HPE6-A48$^{Q\&As}$

Aruba Certified Mobility Expert 8 Written Exam

Pass HP HPE6-A48 Exam with 100% Guarantee

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

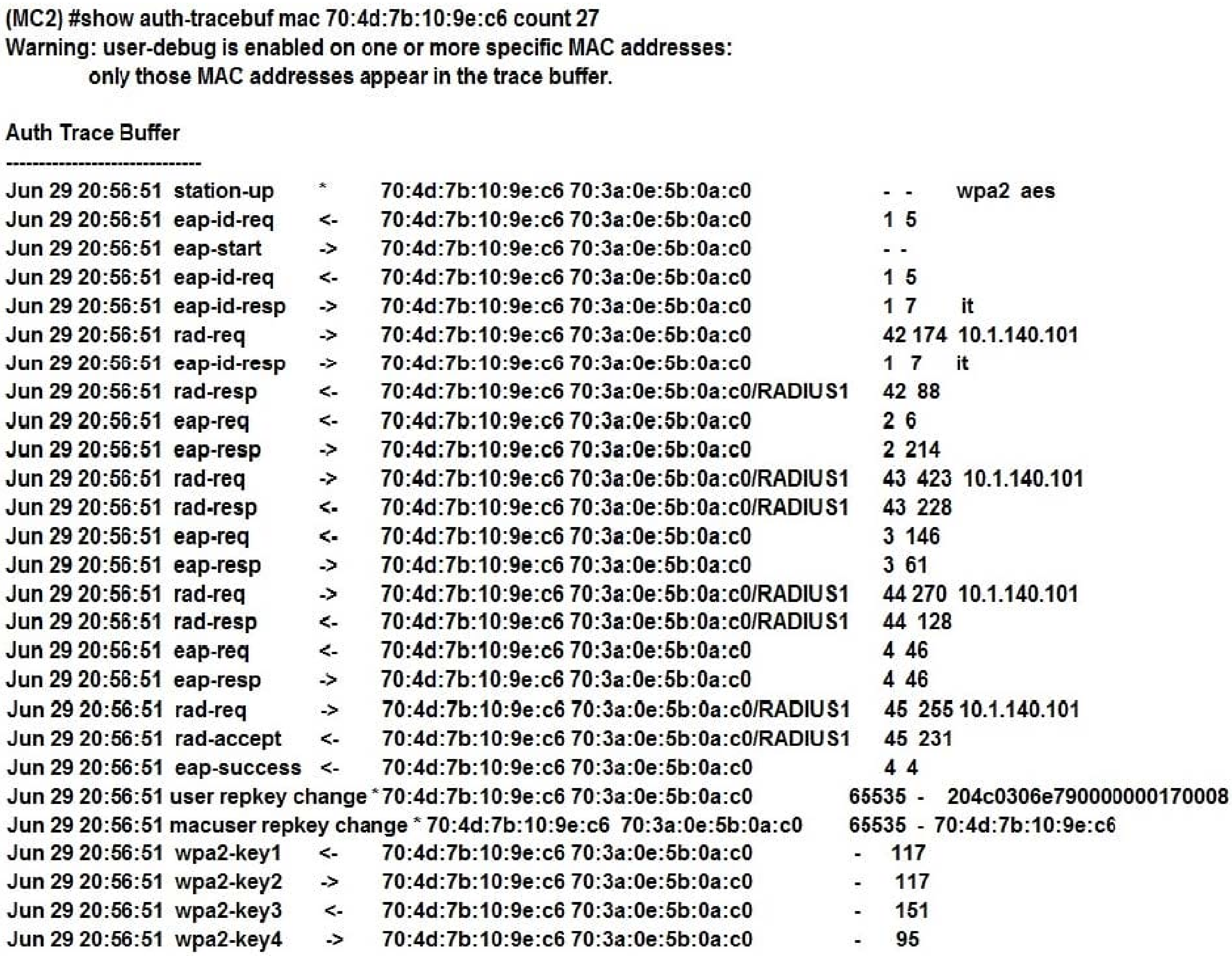
https://www.pass4itsure.com/hpe6-a48.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the 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

QUESTION 2

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

QUESTION 3

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.

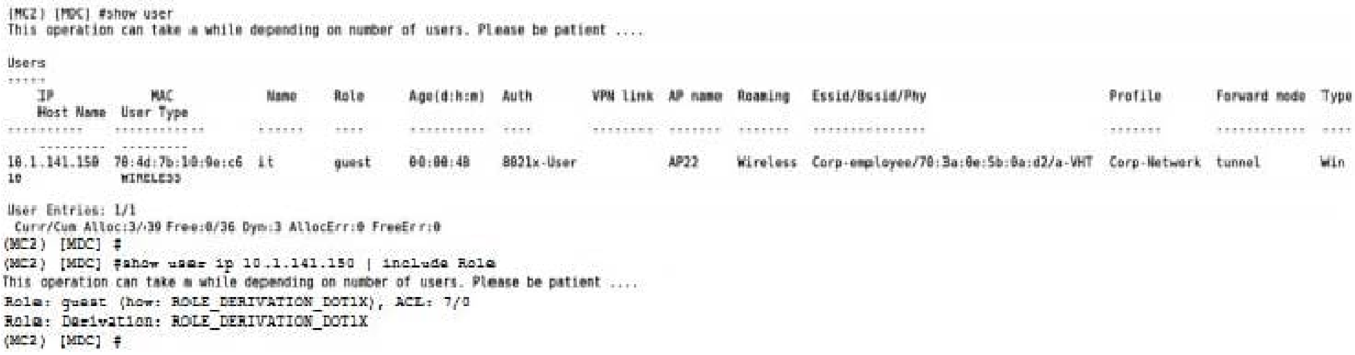
D. Create and AirWave RAPIDS rule with a Suspected Rogue classification and the SSID Does Not Match FXBroker121 condition, then access any RAPIDS List entry that matches the rule and click on Location.

Correct Answer: B

QUESTION 4

Refer to the exhibits.

Exhibit1

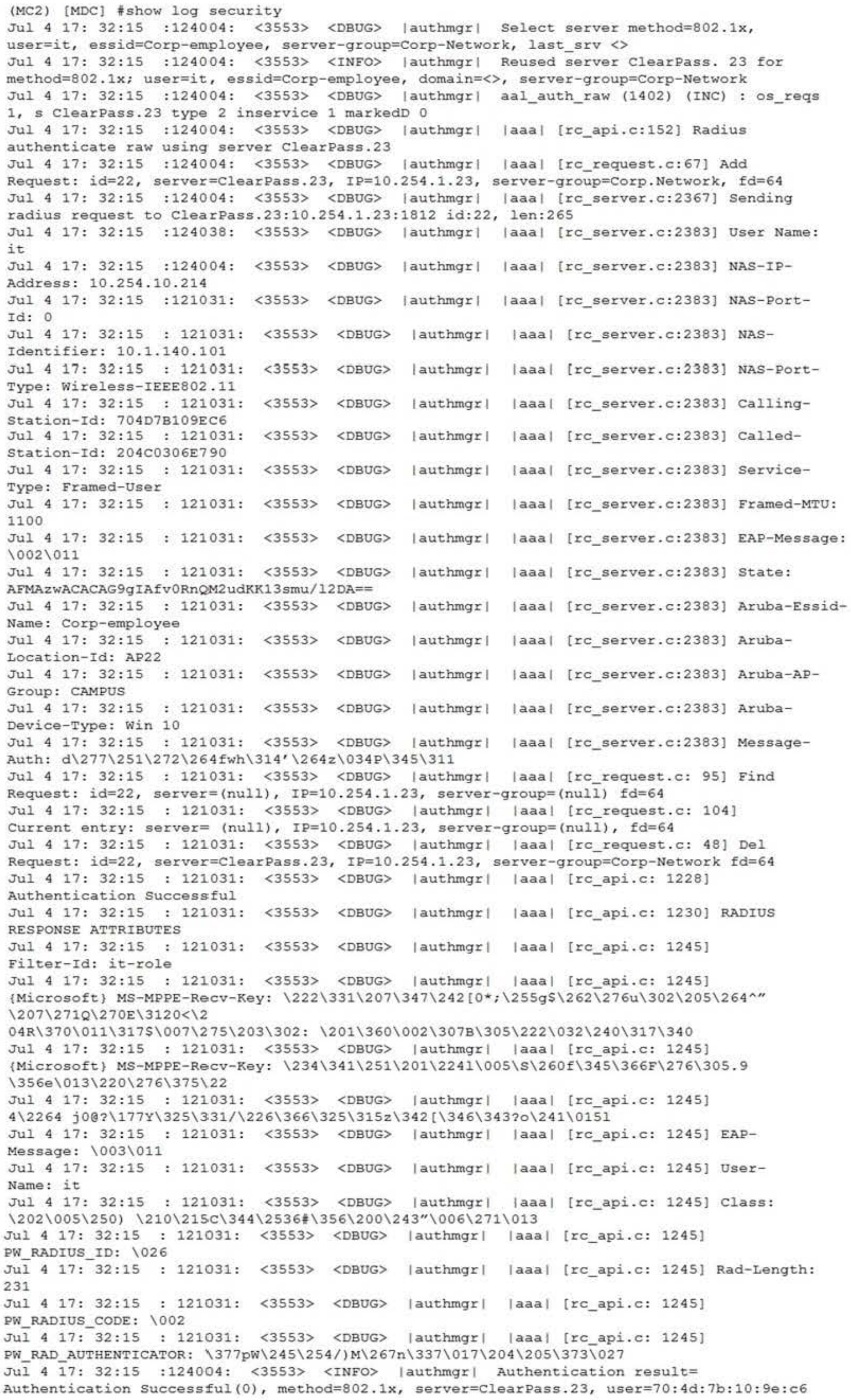


```
(MC2) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

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:10:9e: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\2241\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

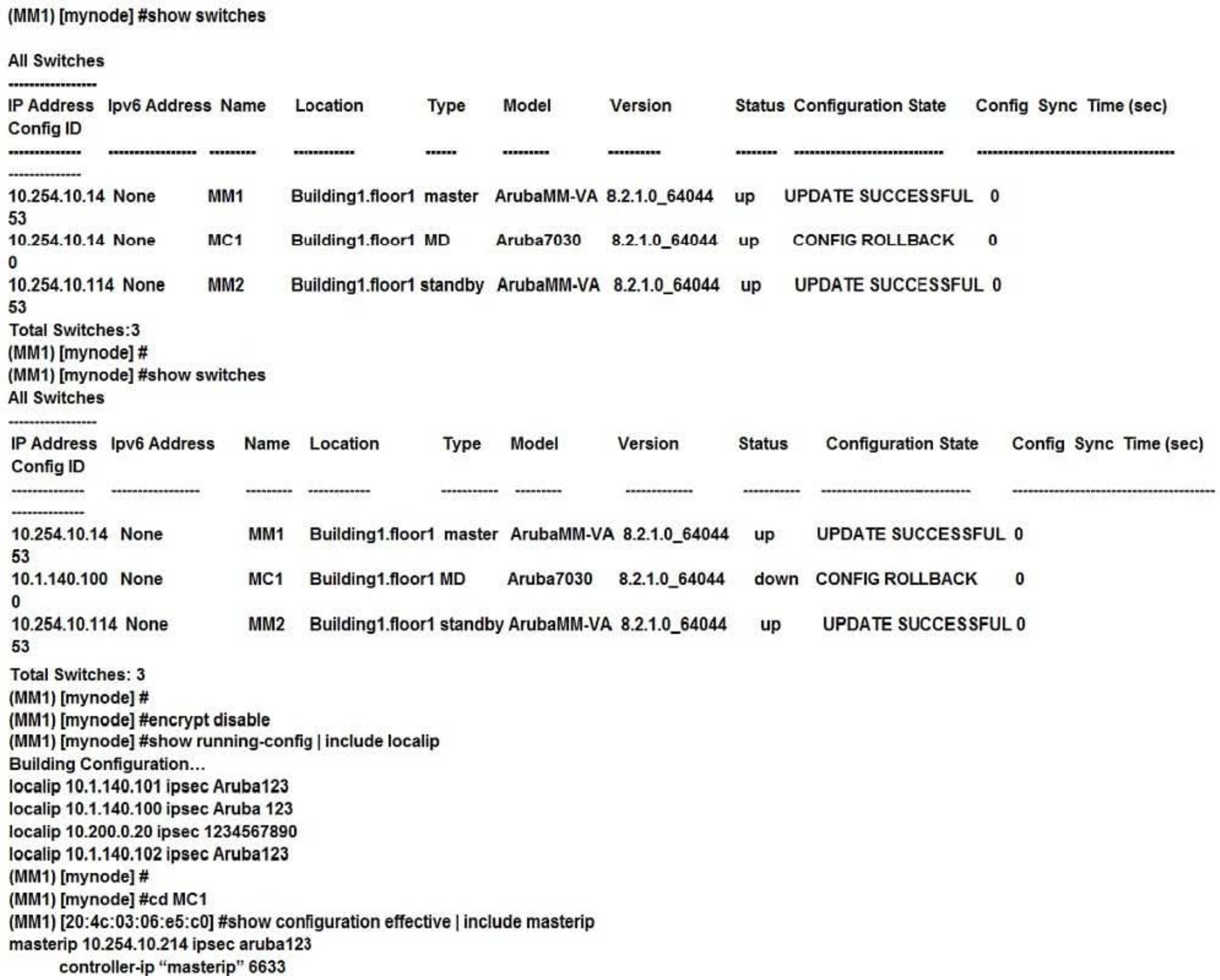
C. aaa server-group Corp-employee set role condition Filter-Id equals it-role set-value it_department

D. aaa server-group Corp-employee set role condition Filter-Id value-of

Correct Answer: B

QUESTION 5

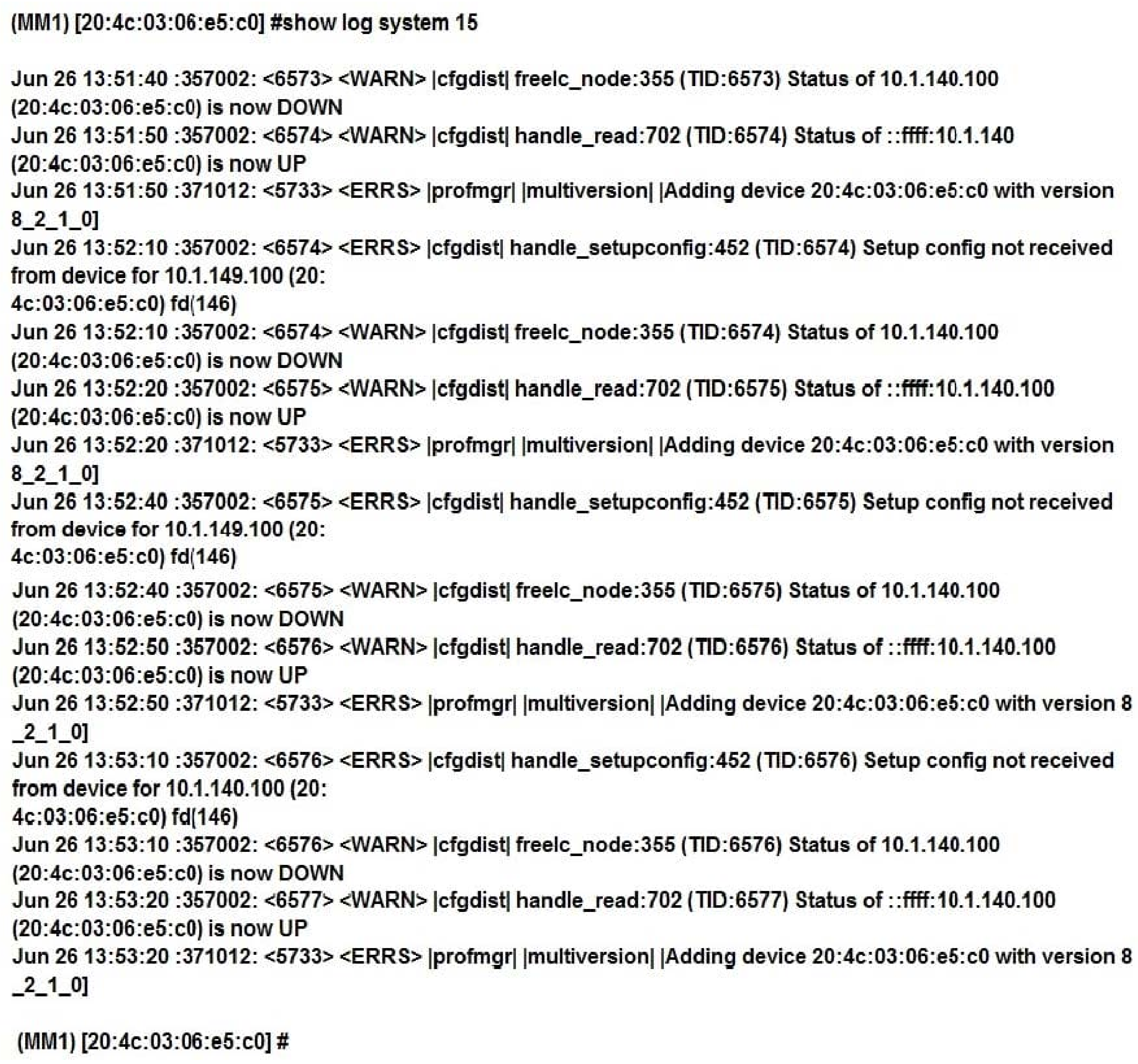
Refer to the exhibits. Exhibit 1



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

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

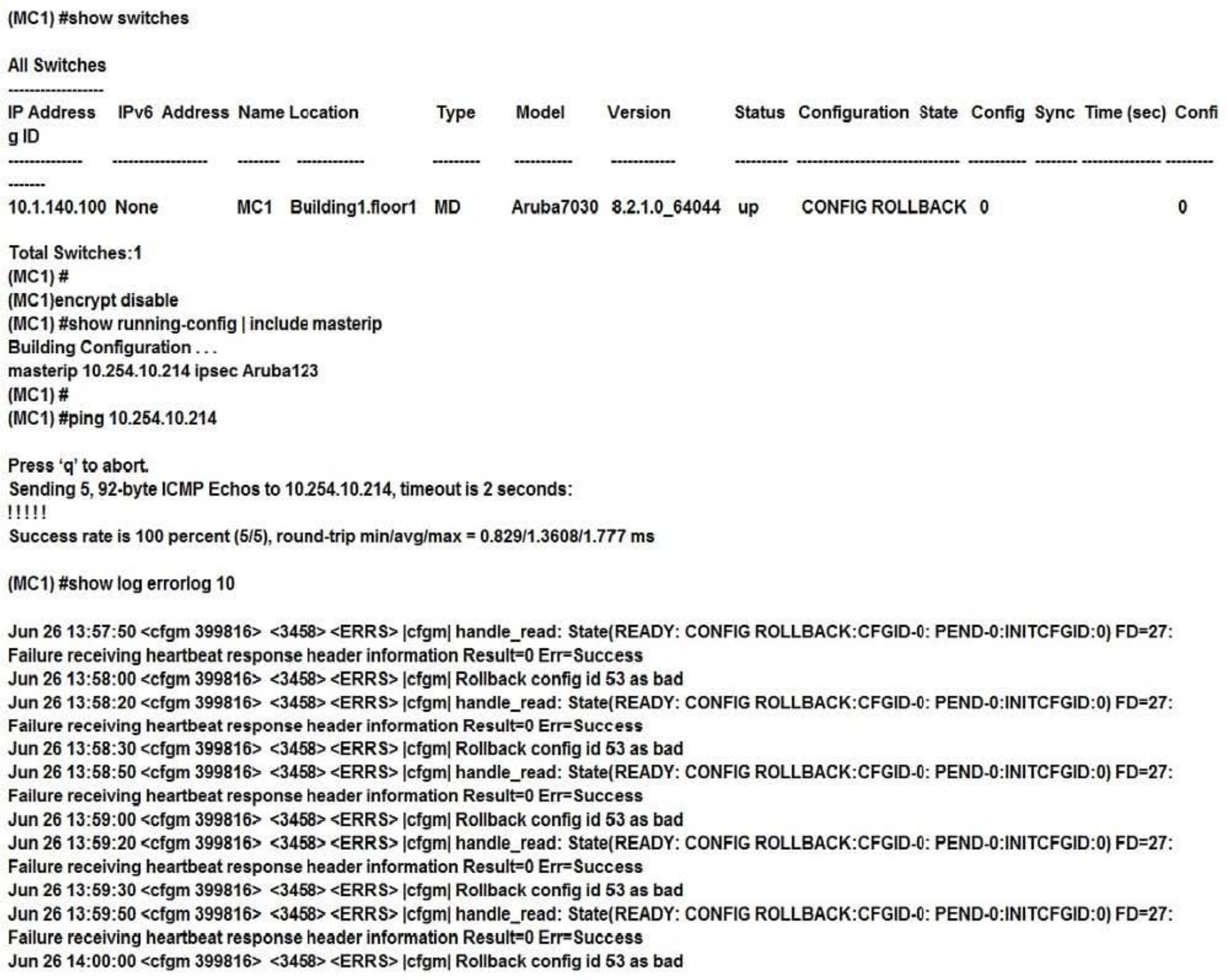
Exhibit 2 Exhibit 3



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

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

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



```
(MC1) #show switches

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

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

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

(MC1) #show log errorlog 10

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

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

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

What should the network administrator do to resolve this problem?

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

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

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

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

Correct Answer: B

HPE6-A48 PDF Dumps HPE6-A48 Study Guide HPE6-A48 Exam Questions