killexams.com

HP

HPE6-A48

Aruba Certified Mobility Expert (ACMX)

ORDER FULL VERSION

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.

Question: 87

Refer to the exhibits. Exhibit 1

CONTROLLERS | ACCESS POINTS | CLIENTS | ALERTS
1   !1   2   !0   1 0   0

> **MC14-1**

Name:	MC14-1
Reachability:	Unreachable
Health:	Good
Uptime:	-
Model:	Aruba7030-US
Serial Number:	CRDD12919
Country:	-
Group:	md > Westcoast > SantaClara > Building1
Configuration State:	-
Configuration Version:	-

(A48.01114452)

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, 0.1%wa, 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.
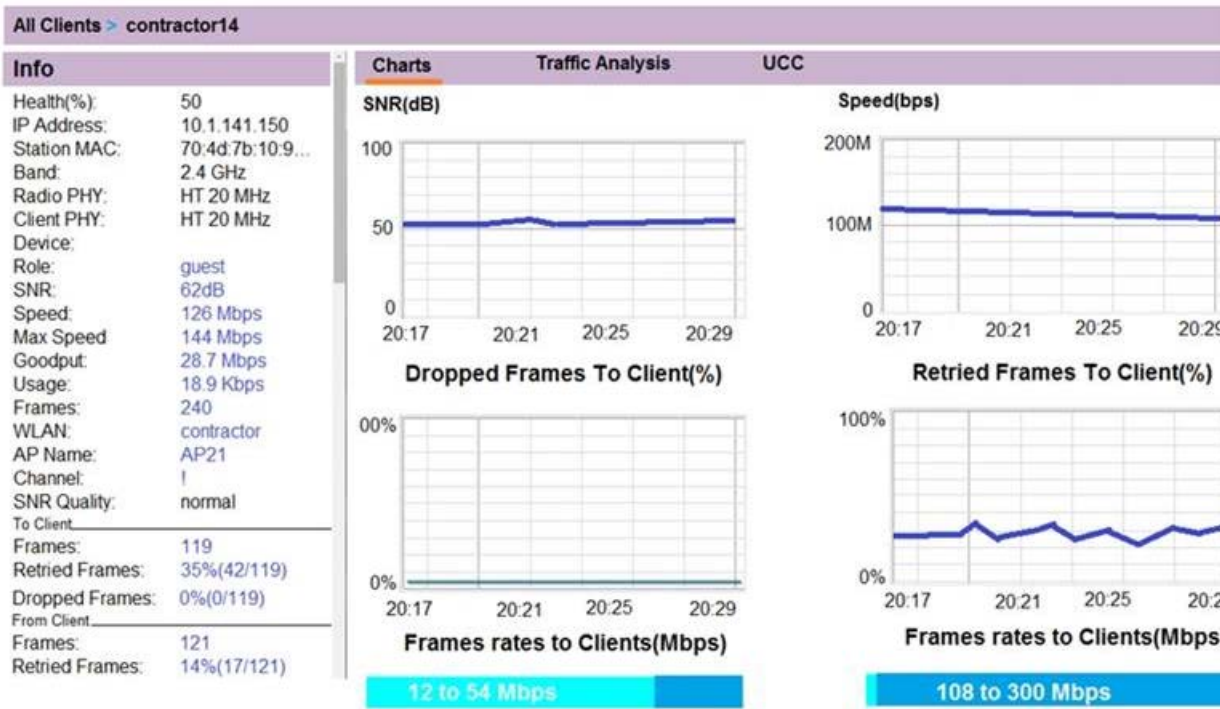
What should the network administrator do next to solve the current problem?
A . Decommission the MC from the MM, and add it again.
B . Open a TAC case, and send the output of tar crash.
C . Verify the license pools in the M
E . Kill two zombie processes, then reboot the M

Answer: D

Question: 88

Refer to the exhibit.

Info

Health(%):	50
IP Address:	10.1.141.150
Station MAC:	70:4d:7b:10:9...
Band:	2.4 GHz
Radio PHY:	HT 20 MHz
Client PHY:	HT 20 MHz
Device:	
Role:	guest
SNR:	62dB
Speed:	126 Mbps
Max Speed	144 Mbps
Goodput:	28.7 Mbps
Usage:	18.9 Kbps
Frames:	240
WLAN:	contractor
AP Name:	AP21
Channel:	!
SNR Quality:	normal

To Client

Frames:	119
Retried Frames:	35%(42/119)
Dropped Frames:	0%(0/119)

From Client

Frames:	121
Retried Frames:	14%(17/121)

(A48.01114413)

Charts   Traffic Analysis   UCC

SNR(dB) — 20:17, 20:21, 20:25, 20:29 (100 / 50 / 0)

Speed(bps) — 20:17, 20:21, 20:25, 20:29 (200M / 100M / 0)

Dropped Frames To Client(%) — 00%, 0% — 20:17, 20:21, 20:25, 20:29

Retried Frames To Client(%) — 100%, 0% — 20:17, 20:21, 20:25, 20:29

Frames rates to Clients(Mbps) — 12 to 54 Mbps

Frames rates to Clients(Mbps) — 108 to 300 Mbps

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.
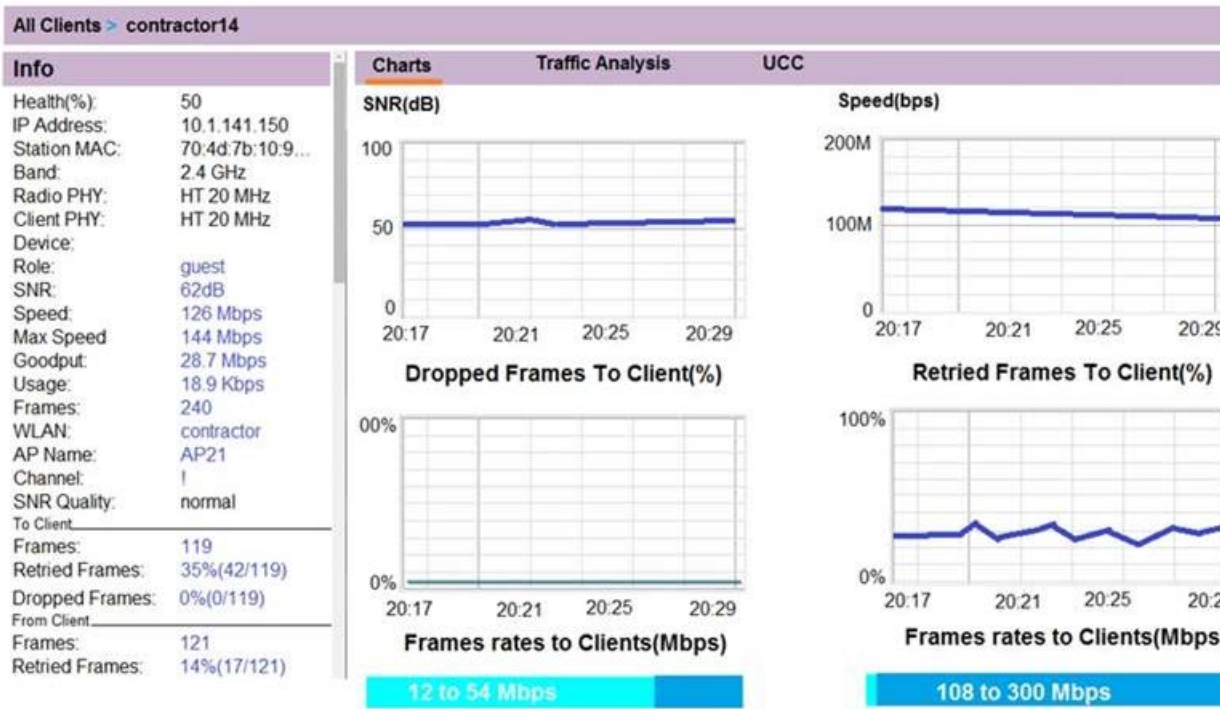
What can the network administrator conclude after analyzing the data?
A . Client health is low, and retried frames are high. It is possible there is high channel utilization.
B . Client health is low, but SNR is high. It is possible data in the dashboard is not accurate and needs to be updated.
C . The speed is good. Client health seems to be related to a problem with the client NI
E . The network is low because of low SN
F . TX power must be increased in both the client and the A

Answer: B

Question: 89

Refer to the exhibit.

Info

Health(%):	50
IP Address:	10.1.141.150
Station MAC:	70:4d:7b:10:9...
Band:	2.4 GHz
Radio PHY:	HT 20 MHz
Client PHY:	HT 20 MHz
Device:	
Role:	guest
SNR:	62dB
Speed:	126 Mbps
Max Speed	144 Mbps
Goodput:	28.7 Mbps
Usage:	18.9 Kbps
Frames:	240
WLAN:	contractor
AP Name:	AP21
Channel:	!
SNR Quality:	normal

To Client

Frames:	119
Retried Frames:	35%(42/119)
Dropped Frames:	0%(0/119)

From Client

Frames:	121
Retried Frames:	14%(17/121)

(A48.01114413)

Charts　　**Traffic Analysis**　　**UCC**

SNR(dB)

Speed(bps)

Dropped Frames To Client(%)

Retried Frames To Client(%)

Frames rates to Clients(Mbps)

12 to 54 Mbps

Frames rates to Clients(Mbps)

108 to 300 Mbps

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.
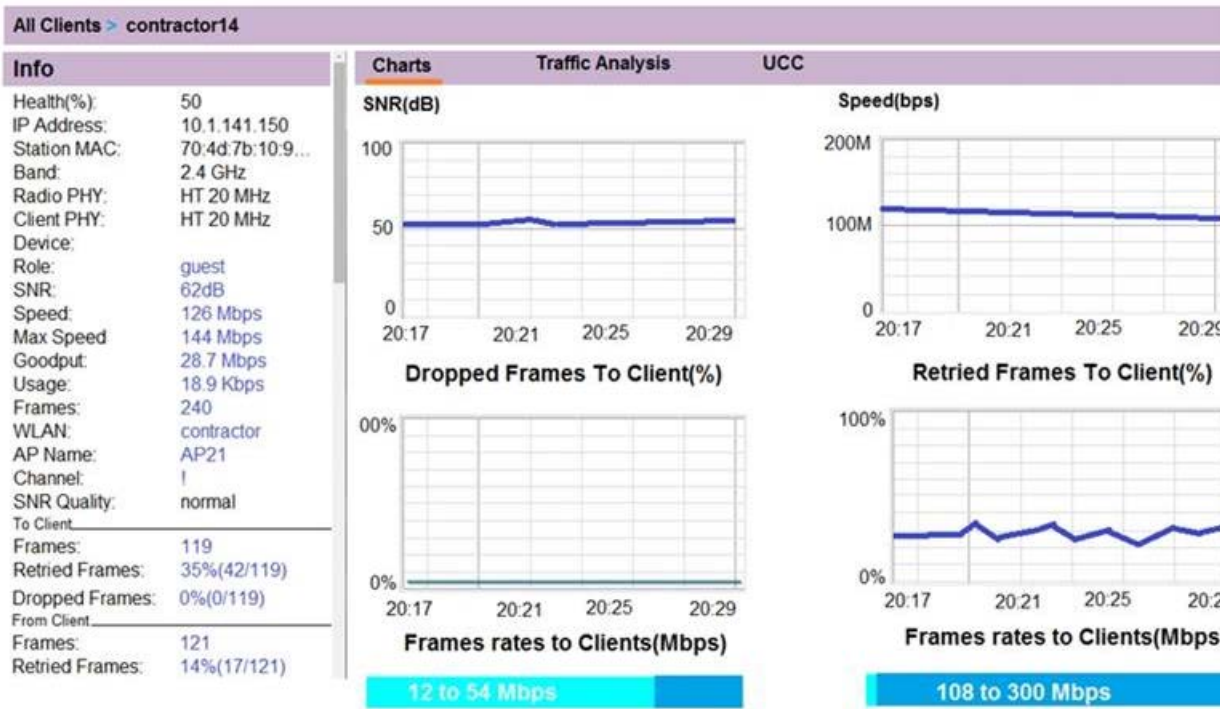
What can the network administrator conclude after analyzing the data?
A . Client health is low, and retried frames are high. It is possible there is high channel utilization.
B . Client health is low, but SNR is high. It is possible data in the dashboard is not accurate and needs to be updated.
C . The speed is good. Client health seems to be related to a problem with the client NI
E . The network is low because of low SN
F . TX power must be increased in both the client and the A

Answer: B

Question: 90

Refer to the exhibit.

Info

Health(%):	50
IP Address:	10.1.141.150
Station MAC:	70:4d:7b:10:9...
Band:	2.4 GHz
Radio PHY:	HT 20 MHz
Client PHY:	HT 20 MHz
Device:	
Role:	guest
SNR:	62dB
Speed:	126 Mbps
Max Speed	144 Mbps
Goodput:	28.7 Mbps
Usage:	18.9 Kbps
Frames:	240
WLAN:	contractor
AP Name:	AP21
Channel:	!
SNR Quality:	normal

To Client

Frames:	119
Retried Frames:	35%(42/119)
Dropped Frames:	0%(0/119)

From Client

Frames:	121
Retried Frames:	14%(17/121)

(A48.01114413)

Charts   Traffic Analysis   UCC

SNR(dB)

Speed(bps)

Dropped Frames To Client(%)

Retried Frames To Client(%)

Frames rates to Clients(Mbps)

12 to 54 Mbps

Frames rates to Clients(Mbps)

108 to 300 Mbps

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 NI
E . The network is low because of low SN
F . TX power must be increased in both the client and the A

Answer: B

Question: 91

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, 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.

Answer: B

Question: 92

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

Answer: C

Question: 93

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 M

D . Create server derivation rules in the server group.
E . Check the Download role from the CPPM option in the AAA profile.

Answer: A

Question: 94

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.
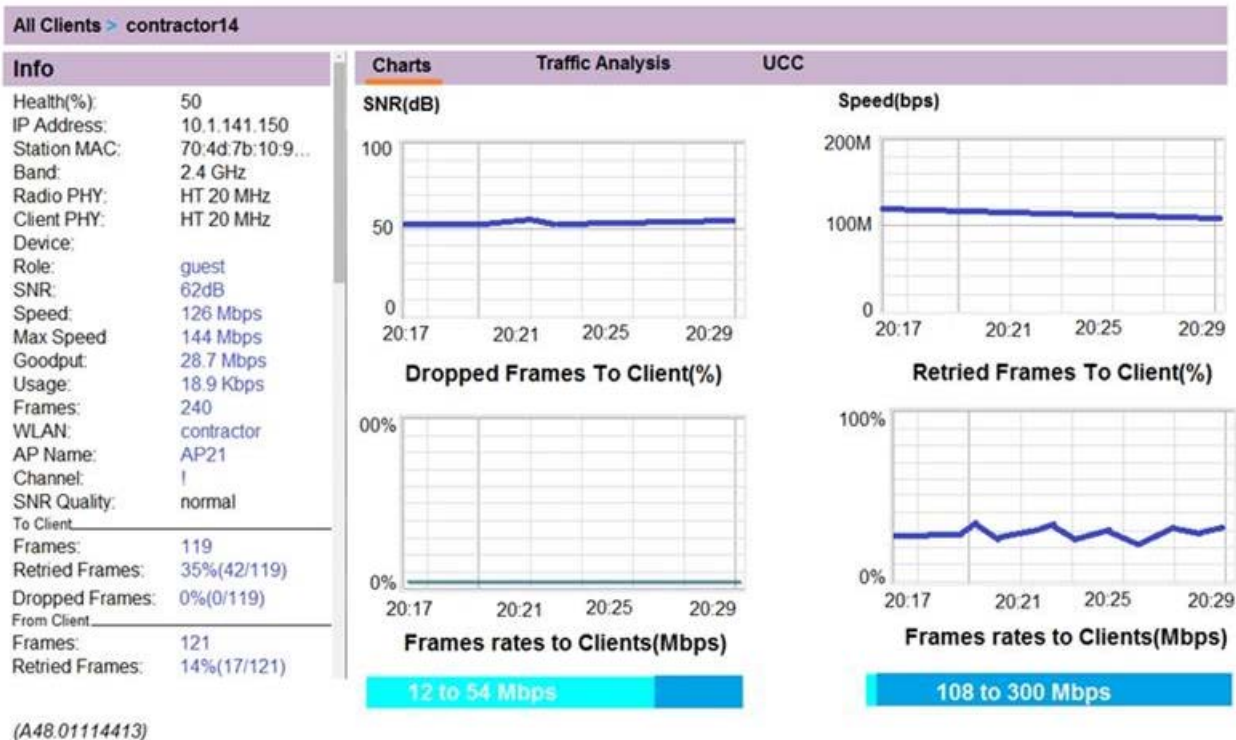
Based on the exhibit, what should the network administrator do next to fix this problem?
A . Confirm that AP12 is certified by the whitelist on MC1 and MC4, and confirm MC1 and MC4 are reachable by AP12.
B . Increase the number of nodes in zones 1 and 4, and confirm MC1 and MC4 are reachable by AP12.
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.

Answer: D

Question: 95

Refer to the exhibit.

All Clients > contractor14

Info	
Health(%):	50
IP Address:	10.1.141.150
Station MAC:	70:4d:7b:10:9...
Band:	2.4 GHz
Radio PHY:	HT 20 MHz
Client PHY:	HT 20 MHz
Device:	
Role:	guest
SNR:	62dB
Speed:	126 Mbps
Max Speed	144 Mbps
Goodput:	28.7 Mbps
Usage:	18.9 Kbps
Frames:	240
WLAN:	contractor
AP Name:	AP21
Channel:	1
SNR Quality:	normal

To Client
Frames:	119
Retried Frames:	35%(42/119)
Dropped Frames:	0%(0/119)

From Client
Frames:	121
Retried Frames:	14%(17/121)

(A48.01114413)

Charts   Traffic Analysis   UCC

SNR(dB)

Speed(bps)

Dropped Frames To Client(%)

Retried Frames To Client(%)

Frames rates to Clients(Mbps)

12 to 54 Mbps

Frames rates to Clients(Mbps)

108 to 300 Mbps

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 NI
E . The network is low because of low SN
F . TX power must be increased in both the client and the A

Answer: B

Question: 96

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 M
D . The IP address of the MC does not match the one that was defined in the M
F . The network administrator has not moved the device into a group yet.

Answer: B

Question: 97

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.
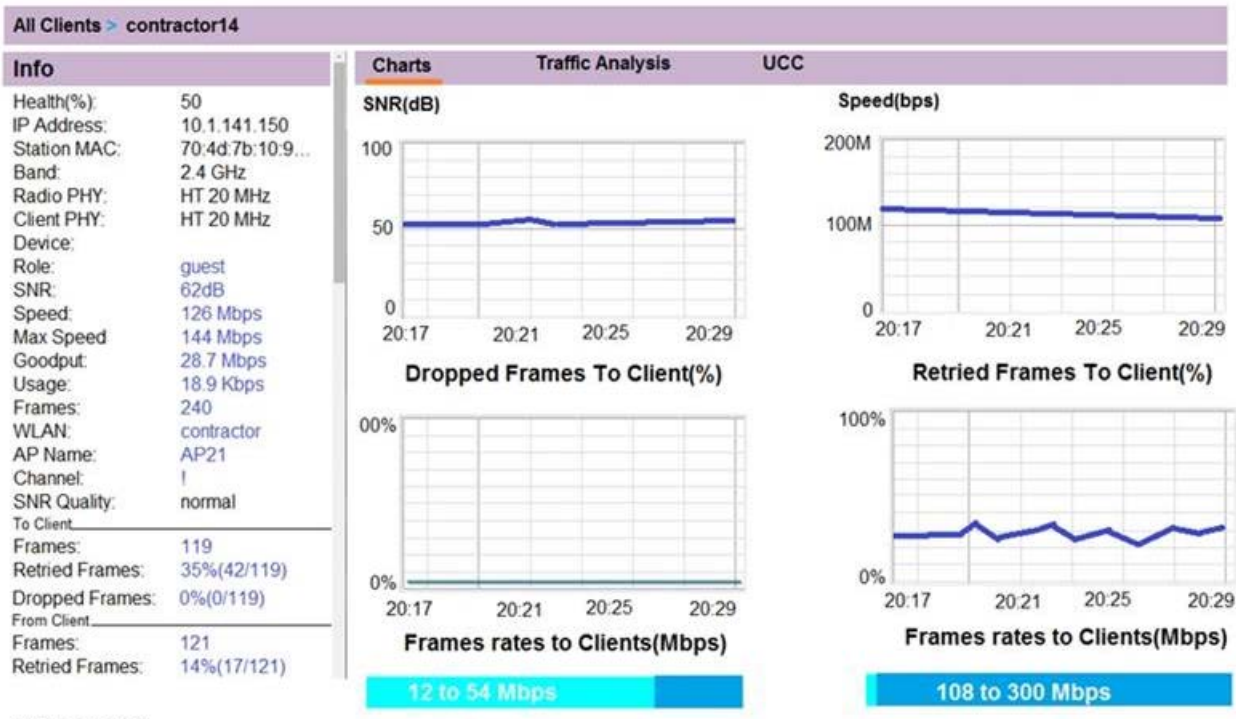
What should the network administrator do to resolve this problem?
A . Change the localip ipsec key to Aruba123 in the mynode device level from the MM, save, and reboot.
B . Enable disaster recovery mode in MC1 and change the masterip ipsec key to Aruba 123, save, and reboot.
C . Change the masterip ipsec 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.

Answer: B

Question: 98

Refer to the exhibit.

Info

Health(%):	50
IP Address:	10.1.141.150
Station MAC:	70:4d:7b:10:9...
Band:	2.4 GHz
Radio PHY:	HT 20 MHz
Client PHY:	HT 20 MHz
Device:	
Role:	guest
SNR:	62dB
Speed:	126 Mbps
Max Speed	144 Mbps
Goodput:	28.7 Mbps
Usage:	18.9 Kbps
Frames:	240
WLAN:	contractor
AP Name:	AP21
Channel:	!
SNR Quality:	normal

To Client

Frames:	119
Retried Frames:	35%(42/119)
Dropped Frames:	0%(0/119)

From Client

Frames:	121
Retried Frames:	14%(17/121)

(A48.01114413)

Charts   **Traffic Analysis**   **UCC**

SNR(dB)

Speed(bps)

Dropped Frames To Client(%)

Retried Frames To Client(%)

Frames rates to Clients(Mbps)
12 to 54 Mbps

Frames rates to Clients(Mbps)
108 to 300 Mbps

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 NI
E . The network is low because of low SN
F . TX power must be increased in both the client and the A

Answer: B

Question: 99

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
----------  ------------  ------  ----  ----------  ----  --------  -------  -------  ----------------  -------  ------------  ----

----------  ----------
16.1.141.150  70:4d:7b:10:9e:c6  it    guest   00:00:48    8021x-User          AP22     Wireless  Corp-employee/70:3a:0e:5b:8a: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\224l\005\S\260f\345\366F\276\305.9
\356e\013\220\276\375\22
Jul 4 17: 32:15 : 121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c: 1245]
4\2264 j0@?\177Y\325\331/\226\366\325\315z\342[\346\343?o\241\0151
Jul 4 17: 32:15 : 121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c: 1245] EAP-
Message: \003\011
Jul 4 17: 32:15 : 121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c: 1245] User-
Name: it
Jul 4 17: 32:15 : 121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c: 1245] Class:
\202\005\250) \210\215C\344\2536#\356\200\243"\006\271\013
Jul 4 17: 32:15 : 121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c: 1245]
PW_RADIUS_ID: \026
Jul 4 17: 32:15 : 121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c: 1245] Rad-Length:
231
Jul 4 17: 32:15 : 121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c: 1245]
PW_RADIUS_CODE: \002
Jul 4 17: 32:15 : 121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c: 1245]
PW_RAD_AUTHENTICATOR: \377pW\245\254/)M\267n\337\017\204\205\373\027
Jul 4 17: 32:15 :124004: <3553> <INFO> |authmgr| Authentication result=
Authentication Successful(0), method=802.1x, server=ClearPass.23, user=70:4d:7b:10:9e:c6

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

Answer: B

Question: 100

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 VLA
C . Connect both controllers with common VLANs, and create an HA fast failover group with public addresses in the internet VLA
E . Connect both controllers with different VLANs, and create an L2-connected cluster using private addresses in the internet VLA
G . Connect both controllers with common VLANs, and configure LMS/BLMS values equal to public addresses in the internet VLA

Answer: A

SAMPLE QUESTIONS

KILL EXAMS

These questions are for demo purpose only. **Full version** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

ORDER FULL VERSION
Special Discount Coupon

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.

For More exams visit https://killexams.com/vendors-exam-list
Kill your exam at First Attempt....Guaranteed!