4 17: 32:15  :124038:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] User Name:
it
Jul 4 17: 32:15  :124004:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] NAS-IP-
Address: 10.254.10.214
Jul 4 17: 32:15  :121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] NAS-Port-
Id: 0
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] NAS-
Identifier: 10.1.140.101
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] NAS-Port-
Type: Wireless-IEEE802.11
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Calling-
Station-Id: 704D7B109EC6
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Called-
Station-Id: 204C0306E790
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Service-
Type: Framed-User
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Framed-MTU:
1100
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] EAP-Message:
\002\011
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] State:
AFMAzwACACAG9gIAfv0RnQM2udKK13smu/l2DA==
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Aruba-Essid-
Name: Corp-employee
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Aruba-
Location-Id: AP22
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Aruba-AP-
Group: CAMPUS
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Aruba-
Device-Type: Win 10
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_server.c:2383] Message-
Auth: d\277\251\272\264fwh\314'\264z\034P\345\311
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_request.c: 95] Find
Request: id=22, server=(null), IP=10.254.1.23, server-group=(null) fd=64
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_request.c: 104]
Current entry: server= (null), IP=10.254.1.23, server-group=(null), fd=64
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_request.c: 48] Del
Request: id=22, server=ClearPass.23, IP=10.254.1.23, server-group=Corp-Network fd=64
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c: 1228]
Authentication Successful
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c: 1230] RADIUS
RESPONSE ATTRIBUTES
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c: 1245]
Filter-Id: it-role
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c: 1245]
{Microsoft} MS-MPPE-Recv-Key: \222\331\207\347\242[0*;\255g$\262\276u\302\205\264^"
\207\271Q\270E\3120<\2
04R\370\011\317$\007\275\203\302: \201\360\002\307B\305\222\032\240\317\340
Jul 4 17: 32:15  : 121031:  <3553>  <DBUG>  |authmgr|  |aaa| [rc_api.c: 1245]
{Microsoft} MS-MPPE-Recv-Key: \234\341\251\201\224\005\s\260f\345\366F\276\305 9
\356e\013\220\276\375\22
```

A network administrator integrates a current Mobility Master (MM)-Mobility Controller (MC) deployment with a RADIUS infrastructure. After using the RADIUS server to authenticate a wireless user, the network administrator realizes that the client machine is not falling into the it_department role, as shown in the exhibits.

Which configuration is required to map the users into the proper role, based on standard attributes returned by the RADIUS server in the Access Accept message?

A. `aaa server-group Corp-Network set role condition Filter-Id equals it-role set-value it_department` B. `aaa server-group GROUP-RADIUS set role condition Filter-Id equals it-role set-value it_department` C. `aaa server-group Corp-employee set role condition Filter-Id equals it-role set-value it_department` D. `aaa server-group Corp-employee set role condition Filter-Id value-of`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5 Refer to the exhibits.

Exhibit 1

Exhibit 2

```
top2 – 22:23:48 up 6:11, 0 users, load average: 0.11, 0.10, 0.08
Tasks: 202 total, 2 running, 198 sleeping, 0 stopped, 2 zombie
Cpu(s): 1.2%us, 2.9%sy, 0.2%ni, 95.6%id, 0.1wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 3085600k total, 1831312k used, 1254288k free, 19488k        buffers
Swap: 1048544k total,        0k useed, 1048544k free, 889680k        cached

PID  USER    PR NI  VIRT   RES   SHR   S   %CPU   %MEM  TIME+     COMMAND
3556  root   20  0   147m  79m   15m   R    85     2.7    0:39.54   profmgr
3017  root   20  0   9472  3952  2656  S    23     0.1    1:30.44   syslogd
3565  root   10 -10  132m 36m   13m   S    15     1.2    0:37.09   auth
4007  root   20  0   68208 8896  5920  S    10     0.3    0:23.41   ofa
3497  root   20  0  334m  137m  10m   S     6     4.6    11:31.80  fpapps
3894  root   20  0  124m   23m  5472  S     6     0.8    0:10.00   dds
4125  root   20  0  52640  6496  3296  S     6     0.2    0:28.97   vrrp
   13  root   20  0      0     0     0  S     4     0.0    0:02.05   events/1
3583  root   20  0  173m   25m  9696  S     4     0.8    1:47.79   stm
12505 root   20  0  3104   1680  1248  R     4     0.1    0:00.03   top2
3511  root   20  0  51088  6288  3712  S     2     0.2    0:04.90   pim
3807  root   20  0  220m   71m  5568  S     2     2.4    0:18.20   fw_visibility
    1  root   20  0  4160   1104  912  S     0     0.0    0:03.13   init
    2  root   20  0      0     0     0  S     0     0.0    0:00.00   kthreadd
```

A network administrator adds a new Mobility Controller (MC) to the production Mobility Master (MM) and deploys APs that start broadcasting the employees SSID in the West wing of the building. Suddenly, the employed report client disconnects.
When accessing the MM the network administrator notices that the MC is unreachable, then proceeds to access the MC's console and obtains the outputs shown in the exhibits.

What should the network administrator do next to solve the current problem?

A. Decommission the MC from the MM, and add it again.
B. Open a TAC case, and send the output of tar crash.
C. Verify the license pools in the MM.
D. Kill two zombie processes, then reboot the MC.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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)   Confi
g 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] #
```

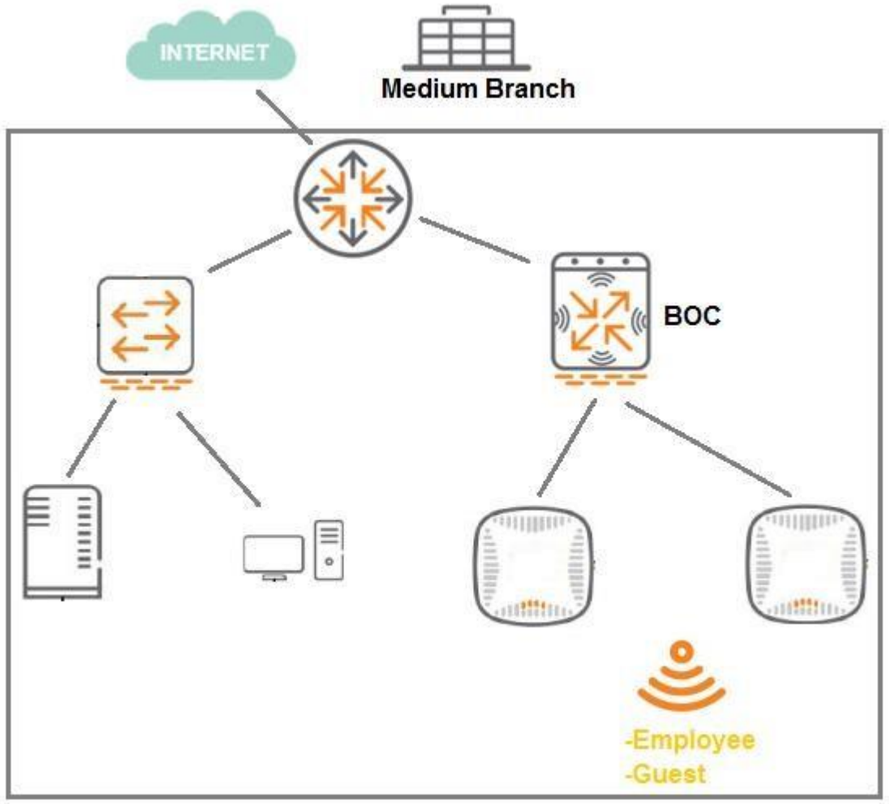
A network administrator adds a Mobility Controller (MC) in the /mm level and notices that the device does not show up in the managed networks hierarchy. The network administrator accesses the CLI, executes the `show switches` command, and obtains the output shown in the exhibit.

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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 7
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.

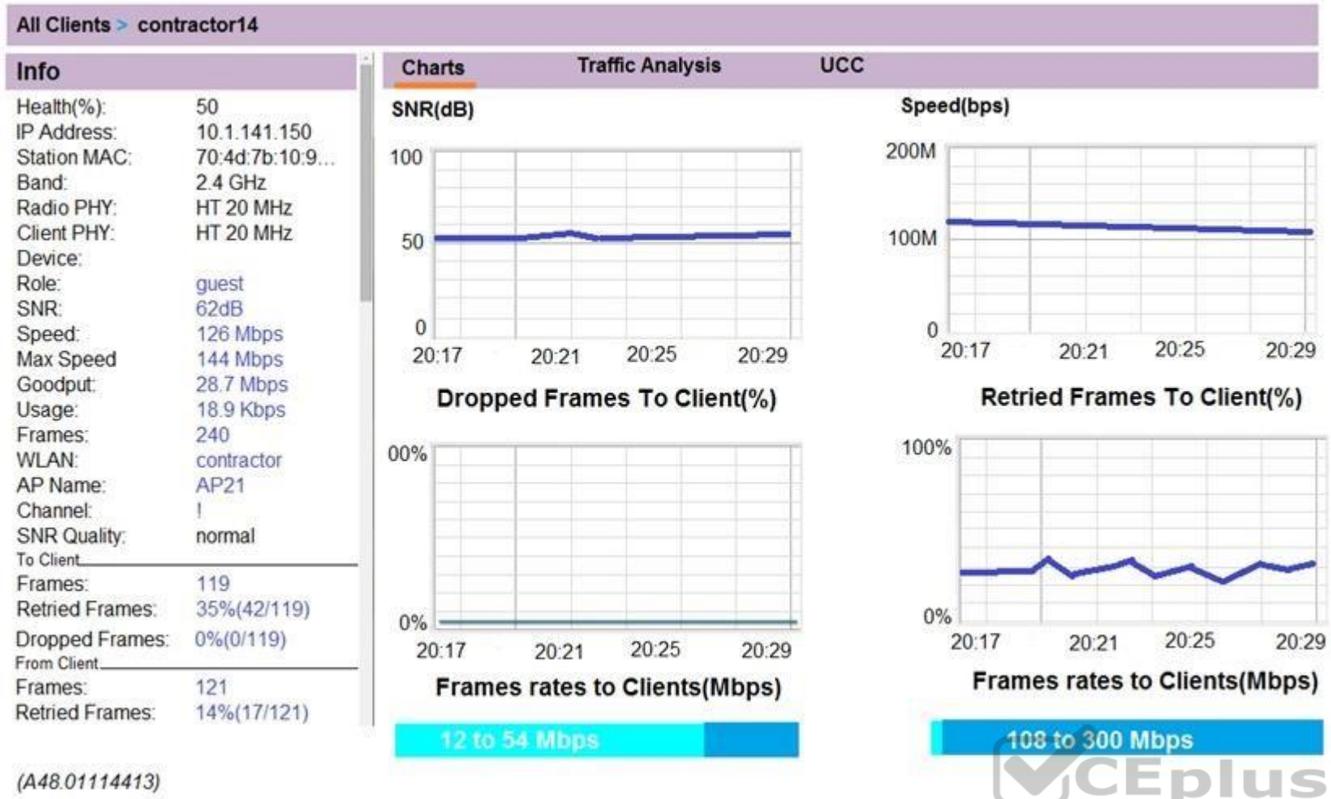
Which two different configuration options ensure that wireless users are able to reach the branch network through the router? (Select two.)

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Refer to the exhibit.



A user reports show response time to a network administrator and suggests that there might be a problem with the WLAN. The user's laptop supports 802.11n in the 2.4 GHz band only. The network administrator finds the user on the Mobility Master (MM) and reviews the output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

A. Client health is low, and retried frames are high. It is possible there is high channel utilization.
B. Client health is low, but SNR is high. It is possible data in the dashboard is not accurate and needs to be updated.
C. The speed is good. Client health seems to be related to a problem with the client NIC.
D. The network is low because of low SNR. TX power must be increased in both the client and the AP.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A customer with a multi-controller network upgrades the ArubaOS from 6.4 to 8. The customer's clients must be able to move between different locations of the campus without disconnecting their applications, when roaming or if there are Mobility Controller (MC) failures. The customer also wants to have full control of the users, and be able to change their session properties from a RADIUS server.

Which steps must the network consultant include in the implementation plan to meet these requirements?

A. 1. Create a controller cluster profile that contains the management and VRRP IP addresses of each member.
   2. Apply the profile to all MCs in the cluster.
   3. Confirm that the cluster is L2 connected.
B. 1. Configure a VRRP instance for all MCs

2. Create a controller cluster profile that contains the management IP and VIP addresses of each MC.
3. Apply the profile to all MCs in the cluster.
4. Confirm that the cluster is L2 connected.

C. 1. Configure a VRRP instance for each MC.
2. Create a controller cluster profile that contains the management IP of each member.
3. Apply the profile to all MCs in the cluster.
4. Confirm that the cluster is L3 connected.

D. 1. Create a controller cluster profile that contains the management and VRRP IP addresses of each member.
2. Apply the profile to the cluster leader.
3. Confirm that the cluster is L2 connected.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Refer to the exhibit.

(MC2) #show datapath session table 10.1.141.150

Datapath Session Table Entries

Flags: F – fast age, S – src NAT, N – dest NAT
D – deny, R – redirect, Y – no syn
H – high prio, P – set prio, T – set ToS
C – client, M – mirror, V – VOIP
Q – Real-Time Quality analysis
u – Upstream Real-Time Quality analysis
I – Deep inspect, U – Locally destined
E – Media Deep Inspect, G – media signal
r – Route Nexthop, h – High Value
A – Application Firewall Inspect
B – Permanent, O – Openflow
L – Log

Source IP	Destination IP	Prot	SPort	Dport	Cntr	Prio	ToS	Age	Destination	TAge	Packets	Bytes	Flags
10.254.1.21	10.1.141.150	17	53	64519	0/0	0	0	1	tunnel 29	12	2	318	FIA
10.254.1.24	10.1.141.150	6	5061	62781	0/0	6	0	0	tunnel 29	5f5	110	79604	I
10.1.141.150	13.107.21.200	6	62852	443	0/0	0	6	1	tunnel 29	25	29	8501	C
10.1.41.150	10.254.1.121	17	64519	53	0/0	0	0	1	tunnel 29	12	2	154	FCIA
10.254.1.24	10.1.141.150	17	51248	5968	0/0	5	34	0	0/0/0	22	1294	270387	FHPTCV
10.1.141.150	10.254.1.24	6	62781	5061	0/0	6	6	0	tunnel 29	5f7	100	32340	CI
10.254.1.24	10.1.141.150	17	51249	5969	0/0	5	34	0	0/0/0	24	208	134541	FHPTCV
23.218.145.187	10.1.141.150	6	443	62849	0/0	0	0	4	tunnel 29	3a	16	15430	
10.1.141.150	13.107.21.200	6	62853	443	0/0	0	6	2	tunnel 29	27	11	1137	C
10.1.141.150	10.254.1.24	17	5968	51248	0/0	0	0	0	0/0/0	24	207	131034	FHPTV
13.107.21.200	10.1.141.150	6	443	62853	0/0	0	0	3	tunnel 29	27	14	8962	
10.1.141.150	23.218.145.187	6	62849	443	0/0	0	6	4	tunnel 29	3a	10	1198	C
13.107.21.200	10.1.141.150	6	443	62852	0/0	0	0	2	tunnel 29	27	32	10610	
10.1.141.150	10.254.1.24	17	5968	51248	0/0	0	0	1	0/0/0	24	19	2304	FHPTV

A network administrator deploys DSCP based prioritization in the entire wired network to improve voice quality for a SIP-based IP telephony system used by the company. However, users report that calls they make from the WLAN have poor audio quality, while desktop phones do not experience the same problem. The network administrator makes a test call and looks in the datapath session table.

Based on the output shown in the exhibit, what is one area that the network administrator should focus on?

A. wireless network congestion
B. WMM support on the WLAN
C. UCC based DSCP correction
D. wired network congestion

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

Refer to the exhibit.

```
a8:bd:27:c5:c3:3a# sh dhcp subnets

DHCP Subnet Table
-----------------------------
VLAN  Type   Subnet        Mask            Gateway       Mode                Rolemap
---------  -------  ------------  ----------  -------------  ---------  -------------
124   I3     10.21.124.32  255.255.255.224  10.21.124.33  local,split-tunnel
81    I2     0.0.0.0       255.255.255.255  0.0.0.0       remote,full-tunnel
```

A network engineer deploys two different DHCP pools in an Instant AP (IAP) cluster for WLANs that will have connectivity to a remote site using Aruba IPSec.

Based on the output shown in the exhibit, which IAP-VPN DHCP modes are being used?

A. distributed L3 and centralized L3 B.
distributed L3 and local L3
C. distributed L3 and centralized L2
D. local L3 and centralized L2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 Refer
to the exhibits.

Exhibit1

```
(MC1) (MDC) #show ap database

AP Database
--------------------
Name   Group                AP Type    IP Address     Status          Flags     Switch IP      Standby IP
----------  -----------  --------------  -----------------  -----------  ---------  ---------------  -----------------
AP1    MainCampus-SC-B1  335        10.1.145.150   Up 4h:14m:10s  2I        10.1.140.100   10.1.140.101
AP12   CAMPUS            335        10.1.146.150   Up 13m:19s     2         10.1.140.100   10.1.140.101

Flags: 1 = 802.1x, authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1.= 802.1x use factory cert; 2 = Using IKE version 2
       B = Built-in AP; C = Cellular RAP; D = Dirty or no config
       E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
       G = No such group; I = Incative; J = USB cert at AP; L = Unlicnesed
       M = Mesh node
       N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
       S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
       Y = Mesh Recovery
       c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
       i = Indoor; o = Outdoor; s = LACP striping; u = Custom-cert RAP; z = Datazone AP

Total APs:2
```

Exhibit 2

```
(MC11) [mynode] #show ap database

AP     Database
----------------------
Name               Group     AP Type    IP Address         Status       Flags   Switch IP      Standby IP
--------           ----------  ----------  ----------------- --------     --------  --------------  ---------------
70:3a:0e:cd:b0:a4  default   335        10.1.145.150       Down         2       10.254.13.14   0.0.0.0
a8:bd:27:c5:c3:3a  default   335        10.1.147.2         Down         2       10.254.13.14   0.0.0.0
AP12               CAMPUS    335        10.1.146.150       Up 21m:37s   2z      10.254.13.14   0.0.0.0
```

Based on outputs shown in the exhibits, what is the reason that AP12 is seen by two different controllers?

A. AP12 connects to a high availability group. MC1 is the active controller, and MC11 is the standby controller.
B. AP12 is a multizone AP. MC1 is part of the primary zone, and MC11 is part of the datazone.
C. AP12 connects to an MC cluster. MC1 is the A-AAC, and MC2 is S-AAC.
D. AP12 is in the middle of the boot process. MC1 is the master IP controller, and MC11 is the LMS IP controller.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Refer to the exhibit.

```
(MM1) [mynode] #show ip interface brief

Interface    IP Address   /  IP Netmask      Admin    Protocol    VRRP-IP
vlan 1       10.254.10.14 /  255.255.255.0   up       up          10.254.10.214
loopback     unassigned   /  unassigned      up       up
mgmt         unassigned   /  unassigned      down     down
(MM1) [mynode] #show vrrp

Virtual Router 140:
        Description MM1
        Admin State UP, VR State BACKUP
        IP Address 10.254.10.214, MAC Address 00:00:5e:00:01:8c, vlan1
        Priority 100, Advertisement 5 sec, Preemption Enable Delay 60
        Auth type PASSWORD, Auth data: ********
        tracking is not enabled
(MM1)  [mynode]#
```

After a recent power outage where MM1 is located, the network administrator could not perform configuration tasks on Mobility Controllers (MC) for several hours. The network administrator decides to acquire another Mobility Master (MM) and deploy L2 MM redundancy. The new MM is assigned the 10.254.10.15 IP address and VRRP is configured in both units. The network administrator verifies that VRRP is running, and prepares to complete the setup with the following scripts.

```
/mm/mynode (MM1):
     master-redundancy
     master-vrrp 140
     peer-ip-address 10.254.10.15 ipsec key123
/mm/mynode (MM2):
     master-redundancy
     master-vrrp 140
     peer-ip-address 10.254.10.14 ipsec key123

/mm (MM1):
database synchronize period 30
```

Which configuration tasks must the network administrator do before applying the script in order to successfully deploy L2 MM redundancy and prevent any other control plane outage?

A. Confirm that the VRRP and master redundancy keys are the same.
B. Change the VIP address of ther VRRP process 140 to 10.254.10.15.
C. Reduce the VRRP priority to 90 and restart the process in MM2.
D. Enable the MM database synchronization in MM2.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Company 1 and Company 2 are medium-sized companies that collaborate in a joint venture. Each company owns a building, and each has their own ArubaOS 8 Mobility Master (MM)-Mobility Controller (MC) deployment. The buildings are located in front of one another. For the initial stage of the project, the companies want to interconnect their networks with fiber, and broadcast each other's SSIDs.

These are the requirements:

- Do not unify the company's network management responsibilities.
- Allow each company to take care of their own SSID setups when broadcasted in the other building.
- Terminate Company 1 user traffic on Company 1 MCs when they connect to Company 2 APs.
- Terminate Company 2 user traffic on Company 2 MCs when they connect to Company 1 APs.

What is needed to meet the solution requirements?

A. Multizone APs
B. Inter MC S2S Ipsec tunnels
C. Multi MC Clusters
D. Inter MC GRE tunnels

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15 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

```
(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] #
```

Exhibit 3

```
(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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A network administrator deploys AirWave over a Mobility Master (MM)-Mobility Controller (MC) network to monitor, audit, and report activities. The main areas of concern are with high user density, not enough APs, or not enough channel bandwidth.

Which two report options can the network administrator user to create a weekly report that shows networking equipment with more users and high-demand applications used by top talkers? (Select two.)

A. Most Utilized Folders by Maximum Concurrent Clients
B. Most Utilized by Usage
C. Top Applications Summary
D. Most Utilized by Maximum Concurrent Clients
E. Top 3 Applications For Top 10 Users

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Several users are connected to the same WLAN and want to play the same multicast-based video stream. The network administrator wants to reduce bandwidth consumption and at the same time increase the transmit rate to a fixed value for WMM marked video streams in a large-scale network. Broadcast Multicast Optimization (BCMCO) is already on.

Which two configuration steps does the network administrator have to perform to optimize the multicast transmissions? (Select two.)

A. Enable Dynamic Multicast Optimization (DMO) and set forwarding mode to tunnel in the VAP profile.
B. Enable Broadcast Multicast Rate Optimization (BC/MC RO) in the SSID profile.
C. Enable Broadcast Multicast Optimization (BCMCO) and set forwarding mode in the VAP.
D. Disable Broadcast Multicast Optimization (BCMCO) in the VLAN.
E. Set Video Multicast Rate Optimization (VMRO) in the SSID profile.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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=Employee, 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:260
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: 704D7B109EC6
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ server.c:2383] Called-Station Id: 005056A5CA1A
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:
AGcATgBnAKj9IQQAkgY0j1ulavminP5/0Vna0PQ==
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: \352F\372\012\250\223
\035/c\256\321\250\214\3445\326
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_request.c:95] Find Request: id=45, server=(null), IP=
10.254.1.23, server-group=(null), fd=63
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_request.c:104] Current entry: server=(null), IP=
10.254.1.23, server-group=(null), fd=63
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_request.c:48] Del Request: id=45, server=ClearPass,
IP=10.254.1.23, server-group=Employee fd=63
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1228] Authentication Successful
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] {Aruba} Aruba-User-Role: contractor
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] {Microsoft} MS-MPPE-Recv-Key: \206\032
\023>L\364\275n\231\004\2521P\217\023|K\0241\303t\332\217\273Fe9\022\346(\372\320= "c\303jK\023\222\276\020
\244\005\331\314e\217\024(
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] {Microsoft} MS-MPPE-Send-Key: \210\316
\275\015\315\012\025j\247\0325\207\021\336 \264t\334 \206\231
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_ api.c:1245] EAP-Message: \003\012
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Message-Auth: z\3312C\022\013\275
\020\243\227
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] User-Name: contractor12
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Class: \202\005\250)\210\215C\344\2536
#\356\200\243"\006\271\013
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RADIUS_ID: -
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Rad-Length: 250
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RADIUS_CODE: \002
Jun 23 21:28:17 :121031: <5533> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RAD_AUTHENTICATOR: RY\273
\370\325$\211\341\027R\363YM\261\236\025
Jun 23 21:28:17 :124003: <5533> <INFO> |authmgr| Authentication result=Authentication Successful (0), method=
802.1x, server=ClearPass, user=70:4d:7b:10:9e:c6
```

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 firewall role.

To do this, the network administrator configures ClearPass in a way that it returns the Aruba-User-Role VSA 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?

A. Set contractor as the default role in the AAA profile.
B. Create the contractor firewall role in the MC.
C. Create server derivation rules in the server group.
D. Check the Download role from the CPPM option in the AAA profile.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
An organization owns a fully functional multi-controller Aruba network with a Virtual Mobility Master (VMM) in VLAN 20. 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? (Select three.)

A. Reserve one IP address for the second MM and another IP address for its gateway
B. Configure an ACL entry that permits IP protocol 50, UDP port 500, and multicast IP 224.0.0.18.
C. Allocate VLAN 20 to the second server, and extend it throughout the switches.
D. Reserve one IP address for the second MM and another for the VIP.
E. Configure an ACL entry that permits UDP 500, UDP 4500, and multicast IP 224.0.0.1.
F. Allocate another VLAN to the second server, and permit routing between them.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Refer to the exhibit.

```
(MC14-1) #show ap database | exclude =
AP Database
-------------------
Name  Group      AP Type   IP Address    Status        Flags   Switch IP    Standby IP
--------  ---------  -----------  ---------------  ---------  ---------  ------------  ----------------
AP10  CAMPUS    335        10.1.145.150  Up 35m:35s    2       10.1.140.100   0.0.0.0
AP20  CAMPUS    335        10.1.146.150  Down                  10.1.140.100   0.0.0.0

Total APs:2
(MC14-1) #ping 10.1.146.150

Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 10.1.146.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.22/0.2528/0.355 ms

(MC14-1) #show log system 5 | include AP20
Aug 6 15:29:08  :303022: <WARN> |AP AP20@10.1.146.150 nanny| Reboot Reason: AP rebooted Wed Dec 31 16:24:10
PST 1969; Unable to set up IPSec tunnel to saved lms, Error: RC_ERROR_IKEV2_TIMEOUT
Aug 6 15:52:43 :311020: <ERRS> |AP AP20@10.1.146.150 sapd| An internal system error has occurred at file
sapd_redun.c function redun_retry_tunnel line 4529 error redun_retry_tunnel: Switching to clear.
Error:RC_ERROR_IKEV2_TIMEOUT. Ipsec not successful after reboot.
Aug 6 15:53:07 :311002: <WARN> |AP AP20@10.1.146.150 sapd| Rebooting: SAPD: Rebooting after setting cert_cap=1.
Need to open a secure channel(IPSEC)
Aug 6 15:53:08 :303086: <ERRS> |AP AP20@10.1.146.150 nanny| Process Manager (nanny) shutting down – AP will
reboot!
Aug 6 15:54:23 :303022: <WARN> |AP AP20@10.1.146.150 nanny| Reboot Reason: AP rebooted Mon Aug 6 15:53:08
PDT 2018; SAPD: Rebooting after setting cert_cap=1. Need to open a secure channel(IPSEC)
(MC14-1) #
```

A network administrator deploys a Mobility Master (MM)-Mobility Controller (MC) solution in the headquarters. The network administrator prepares the wired side of the network with the proper VLAN, DHCP settings, and routing services to ensure that APs can reach the MCs.

The network administrator connects two APs in different IP segments and waits for 20 minutes, but SSIDs are advertised in one of the APs only. The engineer logs into the MC console and sees the output shown in the exhibit.

What is the reason that the AP20 is not broadcasting SSIDs?

A. IPSec traffic is being blocked.
B. IKE traffic is being dropped.
C. PAPI traffic is being blocked.
D. GRE traffic is being blocked.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Refer to the exhibit.

```
(MC11) [mynode] #show ap database long | exclude =

AP Database
-----------
Name  Group    AP Type  IP Address    Status       Flags  Switch IP     Standvy IP  Wired MAC Address  Serial#        Port  FQLN  Outer IP  User
-----  -------  -------  ----------    ------       -----  ----------    ----------  ----------------   -------        ----  ----  --------  ----
AP21  CAMPUS  335      10.1.145.150  Up 3m:20s  UNI    10.254.13.14  0.0.0.0     70:3a:0e:cd:b0:a4  CNBXJOY301  N/A   N/A   N/A
AP21  CAMPUS  335      10.1.146.150  Up 32m:23s         10.254.13.14  0.0.0.0     70:3a:0e:cd:b0ac   CNBXJOY305  N/A   N/A   N/A

Total APs:2
(MC11) [mynode] #Show ap active | exclude =

Active  AP Table
----------
Name Group       IP Address   11g Clients  11g Ch/EIRP/MaxEIRP   11a Clients  11a Ch/EIRP/MaxEIRP   AP Type  Flags  Uptime     Outer IP
----------       ----------   ----------   -------------------   ----------   -------------------   -------  -----  ------     --------
AP21  CAMPUS     10.1.146.150 0            AP:HT:11/9.0/24.0     0            AP:VHT:153E/18.0/28.5 335      Aa     32m:30s    N/A

Channel followed by "+" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrun Override in effect.

Num APs: 1
```

A network administrator deploys a new Mobility Master (MM)-Mobility Controller (MC) network. To test the solution, the network administrator accessess some of the AP consoles and statistically provisions them. However, these APs do not propagate the configured SSIDs. The network administrator looks at the logs and sees the output shown in the exhibit.

Which actions must the network administrator take to solve the problem?

A. Reprovision one of the APs with a different name, and add new entries with the proper group in the whitelist.
B. Reprovision the AP with a different group, and modify the name of one AP in the whitelist.
C. Create another AP group in the MC's configuration and reprovision one AP with a different group.
D. Reprovision one of the APs with a different name, and modify the name of one AP in the whitelist.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A company has headquarters based in the US and rents internation office space in Mexico City so that 10 employees can work remotely. The company must implement a remote access technology so branch office employees can access all servers at the headquareters.

The office has both wired and wireless internet connectivity, with no restrictions on what device connects to the network. However, ports UDP 4500, 5060, and 5061 are blocked by the primeter firewall.

Which remote access technology is required to allow employees to access the servers at the headquarters?

A. BOC with CAPs
B. IAP VPN
C. RAP
D. VIA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 23

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.

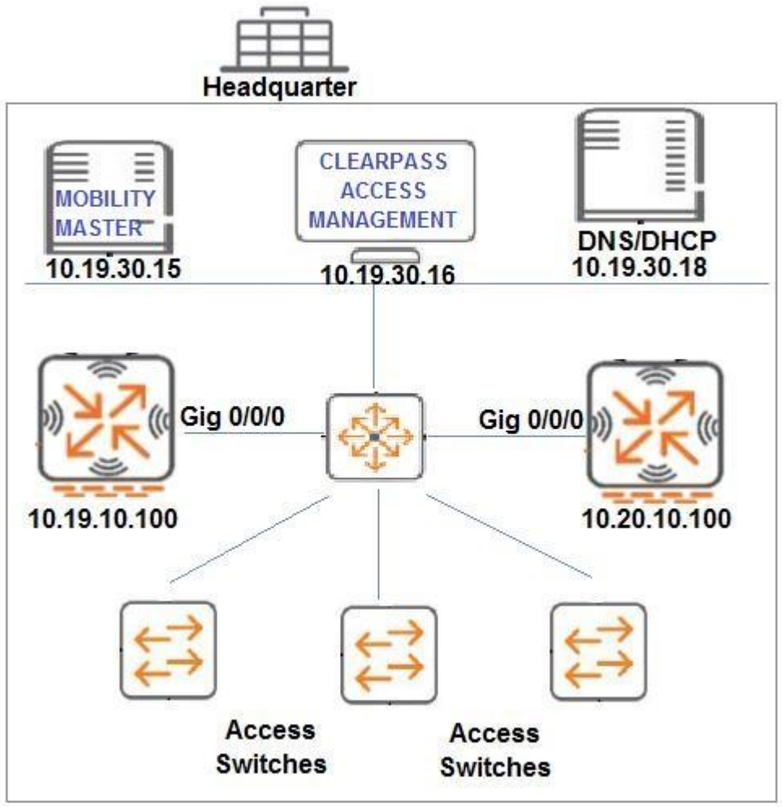
How should the network administrator deploy both controllers in order to provide redundancy while preventing failover events from disconnecting users?

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Refer to the exhibit.



A network administrator is in charge of a wired and wireless Aruba network where access control is needed for both connection methods. For the wired solution, the network administrator wants the users authentication to be performed at the switches, while tunneling their traffic to MC1 whenever possible for firewall policy enforcement. The network administrator configures and tests ClearPass as the RADIUS server in the switches.

Which switch configuration scripts should the network administrator use next to achieve this goal?

A. tunneled-node-server controller-ip
10.19.10.100 backup-controller-ip
10.20.10.100 mode role-based

aaa authentication port-access eap-radius
aaa port-access authenticator 1-22 aaa
port-access authenticator active B.
tunneled-node-server controller-ip
10.20.10.100 backup-controller-ip
10.19.10.100 mode port-based

aaa authentication port-access eap-radius
aaa port-access authenticator 1-22 aaa
port-access authenticator active C.
tunneled-node-server controller-ip
10.20.10.100 backup-controller-ip
10.19.10.100

aaa authentication port-access eap-radius
aaa port-access authenticator 1-22 aaa
port-access authenticator active D.
tunneled-node-server controller-ip
10.19.10.100 backup-controller-ip
10.20.10.100

aaa authentication port-access eap-radius
aaa port-access authenticator 1-22 aaa
port-access authenticator active

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An organization wants to deploy a WLAN infrastructure that provides connectivity to these client categories:

- Employees
- Contractors
- Guest users
- Corporate IoT legacy devices that support no authentication or encryption

Employees and contractors must authenticate with company credentials and get network access based on AD group membership. Guest users are required to authenticate with captive portal using predefined credentials. Only employees will run L2 encryption.

Which implementation plan fulfills the requirements while maximizing the channel usage?

A. Create VAP1 to run WPA2-AES and 802.1x authentication, VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal.
B. Create VAP1 to run WPA2-AES and 802.1x authentication, VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal and L2 fail through.
C. Create a single VAP to run WPA2-AES and 802.1x authentication, MAC authentication L2 fail through, captive portal, and VIA support.
D. Create VAP1 to run WPA2-AES and 802.1x authentication, and VAP2 to run opensystem encryption with MAC authentication and captive portal.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26 Refer to the exhibits.

Exhibit 1

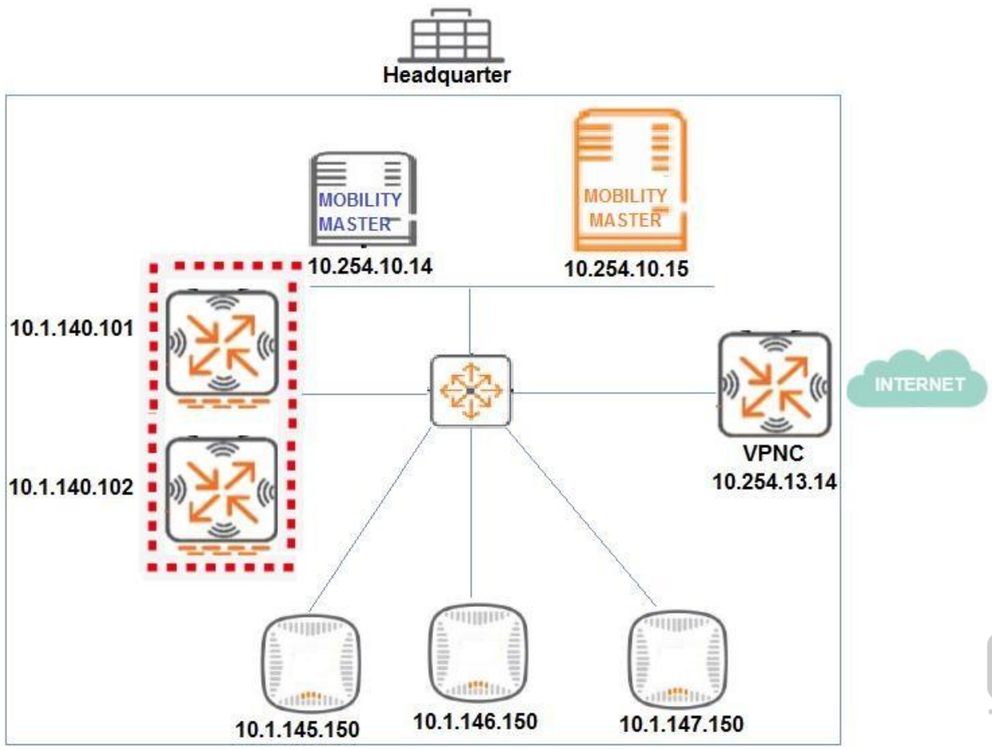


Exhibit 2

```
(MC14-1) #show ap database | exclude =

AP Database
------------------
Name        Group       AP Type     IP Address    Status  Flags  Switch IP  Standby IP
--------    --------    -----------  ----------------  --------  -------  --------------  ----------------

Total APs:0
(MC14-1) #ping 10.1.145.150

Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 10.1.145.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.206/0.2402/0.356 ms
```

Exhibit 3

```
[        11.611533] bonding: bond0: link status definitely down for interface eth1, disabling it
Starting watchdog process…
Getting an IP address…
[        12.689236] device eth0 entered promiscuous mode
10.1.145.150 255.255.255.0 10.1.145.1
Running ADP…Done.Master is 10.1.140.100
[        22.039696] ath_hal: 0.9.17.1 (AR5416, AR9380, REGOPS_FUNC, WRITE_EEPROM, 11D)
[        22.131095] ath_rate_atheros: Copyright (c) 2001-2005 Atheros Communications, Inc, All Rights Reserved

[        37.552112] pktlog_init: Initializing Pktlog for AR900B, pktlog_hdr_size = 16
[        37.638632] pktlog_init: Initializing Pktlog for AR900B, pktlog_hdr_size = 16
AP rebooted due to loss power
shutting down watchdog process (nanny will restart it)…
        <<<<<        Welcome to the Access Point        >>>>>
– # ping 10.1.140.100
PING 10.1.140.100 (10.1.140.100): 56 data bytes
^C
--- 10.1.140.100 ping statistics ---
40 packets transmitted, 0 packets received, 100% packet loss
– # ping 10.1.140.1
PING 10.1.140.1 (10.1.140.1) : 56 data bytes
64 bytes from 10.1.140.1: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 10.1.140.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.1.140.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 10.1.140.1: icmp_seq=3 ttl=255 time=0.3 ms
64 bytes from 10.1.140.1: icmp_seq=4 ttl=255 time=0.3 ms
^C
--- 10.1.140.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.4 ms
– #
```

A network engineer deploys a Master Controller (MC) cluster at Headquarter to offer high levels of redundancy, and prepares the wired side of the network. This preparation includes the VLAN, DHCP Settings, and unicast routing services that APs require to reach the cluster.

The network engineer waits for 20 minutes after connecting the APs and sees that no SSIDs are advertised. The network engineer logs into one of the MCs and one of the AP's consoles to obtain the outputs shown in the exhibits.

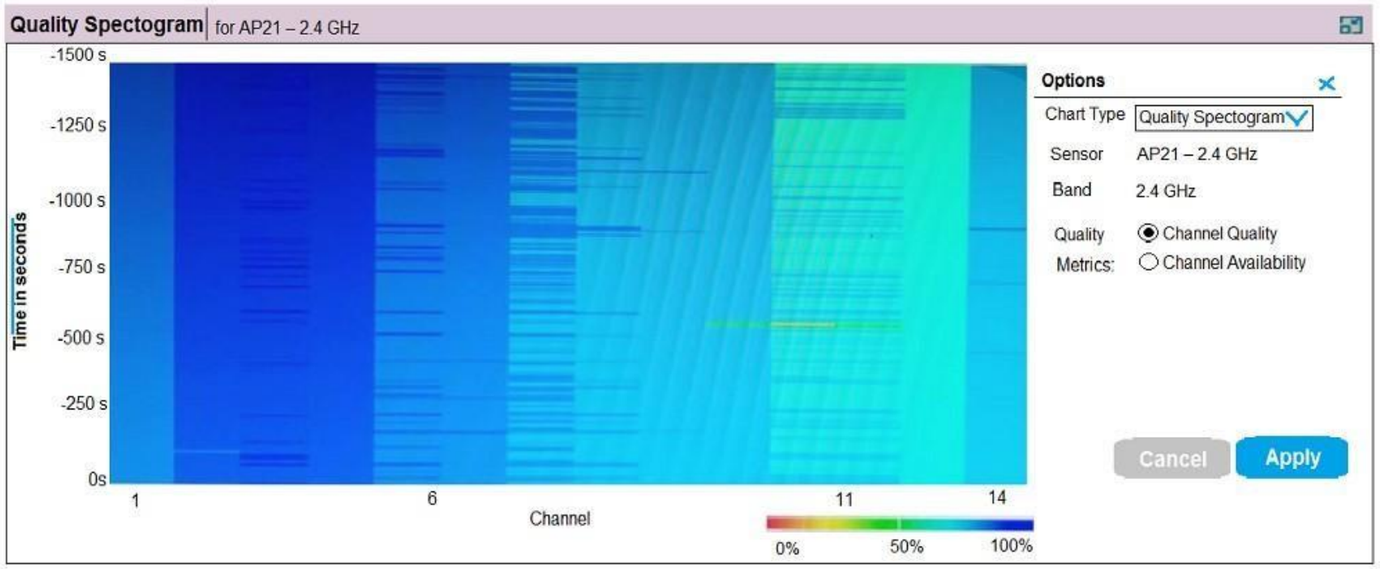
What can the network engineer do to fix the APs discovery process, to ensure the best scalability even if one MC fails?

A. Reprovision the APs with a different Master IP.
B. Modify the IP address in one of the MCs.
C. Modify option 43 in the DHCP pool.
D. Create a VRRP instance in the MCs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Refer to the exhibit.



(A48.01114442)

Based on the output shown in the exhibit, which channel offers the highest quality?

A. Channel 1
B. Channel 6
C. Channel 11
D. Channel 14

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Users run encrypted Skype for Business traffic with no WMM support over an Aruba Mobility Master (MM)-Mobility Controller (MC) based network. When voice, video, and application sharing traffic arrive at the wired side of the network, all the flows look alike due the lack of L2 or L3 markings.

How can the network administrator identify these flows and mark QoS accordingly?

A. Confirm the MC is the Openflow controller of the MMs and Openflow is enabled in VAP and the firewall roles. Then enable WMM in a VAP profile.
B. Confirm the MM is the Openflow controller of the MCs and Openflow is enabled in VAP and the firewall roles. Then integrate the MM with the Skype4Business SDN API, and enable the Skype4Business ALG in the UCC Profiles.
C. Confirm the MC is the OpenFlow controller of the MMs and Openflow is enabled in VAP and the firewall roles. Then enable the Skype4Business ALG in the UCC profiles.
D. Use a media firewall policy that match these three flows, and use permit and TOS actions with 56, 40, and 34 values for voice, video, and application sharing, respectively. Then enable the Skype4Business ALG in the UCC profiles.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Refer to the exhibit.

(MM) [mynode] #show airmatch event all-events ap-name AP2

Band	Event Type	Radio	Timestamp	Chan	CBW	New Chan	New CBW	APName
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-25_07:50:05	100	80MHz	149	80MHz	AP2
5GHz	NOISE_DETECT	38:17:c3:10:17:30	2018-07-24_07:48:42	124	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-23_16:44:36	100	80MHz	124	80MHz	AP2
5GHz	NOISE_DETECT	38:17:c3:10:17:30	2018-07-20_19:12:34	157	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-20_10:02:30	100	80 MHz	157	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-20_08:34:31	56	80 MHz	100	80MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-25_08:31:31	11	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-25_08:31:31	6	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-24_07:46:34	1	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-24_07:46:33	6	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-23_15:13:15	11	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-23_15:12:12	1	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-20_08:07:27	11	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-20_08:07:26	6	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_19:22:45	1	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_19:22:44	11	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_10:45:23	1	20MHz	11	20MHz	AP2

A network administrator deploys a Mobility Master (MM)-Mobility Controller (MC) network with APs in different locations. Users in one of the locations report that the WiFi network works fine for several hours, ang then they are suddenly disconnected. The symptom may happen at any time, up to three times every day, and lasts no more than two minutes.

After some research, the network administrator logs into the MM and reviews the output shown in the exhibit.

Based on this information, what is the most likely reason users get disconnected?

A. AirMatch is applying a scheduled optimization solution.
B. Users in the 2.4 GHz band are being affected by high interference.
C. Adpative Radio Management is reacting to RF events.
D. AirMatch is reacting to non-scheduled RF events.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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.

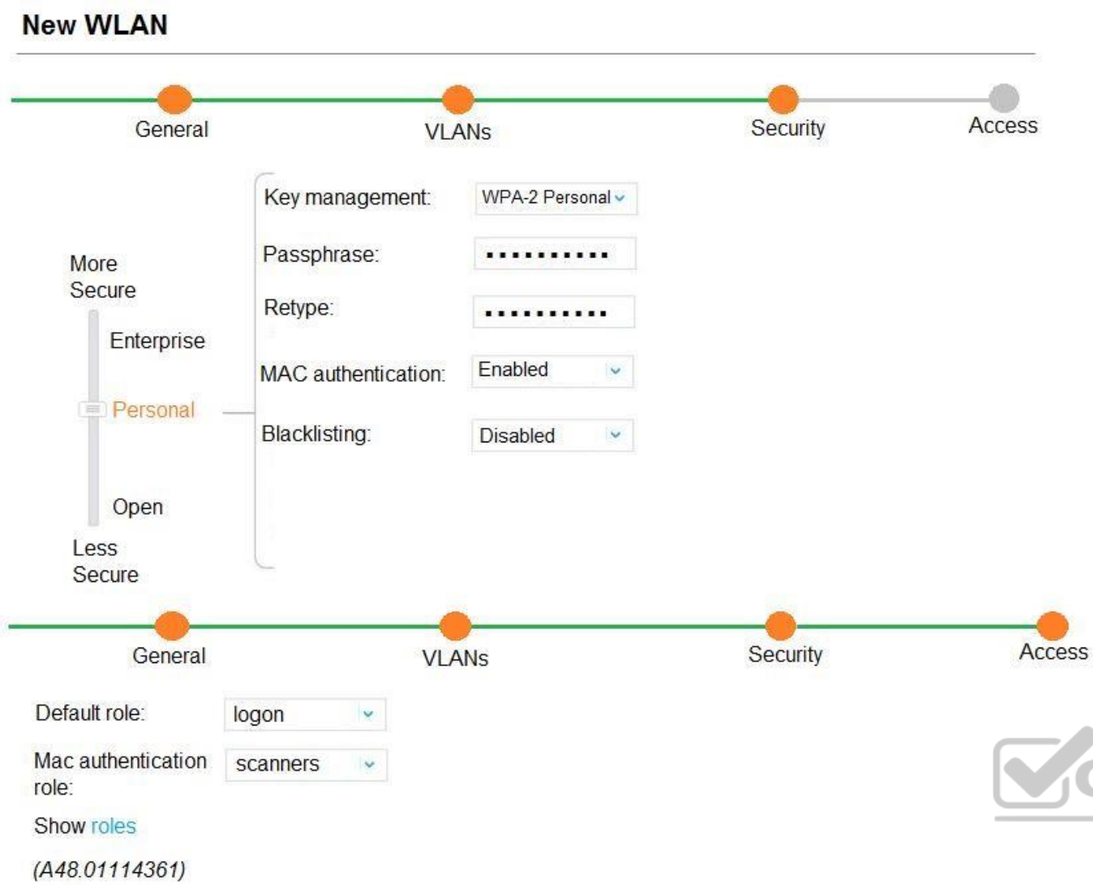
Based on the exhibit, what should the network administrator do next to fix this problem?

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Refer to the exhibit.



A company acquires ten barcode scanners to run inventory tasks. These Wifi devices support WPA2-PSK security only. The network administrator deploys a WLAN named scanners using the configuration shown in the exhibit.

What must the network administrator do next to ensure that the scanner devices successfully connect to their SSID?

A. Add scanner MAC addresses in user derivation rules.
B. Add scanner MAC addresses in the internal database.
C. Set internal as the MAC authentication server group.
D. Enable L2 Authentication Fail Through.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 Refer to the exhibits.

Exhibit 1

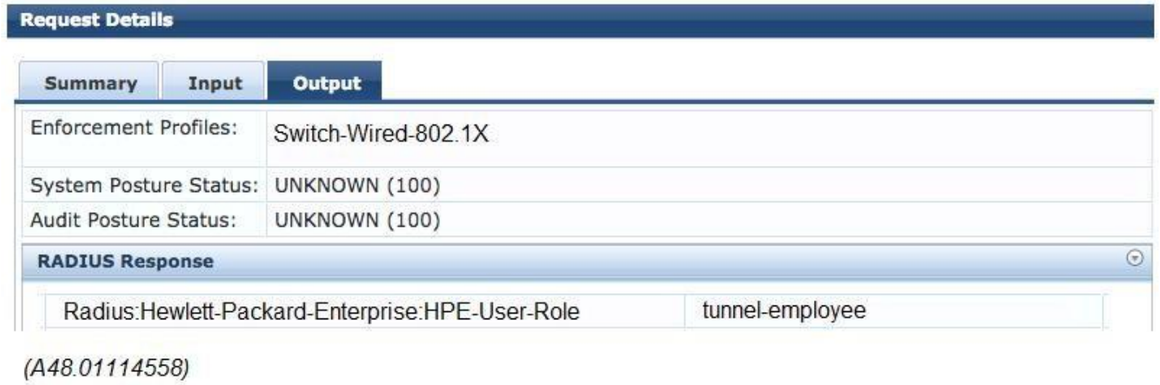


Exhibit 2

```
Access-1(config)# show port-access clients

Port Access Client Status

 Port   Client Name MAC Address    IP Address    User Role  Type
------- ---------------- ------------------------ ----------------- ----------------- ---------
VLAN
---------
 20     test           005056-a5510b      n/a            denyall   8021X
142
```

A network administrator deploys role-based tunneled node in a corporate network to unify the security policies enforcement. When users authenticate with 802.1X, ClearPass shows Accept results, and sends the HPE-User-Role attribute as expected. However, the switch always applies the denyall role.

Why does the switch fail to allocate the tunnel-employee role?

A. Denyall is a secondary role contained within tunnel-employee.
B. The switch is not configured with primary tunneled-node user role.
C. The switch is not configured with secondary tunneled-node user role.
D. RADIUS Access Accept messages time out in the switch.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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.)

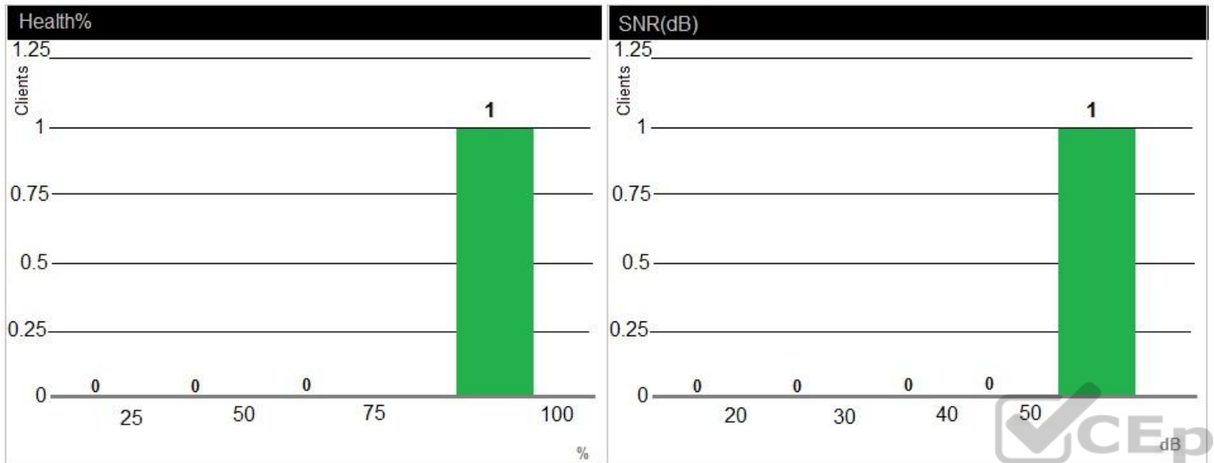
A. Associate the captive portal profile to the initial role
B. Define the web login URL and server group in a captive portal profile

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Refer to the exhibit.



Clients

USERNAME	CLIENT NAME	SNR^	SPEED (MBPS)	GOODPUT (MBPS)	HEALTH (%)	USAGE	DEVICE TYPE	ROLE	DEVICE NAME	LOCATION	SSID	CONNECTION
contractor14	-	58	819	32	93	1.84 Kbps	-	guest	AP12	-	contractor	11ac 5GHz

25 per page Page: 1 GO < 1 >

(A48.01114411)

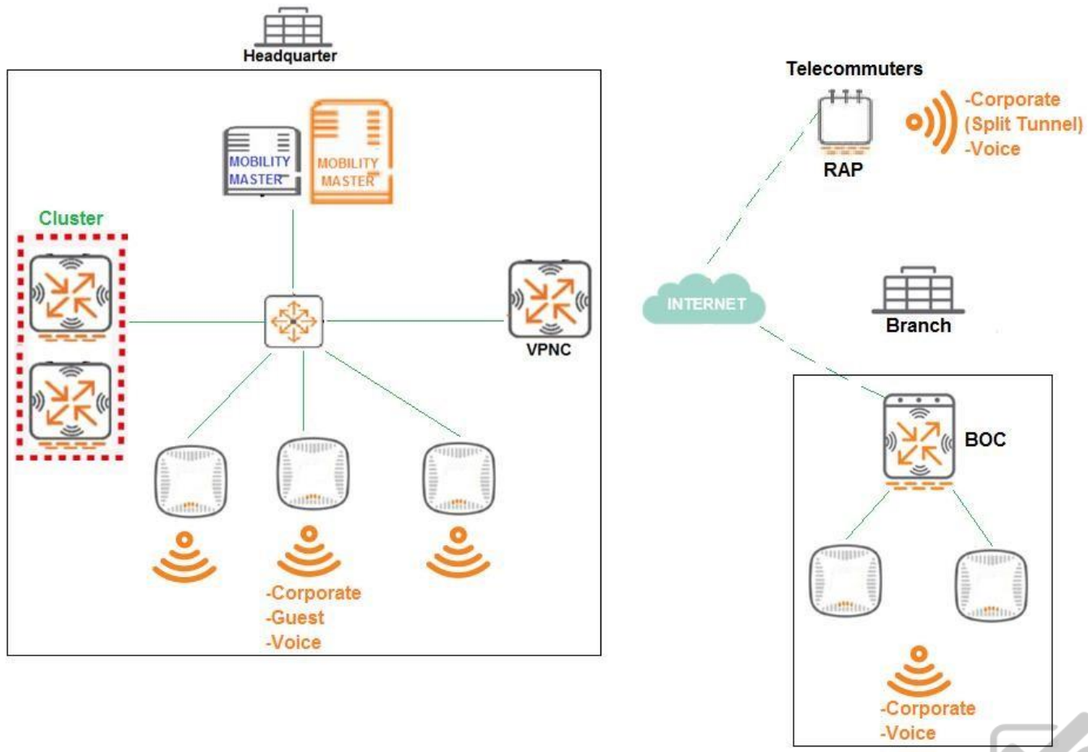
A network administrator receives a call from a contractor that was recently given wireless access to the network. The user reports that the response time is slow and suggests there might be a problem with the WLAN. The network administrator checks RF performance in AirWave to find the user and sees the output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

A. Client health and CNR are high, therefore, it is unlikely the client is experiencing an RF-related issue.
B. Goodput is low in relation to connection speed, which suggests a channel with high utilization, another channel should be used.
C. Client health and SNR are high but usage is low; therefore, there might be packet drops.
D. Client health is low, which suggests that there are packet drops and collisions in the RF environment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 35
Refer to exhibit.



A company has a multiple Arua implementation with three different locations named Headquarter, Branch, and Telecommuters.

The network design includes the following:

▪ Headquarter APs terminate at the Mobility Controller (MC) cluster and propagate Corporate, Guest, and Voice SSIDs
▪ Branch APs terminate at the Branch Office Controller (BOC) and propagate Corporate and Voice SSIDs ▪ BOC reaches the Mobility Master (MM) through a VPNC.
▪ Telecommuter RAPs terminate at VPNC and propagate Corporate and Voice SSIDs. ▪ The Corporate SSID on the RAPs is split-tunnel, all other SSIDs are tunnel.

The network design requires minimal AP group and VAP configuration effor, while preventing unnecessary VAP propagation to lower hierarchy levels.

Following Aruba node hierarchy desing recommendations, which group hierarchy design helps meet these requirements?

A. `/md`
`/md/Corp1/`
`/md/Corp1/Offices`
`/md/Corp1/Offices/Headquarter`
`/md/Corp1/Offices/Branch`
`/md/Corp1/Telecommuters`
`/mm`
`/mm/mynode`

B. `/md`
`/md/Headquarter`
`/md/Branch`
`/md/Telecommuters`
`/mm`
`/mm/mynode`

C. `/mm`

```
/md/Locations
/md/Locations/Headquarter
/md/Locations/Branch
/md/Locations/Telecommuters
/mm
/mm/mynode
```

D. /md

```
/md/Location1/
/md/Location1/Branch
/mdLocation1/Offices
/md/Location1/Offices/Headquarter
/md/Location1/Telecommuters
/mm
/mm/mynode
```

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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

Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A foreign exchange broker in a shared office space uses an Aruba Mobility Master (MM)-Mobility Controller (MC) architecture along with ClearPass and AirWave. The corporate network is FXBroker121, but users report that they cannot access the FXBroker111 SSID. The team suspects that a rogue AP is in place and a malicious user tried to disguise the WLAN name.

How can the organization's network administrator identify and locate the potential rogue AP?

A. Create an AirWave RAPIDS rule with a Suspected Rogue classification and the SSID Matches FXBroker111 condition, then access any RAPID List entry that matches the rule and click on Location.
B. Use ClearPass Event viewer and search for entries with the FXBroker111 Aruba-Essid-Name VSA attribute, then obtain the value of the Aruba-AP-Group attribute.
C. Use ClearPass Event viewer and search for entries with the FXBroker111 Aruba-Essid-Name VSA attribute, then obtain the value of the Aruba-Location-id attribute.
D. Create and AirWave RAPIDS rule with a Suspected Rogue classification and the SSID Does Not Match FXBroker121 condition, then access any RAPIDS List entry that matches the rule and click on Location.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac 70:4d:7b:10:9e:c6 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      *    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          -  -     wpa2  aes
Jun 29 20:56:51  eap-id-req      <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          1  5
Jun 29 20:56:51  eap-start       ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          -  -
Jun 29 20:56:51  eap-id-req      <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          1  5
Jun 29 20:56:51  eap-id-resp     ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          1  7     it
Jun 29 20:56:51  rad-req         ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          42 174  10.1.140.101
Jun 29 20:56:51  eap-id-resp     ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          1  7     it
Jun 29 20:56:51  rad-resp        <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1  42  88
Jun 29 20:56:51  eap-req         <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          2  6
Jun 29 20:56:51  eap-resp        ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          2  214
Jun 29 20:56:51  rad-req         ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1  43  423  10.1.140.101
Jun 29 20:56:51  rad-resp        <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1  43  228
Jun 29 20:56:51  eap-req         <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          3  146
Jun 29 20:56:51  eap-resp        ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          3  61
Jun 29 20:56:51  rad-req         ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1  44 270  10.1.140.101
Jun 29 20:56:51  rad-resp        <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1  44  128
Jun 29 20:56:51  eap-req         <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          4  46
Jun 29 20:56:51  eap-resp        ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          4  46
Jun 29 20:56:51  rad-req         ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1  45  255 10.1.140.101
Jun 29 20:56:51  rad-accept      <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1  45  231
Jun 29 20:56:51  eap-success     <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          4  4
Jun 29 20:56:51 user repkey change * 70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0      65535  -   204c0306e790000000170008
Jun 29 20:56:51 macuser repkey change * 70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0  65535  -  70:4d:7b:10:9e:c6
Jun 29 20:56:51  wpa2-key1       <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          -   117
Jun 29 20:56:51  wpa2-key2       ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          -   117
Jun 29 20:56:51  wpa2-key3       <-   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          -   151
Jun 29 20:56:51  wpa2-key4       ->   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          -   95
```

A network administrator is validating client connectivity and executes the `show` command shown in the exhibit. Which authentication method was used by the wireless station?

A. 802.1X user authentication
B. EAP authentication
C. 802.1X machine authentication
D. MAC authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A network administrator deplos a guest solution over WiFi and creates a corp_guest role for this purpose. The network administrator must configure the solution with a custom policy that permits visitors to get an IP address, perform DNS resolutions, and get internet access while blocking any attempt to reach internal resources at the 10.0.0.0/8 network. The solution should prevent visitors from acting as rogue DHCP servers, then blacklist and log the attempt if this ever happens.

Which setup meets these requirements?

A. netdestination corporate_network
network 10.0.0.0 255.0.0.0
ip access-list session corp_guests
user any udp 68 deny log blacklist
any any svc-dhcp permit user alias
coroporate_network deny user any
any permit

user-role Corp_guest access-
list session corp_guests

B. netdestination corporate_network
network 10.0.0.0 255.0.0.0

ip access-list session corp_guests
any any udp 68 deny log blacklist
any any svc-dhcp permit user alias
coroporate_network deny user any
any permit

user-role Corp_guest access-
list session corp_guests

C. netdestination corporate_network
network 10.0.0.0 255.0.0.0

ip access-list session corp_guests
user any udp 67 deny log blacklist
any any svc-dhcp permit user alias
coroporate_network deny user any
any permit

user-role Corp_guest access-
list session corp_guests

D. netdestination corporate_network
network 10.0.0.0 255.0.0.0

ip access-list session corp_guests
any any udp 67 deny log blacklist
any any svc-dhcp permit user alias
coroporate_network deny user any
any permit

user-role Corp_guest access-
list session corp_guests

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 Refer
to the exhibits.

Exhibit 1

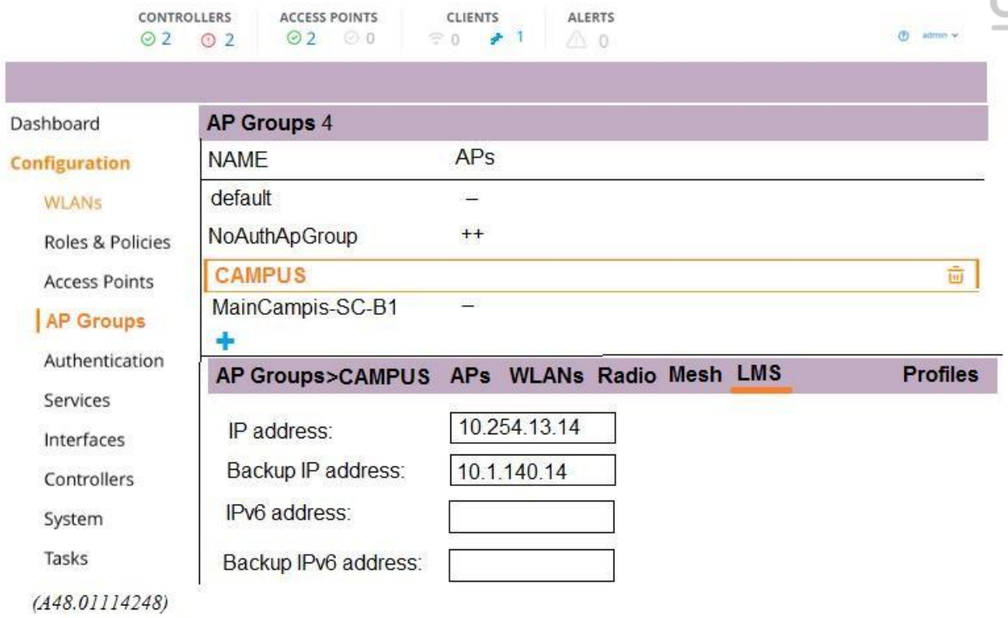
```
(MC14-2) #show ip interface brief | exclude unassigned

Interface     IP Address  / IP Netmask        Admin          Protocol     VRRP-IP
vlan 140      10.1.140.101 / 255.255.255.0        up          up           10.1.140.14
vlan 143      192.168.14.1 / 255.255.255.0        up          up
(MC14-2) #
(MC14-2) #show lc-cluster group-membership | exclude %

Cluster Enabled, Profile Name = "Cluster 2"
Redundancy Mode On
AP Load Balancing: Disabled
Cluster Info Table
-------------------------
Type  IPv4  Address   Priority  Connection-Type  STATUS
------- --------------------- ------------- ------------------------------ -------------
peer  10.1.140.100          128  L2-Connected   CONNECTED (Member, last HBT_RSP 85ms ago, RTD = 0.504 ms)
self  10.1.140.101          128          N/A    CONNECTED (Leader)
(MC14-2) #
(MC14-2) #show ap database | exclude "="

AP Database
------------------
Name  Group        AP Type      IP Address   Status          Flags  Switch IP       Standby IP
-------- --------------  -------------  ---------------  ----------  -------  -----------------  -------------------
AP11  CAMPUS     335          10.1.145.150  Up 27m:53s          10.1.140.101 10.1.140.100
AP12  CAMPUS     335          10.1.146.150  Up 28m:14s          10.1.140.101 10.1.140.100
```

Exhibit 2



A network administrator deploys a test environment with two Mobility Masters (MMs), two two-member Mobility Controller (MC) clusters, and two CAPs, with the intention of testing several ArubaOS features, Cluster members run VRRP for AP boot redundancy. Based on the information shown in the exhibits, what is the current status of the APs?

A. APs are currently communicating with LMS IP, and 10.1.140.100 is S-AAC.

B. APs are currently communicating with BLMS IP, and 10.1.140.101 is A-AAC.C. APs are currently communicating with BLMS IP, and 10.1.140.101 is S-AAC.

D. APs are currently communicating with BLMS IP, and 10.1.140.100 is A-AAC.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Refer to the exhibit.

(A48.0.1114234)

A network administrator wants to configure an 802.1x supplicamt for a wireless network that includes the following:
- AES encryption
- EAP-MSCHAP v2-based user and machine authentication
- Validation of server certificate in Microsoft Windows 10

The network administrator creates a WLAN profile and selects the change connection settings option. Then the network administrator changes the security type to Microsoft: Protected EAP (PEAP), and enables user and machine authentication under Additonal Settings.

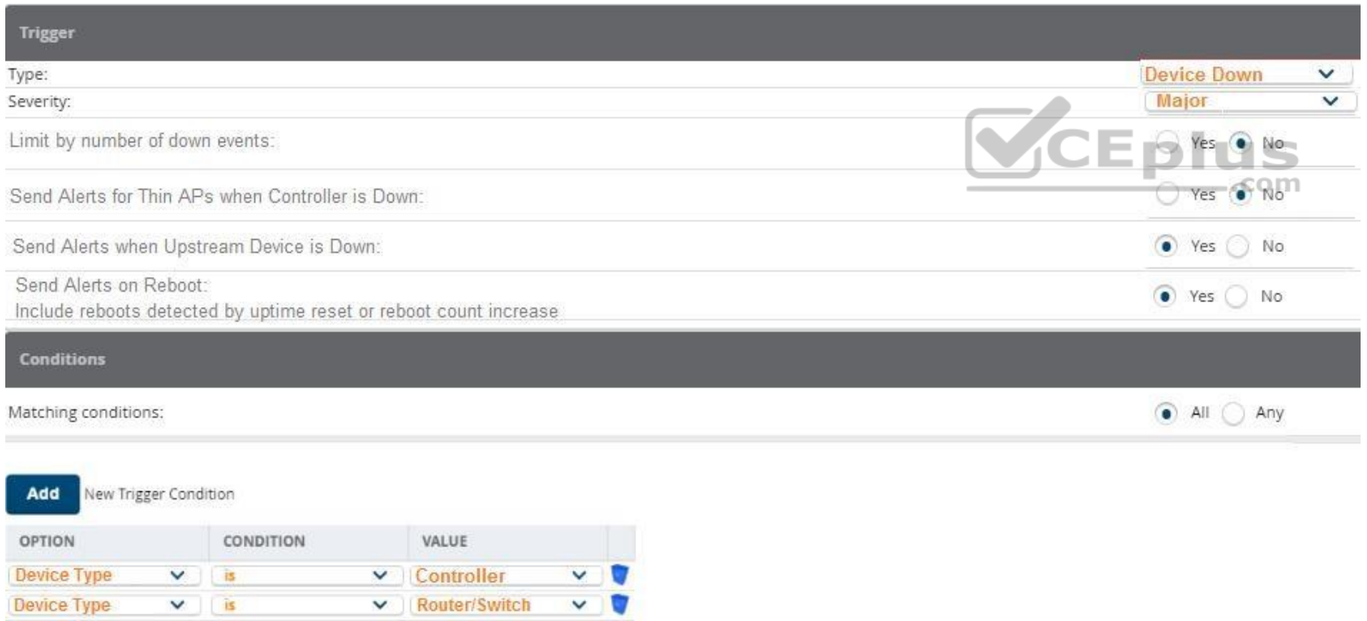
What must the network administrator do next to accomplish the task?

A. Enable user authentication under Settings.
B. Change the security type to Microsoft. Smart Card or other certificate.
C. Enable server certificate validation under Settings.
D. Enable computer autentication under Settings.

Correct Answer: B
Section: (none)
Explanation

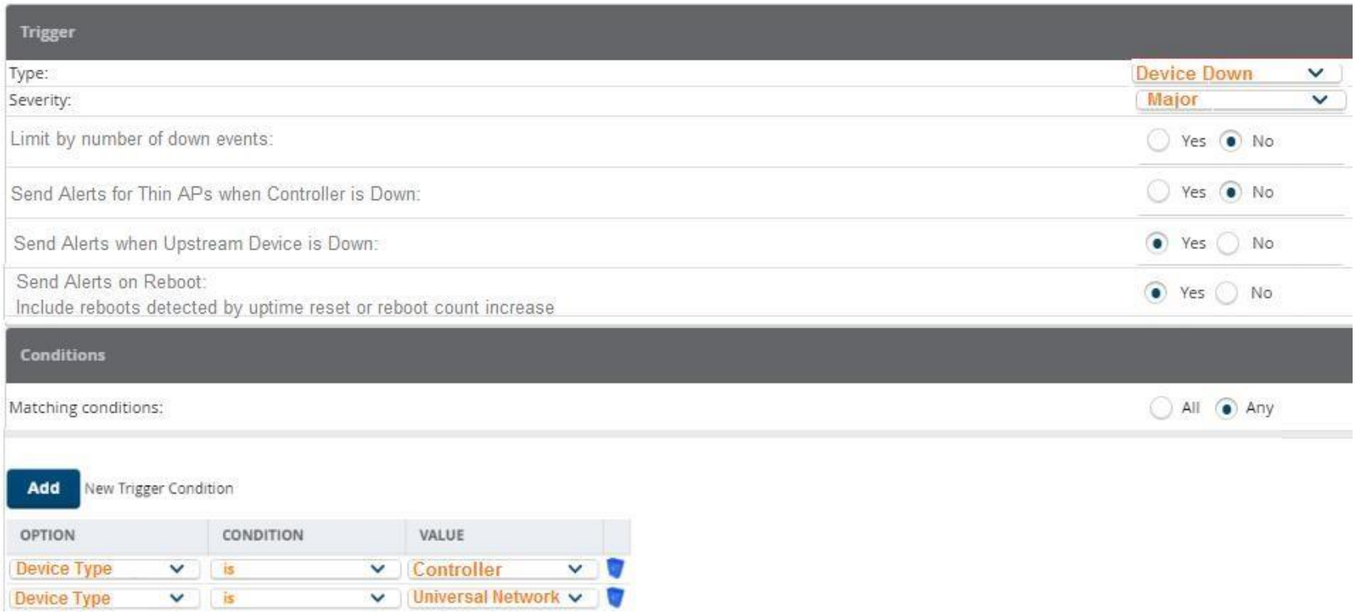
Explanation/Reference:

QUESTION 42
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.

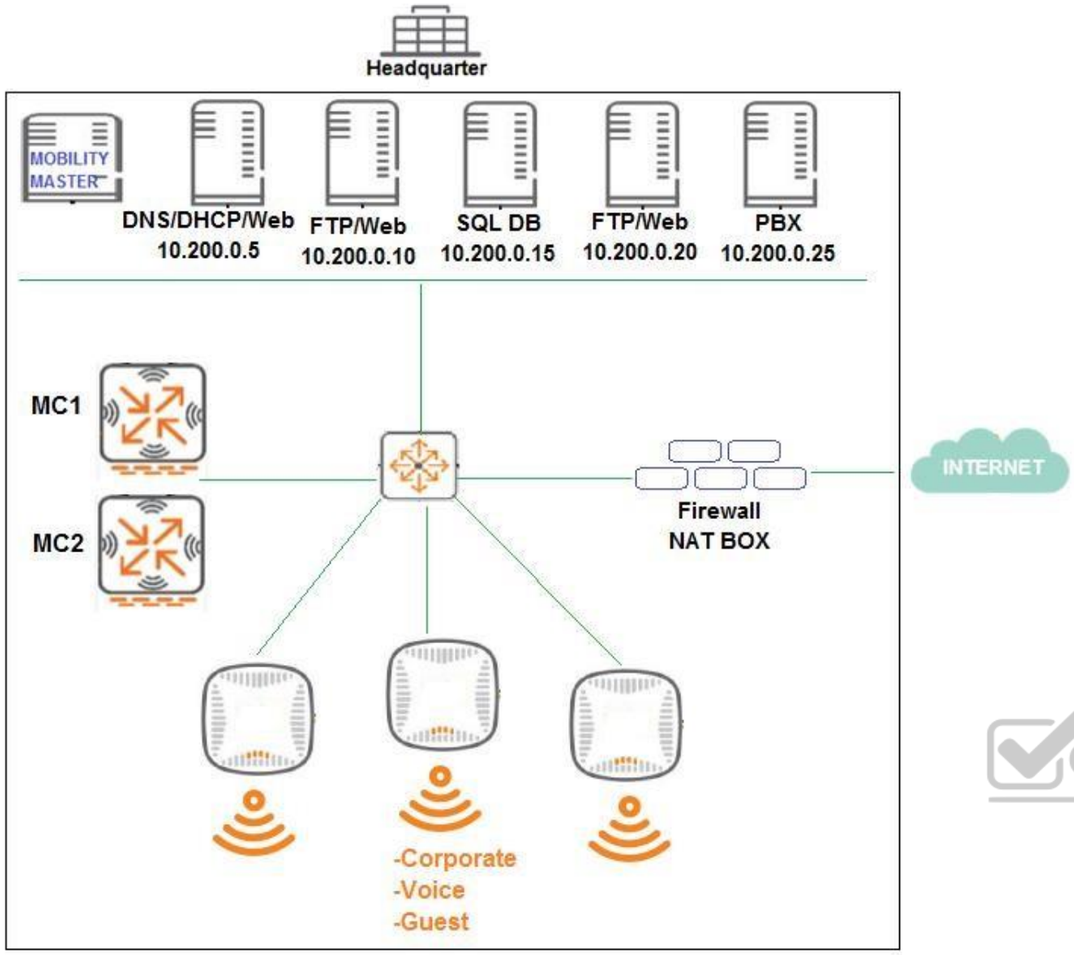
B.

C. 

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 Refer
to the exhibits.

Exhibit 1

(MC1) [MDC] #show ip interface brief

Interface	IP Address / IP Netmask	Admin	Protocol	VRRP-IP
vlan 140	10.1.140.100 / 255.255.255.0	up	up	
vlan 1	unassigned / unassigned	down	down	
loopback	10.1.140.99 / 255.255.255.255	up	up	

Exhibit 2

Auth Servers | AAA Profiles | L2 Authentication | L3 Authentication | User Rules | **Advanced**

> Survivability

> Authentication Timers

v **RADIUS Client**

NAS IPv4 address: 10.1.140.101

Source interface v4: Loopback v

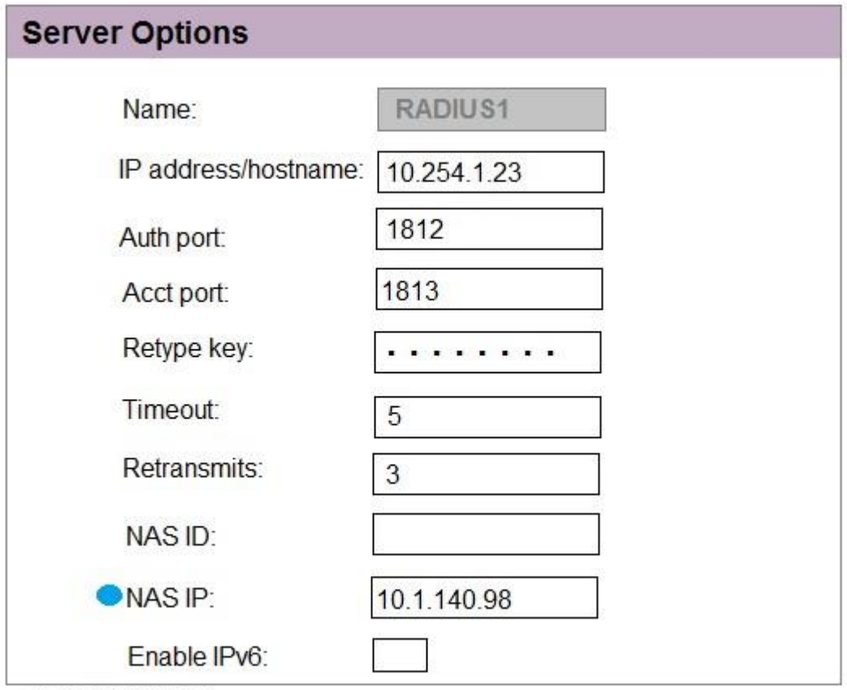
NAS IPv6 address:

Source interface v6: None v

> DNS Query Interval

(A48.01114254)

Exhibit 3



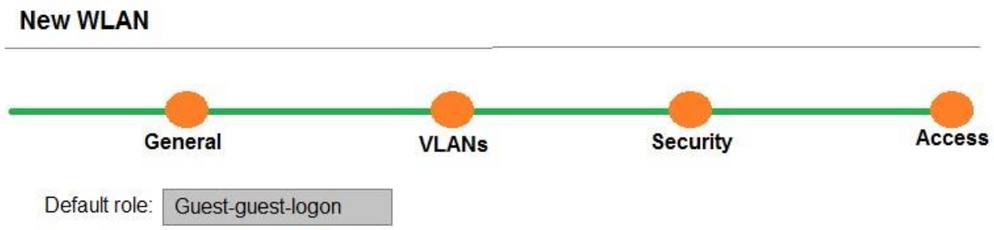
(A48.01114850)

A network administrator must ensure that a ClearPass server can receive the RADIUS authentication request from a single Mobility Controller (MC) managed by a Mobility Master (MM). Based on the exhibits, what is the value of NAS-IP contained in the RADIUS access requests?

A. 10.1.140.98
B. 10.1.140.99
C. 10.1.140.100D. 10.1.140.101 **Correct Answer:** A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Refer to the exhibit.



(A48.01114253)

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.

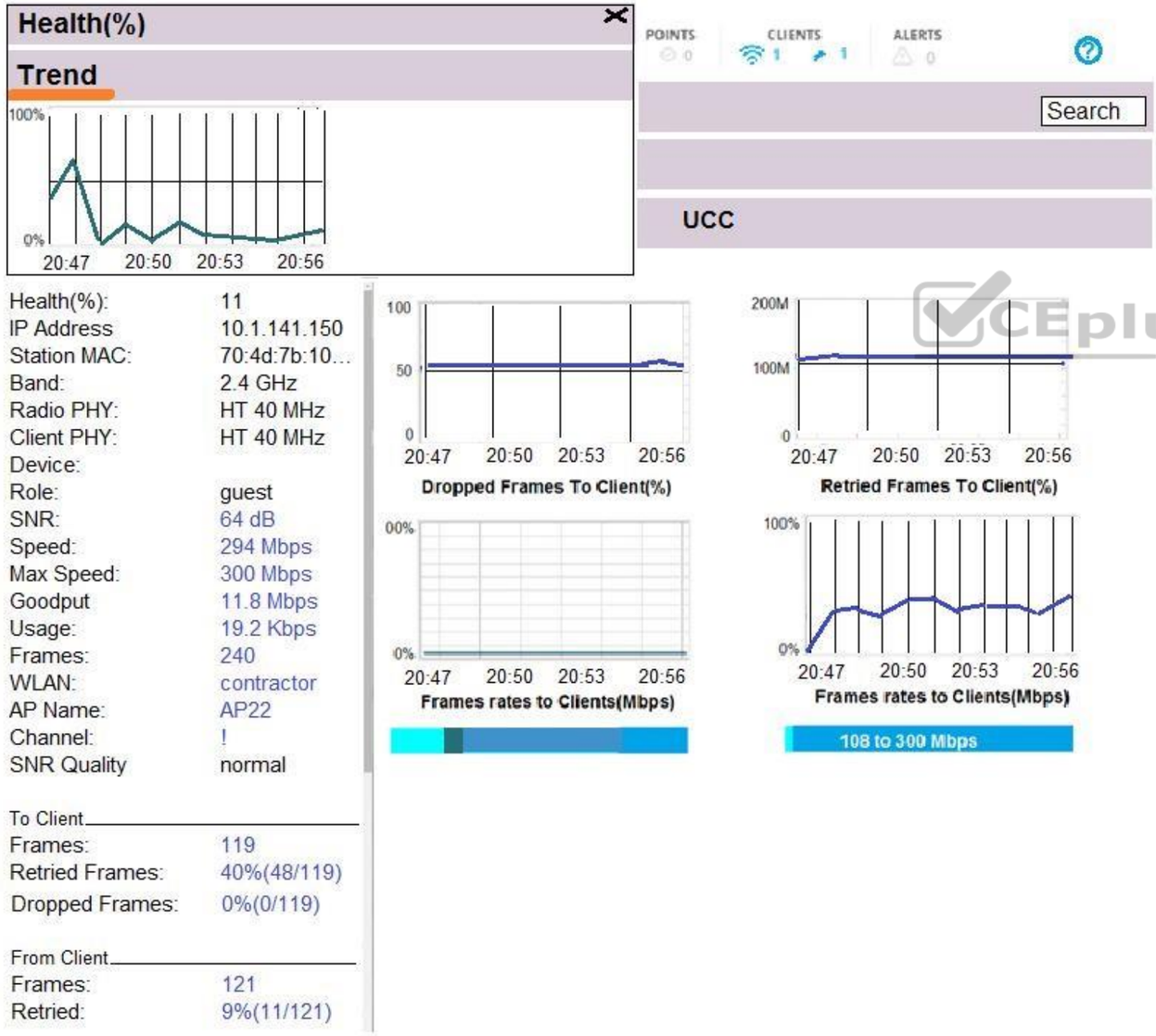
Which additional step must the network administrator complete in order to prevent authenticated users from reaching internal corporate resources while allowing Internet access?

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Refer to the exhibit.



A user's laptop only operates in the 2.4 GHz band and supports 802.11n. This user reports that the network is slow at the cafeteria that is serviced by three APs, and suggests that there might be a problem with the WLAN. The network administrator finds the user in the MM, and obrains the output shown in the exhibit.

What should the network administrator do to optimize the client connection?

A. Disable lower transmit rates in the SSID profile.
B. Change the channel being used in the radio profile.
C. Reduce Min/Max channel bandwidth in the radio profile.
D. Reduce Min/Max EIRP in the ARM profile.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 47
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
Section: (none)
Explanation

Explanation/Reference:

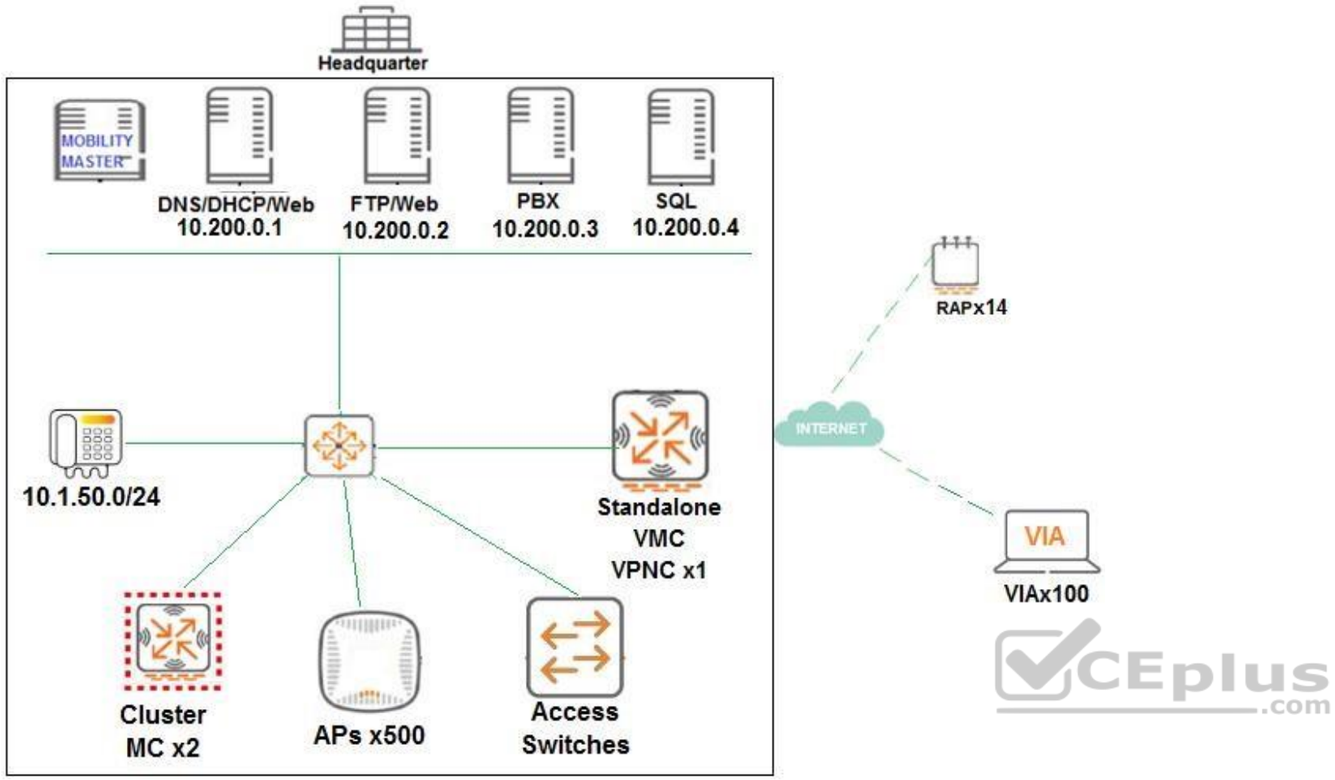
QUESTION 48
A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM)-Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

- RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access.
- Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ

▪ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment ▪ Local Internet access should be granted.

Refer to the exhibit.



Refer to the scenario and the exhibit.

```
(MC2) [MDC] #show ip access-list split-tunneling

ip access-list session split-tunneling
split-tunnelimg
------------------------
Priority    Source          Destination                 Service     Application  Action   TimeRange
------------  ------------  ---------------------       ------------ ----------------- ----------- -------------------
1           any             any                         svc-dhcp                         permit

Log   Expired    Queue       TOS    8021P  Blacklist  Mirror DisScan    IPv4/6
--------- ----------  -----------  --------- ----------  ------------  ----------------------  -------------
                 Low                                                                  4
2          user                10.200.0.0.255.255.255.252   any                      permit

                 Low                                                                  4
3       10.200.0.0 255.255.255.252  user                        any                    permit

                 Low                                                                  4
4          user                10.1.50.0 255.255.255.0          svc-rtsp               permit

                 Low                                                                  4
5          user                10.1.50.0 255.255.255.0          svc-sip-udp            permit

                Low                                                                   4
6          10.1.50.0 255.255.255.0  user                        svc-rtsp               permit

                Low                                                                   4
7          10.1.50.0 255.255.255.0  user                        svc-sip-udp            permit

                Low                                                                   4
```

Which command must the network administrator add in the split-tunneling policy to meet the requirements for the RAP employee SSID?

A. `user any svc-http permit`
B. `user any any src-nat pool dynamic-srcnat`
C. `any user any src-nat pool dynamic-srcnat`
D. `user any any dst-nat`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

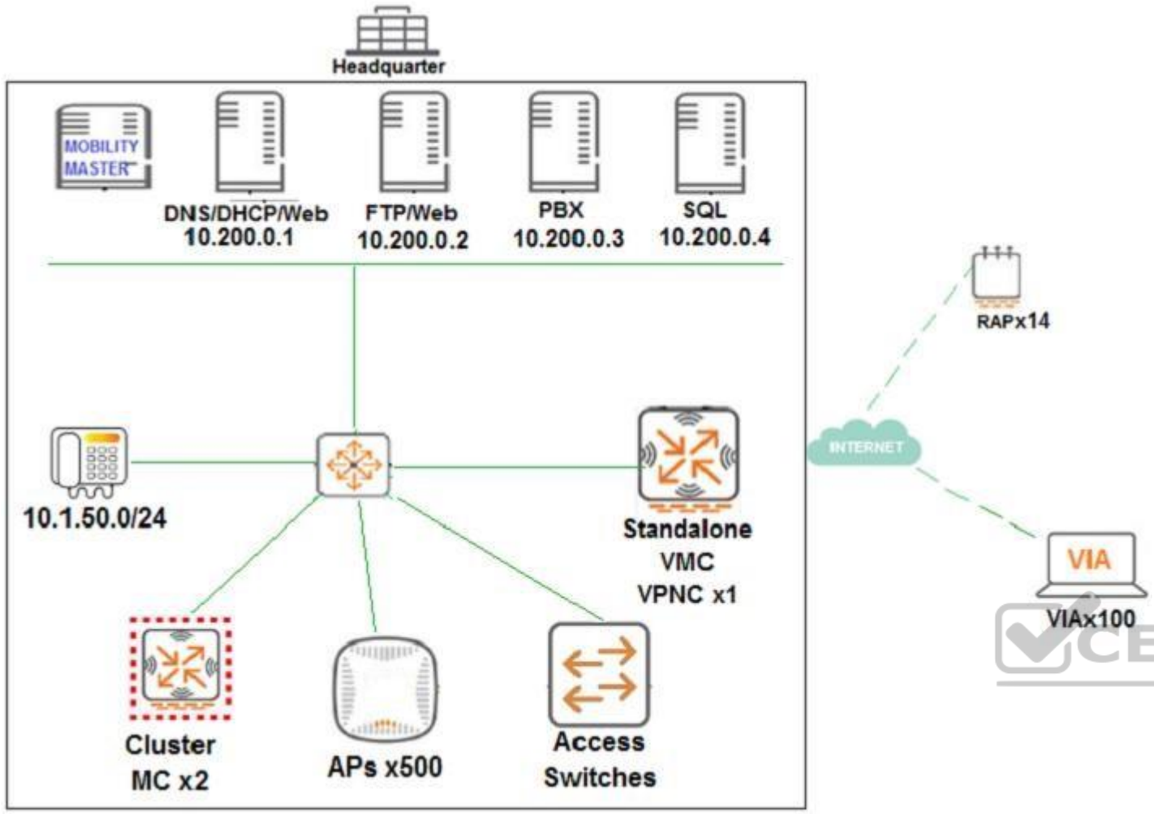
QUESTION 49
A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM)-Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

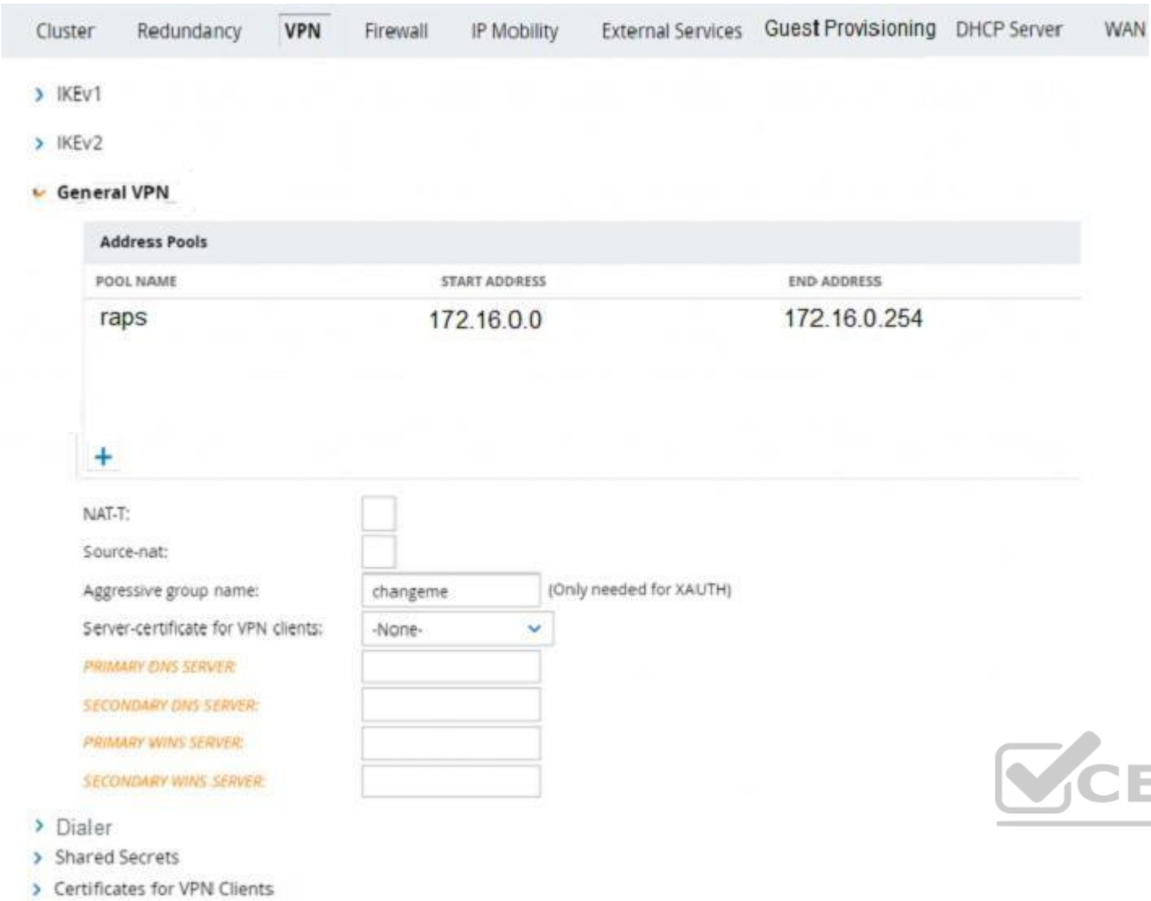
- RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access.

▪ Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ
▪ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. ▪ Local Internet access should be granted.

Refer to the exhibit.



Refer to the scenario and the exhibit.



The standalone VMC will act as a VPN Concentrator of the RAPs. The network administrator configures the Standalone VMC with a pool of addresses and the SOHOs AP Group from the MM.

Which additional steps must the network administrator perform to allow the RAPs to terminate their IPSec tunnels and associate to the Standalone VMC?

A. Add RAP MAC addresses into the RAP whitelist, and associate them with the SOHOs AP-Group.
B. Add RAP MAC addresses into the CPSec whitelist, and associate them with the SOHOs AP-Group.
C. Configure the same IP Pool at the MM group level, then create user accounts for the RAPs in the internal database.
D. Create user accounts with the sys-ap-role, and define shared secrets to associate to RAP IP addresses at the MM group level.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

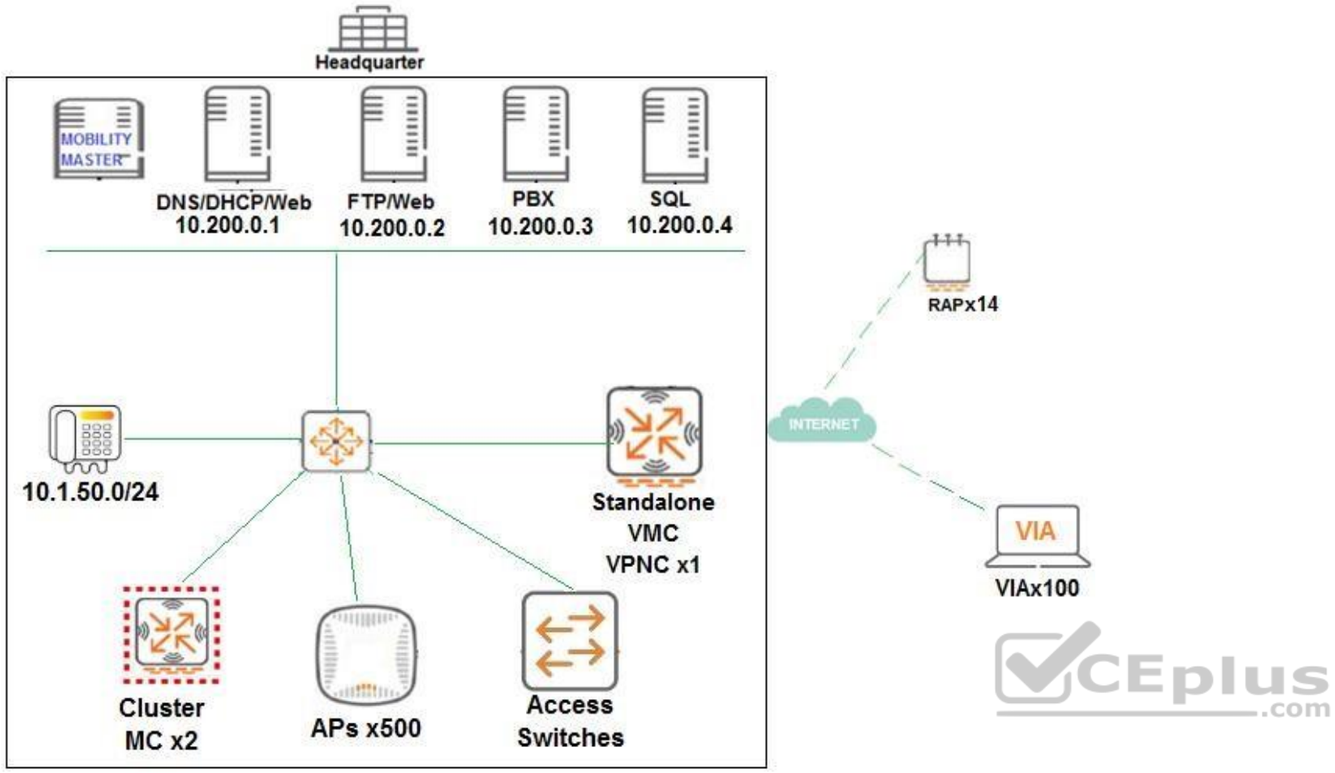
QUESTION 50
A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM)-Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

- RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access.
- Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ

▪ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment ▪ Local Internet access should be granted.

Refer to the exhibit.



Refer to the scenario and the exhibit.

What is the minimal license capacity in use to support this proposal? A.

License	Number
MM-VA	502
Access Points	514
PEF	514
RF Protect	514
VIA	100

B.

License	Number
MM-VA	503
MC-VA	14
Access Points	514
PEF	514
VIA	100

License	Number
MM-VA	517
MC-VA	114
Access Points	514
PEF	514
VIA	100

C.

License	Number
MM-VA	502
MC-VA	14
Access Points	514
PEF	514
RF Protect	500
VIA	100

D.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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.

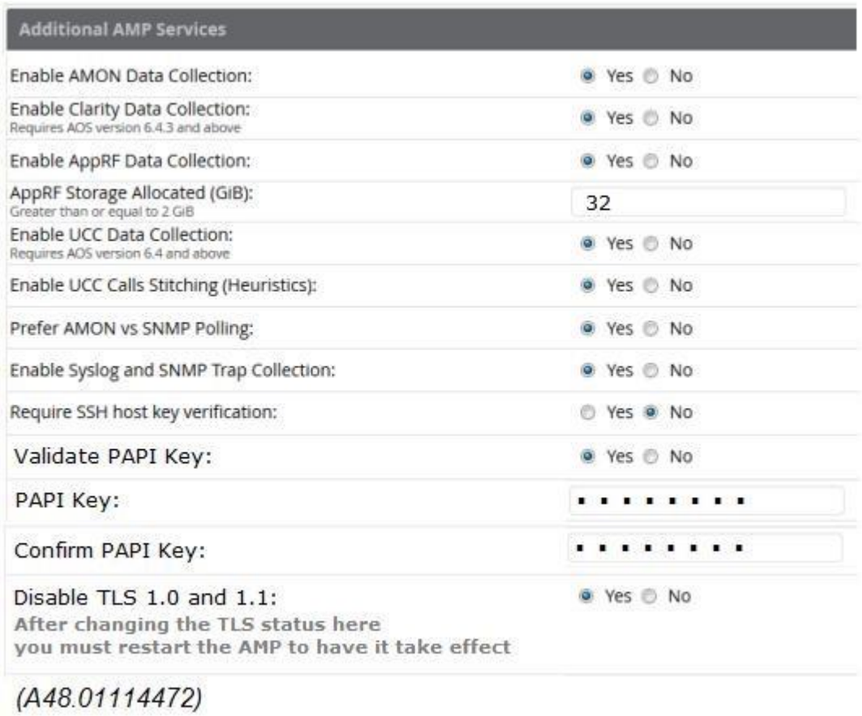
What could be the cause of the problem that the users reported?

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Refer to the exhibit.



A network administrator configures a Mobility Master (MM)-Mobility Controller (MC) solution and integrates it with AirWave. The network administrator configures the SNMP and terminal credentials in the MM and MC, and then monitors the mobility devices from AirWave, including Clarity for user association and basic network services verification. However, AirWave does not display any UCC data that is available in the MM dashboard.

Based on the information shown in the exhibit, which configuration step should the network administrator do next in the MM to complete the integration with AirWave?

A. Define AirWave as a management server in the MM.
B. Enable the inline network services statistics in the AMP profile.
C. Enable UCC monitoring in the AMP profile.
D. Verify the papi-security key in the AMP profile.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Refer to the exhibit.

```
(MC14-1) [MDC] #show iap table long

Trusted Branch Validation:      Enabled
IAP  Branch Table
-------------------------
Name VC  MAC Address  Status  Inner IP     Assigned Subnet   Assigned Vlan     Key                                                    Bid(Subnet Name)
                                                Tunnel End Points
-------- ----------------------- --------- ------------     ----------------------- ----------------------     ---------                                              ----------------------------
                                                                                    -------------------------

IAP-1  a8:bd:27:c5:c3:3a UP     2.2.2.2                  10.21.124.32/27     25          1f70772b01fdc02472357885f21393a9120e1823e154e98839  0(10.21.124.1-10.21.1
24.254,16), 0 (10.25.16.2-10.25.23.254,110:25)

Total No of UP Branches         :1
Total No of DOWN Branches       :0
Total No of Branches            :1
```

A network administrator configures an Instant AP (IAP) to establish an Aruba IPSec tunnel across the Internet, and configures two DHCP pools for wireless users.

Based on the output shown in the exhibit, which device behaves as a DHCP server for the users?

A. Mobility Master
B. Mobility Controller
C. External server
D. DSL modem
E. Virtual Controller

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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 policies 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 ports to the MMs except UDP 500 and 4500.
C. Install a PEFV license, and configure firewall policies that protect the MM.
D. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Refer to the exhibit.

```
(MC14-1) #show log security 180

Jul 16 01:09:55    :124004:    <3573> <DBUG> |authmgr| Select server for method=802.1x,
user=host/wireless14.training.arubanetworks.com, essid=Corp-network, server-group=CAMPUS, last_srv <>
Jul 16 01:09:55    :124038:    <3573> <INFO> |authmgr| Reused server ClearPass for method=802.1x;
user=host/wireless14.training.arubanetworks.com, essid Corp-network, domain=<>, server-group=CAMPUS
Jul 16 01:09:55    :124004:    <3573> <DBUG> |authmgr| aal_auth_raw (1399) (INC) : os_auths 1, s ClearPass type 2 inservice 1
markedD 0 sg_name CAMPUS
Jul 16 01:09:55    :124004:    <3573> <DBUG> |authmgr| aal_auth_raw (1402) (INC) : os_reqs 1, s ClearPass type 2 inservice 1 markedD
0
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=18, server=ClearPass, IP=10.254.1.23,
server-group=CAMPUS, fd=87
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass: 10.254.1.23:1812
id:18, len:249
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name:
host/wireless14.training.arubanetworks.com
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-IP-Address: 10.254.10.214
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Id: 0
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Identifier: 10.1.140.100
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Calling-Station-Id: 704D7B109EC6
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 204C0306E5C0
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Service-Type: Framed-User
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Framed-MTU: 1100
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] EAP-Message: \002\006
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Essid-Name: Corp-network
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Location-Id: AP21
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-AP-Group: CAMPUS
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2381] Aruba-Device-Type: (VSA with invalid
length – Don't send it)
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Message-Auth: phu\025\347\376\016\030
\253a-\014a\033\200\234
Jul 16 01:09:55    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_sequence.c:117] seq_num_timeout_handler: Freed 0
entries
Jul 16 01:10:00    :124004:    <3573> <WARN> |authmgr| |aaa| RADIUS server ClearPass server-group CAMPUS –
10.254.1.23-1812 timoeout for client=70:4d:7b:10:9e:c6 auth method 802.1x
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_server.c:1203] Sending radius request to ClearPass
server-group CAMPUS -10.254.1.23-1812 (retry1)
Jul 16 01:10:00    :124004:    <3573> <DBUG> |authmgr| APAE_Aborting_Tineout (5076) (DEC) : os_auths 0, s ClearPass
type 2 inservice 1 markedD 0 sg_name CAMPUS
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_request.c:95] Find Request: id=18, server=(null), IP=
10.254.1.23, server-group=(null) fd=87
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_request.c:104] Current entry: server= (null), IP=
10.254.1.23, server-group=(null), fd=87
Jul 16 01:10:00    :121014:    <3573> <ERRS> |authmgr| |aaa| Received invalid reply digest from RADIUS server
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc_request.c:48] Del Request: id=18, server=ClearPass, IP=
10.254.1.23, server-group=CAMPUS fd=87
Jul 16 01:10:00    :121031:    <3573> <DBUG> |authmgr| |aaa| [rc api.c:1228] Bad or unknown response from AAA server
```

A network administrator deploys a new WLAN named Corp-Network. The security suite is WPA2 with 802.1X. A new ClearPass server is used as the authentication server. Connection attempts to this WLAN are rejected, and no trace of the attempt is seen in the ClearPass Policy Manager Access Tracker. However, the network administrator is able to see the logs shown in the exhibit.

What must the network administrator do to solve the problem?

A. Add the correct network device IP address in ClearPass.
B. Change the ClearPass server IP address in the MC.
C. Fix the RADIUS shared secret in the MC.
D. Disable machine authentication in the MC and client PC.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A network administrator needs to deploy L2 Mobility Master (MM) redundancy. MM1 uses IP address 10.201.0.10 and MAC address 1c:98:ec:25:48:50, and MM2 uses IP address 10.201.0.20 and MAC 1c:98:ec:99:8a:80. Both run VRRP process with VRID 201.

Which configuration should the network administrator use to accomplish this task?

A. /mm (MM1): database synchronize
period 30

/mm/mynode (MM1): master-
redundancy master-vrrp 201
peer-ip-address 10.201.0.20 ipsec key123

/mm/mynode (MM2): master-
redundancy master-vrrp 201
peer-ip-address 10.201.0.10 ipsec key123

B. /mm (MM1):

master-redundancy master-
vrrp 10
peer-ip-address 10.201.0.20 ipsec key123

database synchronize period 30

/mm/mynode (MM2): master-
redundancy master-vrrp 201
peer-ip-address 10.201.0.10 ipsec key123

C. /mm/mynode (MM1):

master-redundancy master-
vrrp 201
peer-ip-address 10.201.0.20 ipsec key123

database synchronize period 30

/mm/mynode (MM2): master-
redundancy master-vrrp 201
peer-ip-address 10.201.0.20 ipsec key123
database synchronize period
30 D. /mm (MM1): database
synchronize period 30 /mm/mynode
(MM1): master-redundancy master-
vrrp 201 peer-ip-address
10.201.0.10 ipsec key123

```
/mm/mynode (MM2): master-redundancy
master-vrrp 201 peer-ip-address
10.201.0.20 ipsec key123
```

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Refer to the exhibit.

```
(MC14-1) #show ap database | exclude =

AP Database
-----------
Name                Group      AP Type    IP Address       Status       Flags  Switch IP      Standby IP
---------           ---------  ---------- ---------------- ------------ ------ -------------- ---------------
70:3a:0e:cd:b0:a4   default     335       10.1.145.150     Up 3m:4s     IL     10.1.140.100   0.0.0.0
70:3a:0e:cd:b0:ac   default     335       10.1.146.150     Up 3m:12s    IL     10.1.140.100   0.0.0.0

Total APs:2
(MC14-1) #
(MC14-1) #show license client-table

Built-in limit: 0
License Client Table
--------------------------
Service Type                                      System Limit  Server Lic.  Used Lic.   Remaining Lic.  FeatureBit
-----------                                       ------------  -----------  ---------   --------------  ----------
Access Points                                     64            7            0           7               enabled
Next Generation Policy Enforcement Firewall Module 64           7            0           7               enabled
RF Protect                                        64            7            0           7               enabled
Advanced Cryptography                             4096          0            0           0               disabled
WebCC                                             64            0            0           0               disabled
MM-VA                                             65            0            1           0               enabled
MC-VA-RW                                          64            0            0           0               disabled
MC-VA-EG                                          64            0            0           0               disabled
MC-VA-IL                                          64            0            0           0               disabled
MC-VA-JP                                          64            0            0           0               disabled
MC-VA-US                                          64            0            0           0               disabled
VIA                                               4096          0            0           0               disabled
(MC14-1) #
(MC14-1) #show version | include Aruba

Aruba Operating System Software.
ArubaOS (MODEL: Aruba7030-US), Version 8.2.1.0
(MC14-1) #
```

A network engineer configures some VAPs in customer groups and creates a pool of licenses with enough units for seven APs. The network engineer deploys the first two APs, looks at the ap database, and notices the APs are inactive and experience licensing-related issues.

Based on the `show` command outputs shown in the exhibit, what must the engineer do to solve the problem?

A. Allocate two more MM-VA licenses to the pool.
B. Allocate two more MC-VA-US licenses to the pool.
C. Allocate seven more MM-VA licenses to the pool.
D. Allocate seven more MC-VA-US licenses to the pool.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Refer to the exhibit.

```
(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
-----------------------  ------------------  -----------  ---------  ----------------  --------  ------------  ----------  ----------------
------------------
10.1.141.150            70:4d:7b:10:9e:c6 it                guest           00:00:00   802.1x                AP22       Wireless
Corp-employee/70:3a:0e:5b:0a:c2/g-HT                Corp-Network tunnel                Win 10
WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:3/40 Free:0/37 Dyn:3 AllocErr:0 FreeErr:0
(MC2) [MDC] #show user mac 70:4d:7b:10:9e:c6
This operation can take a while depending on  number of users. Please be patient. . . .

Name: it, IP: 10.1.141.150, MAC: 70:4d:7b:10:9e:c6, Age: 00:00:00
Role: guest (how: ROLE_DERIVATION_DOT1X), ACL: 7/0
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: ClearPass.23
Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Role Derivation: ROLE DERIVATION DOT1X
```

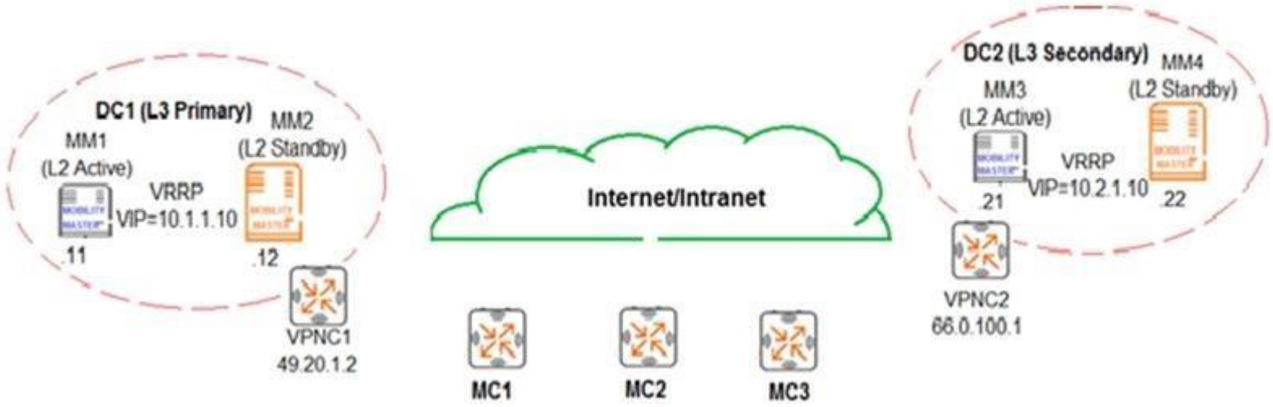
A network administrator evaluates a deployment to validate that users are assigned to the proper roles. Based on the output shown in the exhibit, what can the network administrator conclude?

A. The MC assigned the machine authentication default user role.
B. The MC assigned the role based on user-derivation rules.
C. The MC assigned the role based on server-derivation rules.
D. The MC assigned the default role of the authentication method.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Refer to the exhibit.



An Aruba network is deployed with L2 and L3 Mobility Master (MM) redundancy across two datacenters, as shown in the exhibit. The network administrator confirms that all Mobility Controllers (MC) are currently communicating with MM1, which is the L2 Active, and L3 Primary. Which MM IP will MCs communicate with if MM1 fails?

A. 10.1.1.10
B. 10.1.1.12
C. 10.2.1.10
D. 10.2.1.21

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference: