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.leads4pass.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

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

QUESTION 2

Refer to the exhibit.

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

Local Master Server (LMS) State

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

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

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

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

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

A. a pair of MCs within a cluster

B. a single standalone MC

C. a pair of MCs with APFF enabled

D. a pair of switches

Correct Answer: B

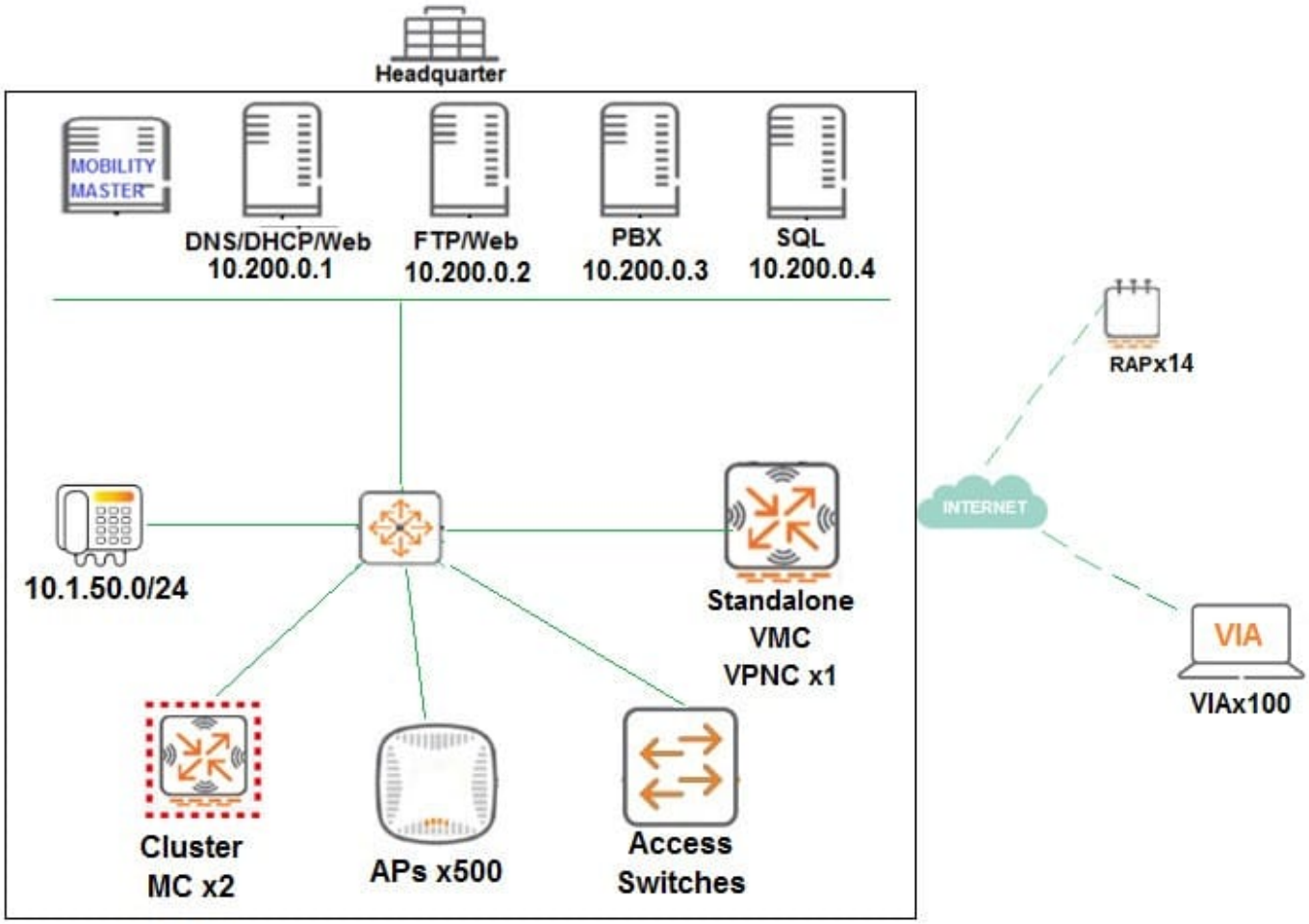
QUESTION 3

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

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  78:4d: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 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