HP

HPE6-A48 Exam

HP Aruba Certified Mobility Expert 8 Written Exam

Thank you for Downloading HPE6-A48 exam PDF Demo

You can Buy Latest HPE6-A48 Full Version Download

https://www.certkillers.net/Exam/HPE6-A48

Version: 8.0

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

Answer: A

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

	Answer: B

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

	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:10:0e: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/12DA==
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

Answer: B

Question: 5

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, 0.1wa, 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.

Answer: D

Thank You for trying HPE6-A48 PDF Demo

To Buy Latest HPE6-A48 Full Version Download visit link below

https://www.certkillers.net/Exam/HPE6-A48

Start Your HPE6-A48 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your HPE6-A48 preparation with actual exam questions.