HPE6-A79 Q&As

Aruba Certified Mobility Expert Written Exam

Pass HP HPE6-A79 Exam with 100% Guarantee

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

https://www.leads4pass.com/hpe6-a79.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)  [MDC] #show user mac xx:xx:xx:xx:xx:xx
This operation can take a while depending on number of users. Please be patient ....


Name: contractor14, IP:10.1.141.150, MAC: xx:xx:xx:xx:xx:xx, Age: 00:00:00
Role: contractor (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 128/0
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: ClearPass.23
Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE_DERIVATION_DOT1X_VSA
```

A network administrator is evaluating a deployment to validate that a user is assigned the proper role and reviews the output in the exhibit. How is the role assigned to user?

A. The MC assigned the role based on Aruba VSAs.

B. The MC assigned the machine authentication default user role.

C. The MC assigned the default role based on the authentication method.

D. The MC assigned the role based on server derivation rules.

Correct Answer: C

QUESTION 2

Refer to the exhibits. Exhibit 1

```
(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  xx:xx:xx:xx:xx:xx  it    guest   00:00:48   802.1x            AP22     Wireless Corp-employee/yy:yy:yy:yy:yy:yy/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_DEPRIVATION_DOTIX), ACL: 7/0
Role Deprivation: ROLE_DEPRIVATION_DOTIX
(MC2) [MDC] #
```

Exhibit 2

```
(MC2) [MDC] #show log security 300

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 :124038: <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) : cs_reqs 1, s ClearPass.23 type 2 inservice 1 markedD 0
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass.23
Jul 4 17:32:15 :121031: <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 :121031: <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 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name: it
Jul 4 17:32:15 :121031: <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: 814F0C517FS6
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 193D1247D881
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: AFMAzwACACAG9gIAfvORnQM2udKK13smu/I2DA==
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\466\487\328\679wvx\487"\642z\812P\540\115
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.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_server.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_server.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: \555\554\801\861\353[1*;\877g$\574\856u\302\215\237^"\857\2257\843F\4265<\2
57R\487\016\547$\109\146\506\605:\384\603\200\716R\508\666\032\750\413\480
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] (Microsoft) MS-MPPE-Send-Key: \456\311\781\648\789I\549\K\950\345\366F\276\789.7\642e\917\331\983\389\11
5\7764|D@?\763T\649\865/\339\992\587\756x\456[\487\493?u\415\308I
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] Message-Auth: \789,\156\734I\111\555\871\456t\478\119\752{\723\490
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: \514\678\820)\430\513C\749\0548#\648\700\438"\112\754\261
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: \447rV\623\765/)F\894t\384\065\413\395\243\084
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass.23, user=xx:xx:xx:xx:xx:xx
```

A network administrator integrates a current Mobility Master (MM) - Mobility Controller (MC) deployment with a RADIUS server to authenticate a wireless user, the network administrator realizes that the client machine is not failing into the it_department role, as shown 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 Corp-employee set role condition Filter-Id value-of

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

D. aaa server-group ClearPass set role condition Filter-Id equals it_department set-value it-role

E. aaa server-group Corp-Network set role condition Filter-Id equals it_department set-value it-role

Correct Answer: C

QUESTION 3

Refer to the exhibit.

```
Access-1# show ubt state

Local Master Server (LMS) State:

LMS Type      IP Address     State
-------------------------------------------------------
Primary     : 10.1.224.100   ready_for_bootstrap
Secondary   : 10.1.140.100   ready_for_bootstrap

Switch Anchor Controller (SAC) State:

              IP Address        MAC Address         State
-------------------------------------------------------------------
Active      : 10.1.224.100      xx:xx:xx:xx:xx:xx   Registered


User Anchor Controller(UAC): 10.1.224.100

User               Port    State                              Bucket ID   Gre Key
-------------------------------------------------------------------------------
xx:xx:xx:xx:yy:yy   1/1/20 registered                         255         20
Access-1#
```

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

A. a pair of standalone MCs

B. a pair of switches running VXLAN

C. a pair of MCs within a L3 cluster

D. a single standalone MC

Correct Answer: C

QUESTION 4

Refer to the exhibit

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

AP Database
-----------
Name  Group    AP Type  IP Address    Status   Flags  Switch IP     Standby IP
----  -----    -------  ----------    ------   -----  ----------    ----------
AP21  CAMPUS   355      10.1.145.150  Down            10.254.13.14  0.0.0.0
AP22  CAMPUS   355      10.1.146.150  Up 7m:4s IL     10.254.13.14  0.0.0.0


Total Aps:2
(MC11) [mynode] #show version | include Aruba

Aruba Operating System Software.
ArubaOS (MODEL: ArubaMC-VA-US), Version 8/2/1/0
(MC11) [mynode] #
(MC11) [mynode] #show log system 5| include "license"
Jun 21 12:20:25 :399814: <5481> <DBUG> |cfgn| Config Manager is not ready to send the new license config to the applications yet
Jun 21 12:29:34 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP xx:xx:xx:xx:xx:xx
Jun 21 12:29:38 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP xx:xx:xx:xx:xx:xx
Jun 21 12:34:42 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP AP22
Jun 21 12:34:46 :305038: <5624> <WARN> |stm| No available license type SECURITYGW for AP AP22
(MC11) [mynode] #
(MC11) [mynode] #show license aggregate

Aggregate License Table for pool /
----------------------------------
Hostname     IP Address   Mac addr           AP   REF  RF Protect  ACR  WebCC  MM  MC-VA-RW  MC-VA-EG  MC-VA-IL  MC-VA-JP  MC-VA-US  VIA
 Last update (secs. ago)
--------     ----------   --------           ---- ---- ----------  ---- -----  --- --------- --------  --------  --------  --------  ---
 ------------------------
From Server  10.254.13.14 yy:yy:yy:yy:yy:yy  16   0    0           0    0      0   0         0         0         0         0         0


Total no. of clients: 0
```

A network administrator deploys a standalone Mobility Controller (MC) and configures some VAPs within the CAMPUS AP group. The network administrator realizes that none of the VAPs are being broadcasted.

Based on the output shown in the exhibit, what should the network administrator do to solve this problem?

A. Install MC-VA licenses, then install PEF licenses and enabled the PEF feature.

B. Install MC-VA licenses, then reprovision the APs.

C. Install MM licenses, then install PEF licenses and enable the PEF feature.

D. Install MM licenses and install MC-VA licenses, then install RFP licenses.

Correct Answer: D

QUESTION 5

Refer to the exhibit.

```
(MC_VA) [mynode] #show aaa debug role user mac xx:xx:xx:xx:xx:xx


Role Derivation History
=======================
    0: l2 role->logon, mac user created
    1: l2 role->authenticated, station Authenticated with auth type: 802.1x
    2: l2 role->corp, RFC 3576 l3 role change COA
(MC_VA) [mynode] #
```

A network administrator has Mobility Master (MM) - Mobility Controller (MC) based network and has fully integrated the MCs with ClearPass for RADIUS-based AAA services. The administrator is testing different ways to run user role

derivation.

Based on the show command output, what method has the administrator use for assigning the "corp" role to client with MAC xx:xx:xx:xx:xx:xx?

A. Dynamic Authorization using VSA attributes.

B. Dynamic Authorization using IETF attributes.

C. Server Derivation Rules using IETF attributes.

D. User Derivation Rules using the client\\'s MAC.

Correct Answer: A