Aruba Certified Mobility Expert Written Exam

Exam Description
This exam tests your technical expert skills with WLAN design, implementation, and configuration in complex multisite highly available network environments using the Aruba Controller, Access Point, and AirWave product lines. It also tests your ability to design, implement, monitor, troubleshoot, and maintain end-to-end WLAN campus and branch solutions, and resolve issues in an existing customer infrastructure.

Ideal Candidate For This Exam
Typical candidate is recognized as an expert-level resource, advisor, and mentor to networking professionals. Candidate has extensive hands-on experience in designing, architecting, implementing, and troubleshooting WLANs and networks. Candidate have more than 4 years of experience implementing complex, highly available, multisite Aruba WLANs, and a minimum of one year experience using AirWave to manage and monitor Aruba WLAN deployments. Candidate also has a minimum of 3 years of switching and routing experience.

Exam Contents
This exam has 60 questions.

Advice To Help You Take This Exam
- Complete the training and review all course materials and documents before you take the exam.
- Exam items are based on expected knowledge acquired from job experience, an expected level of industry standard knowledge, or other prerequisites (events, supplemental materials, etc.).
- Successful completion of the course alone does not ensure you will pass the exam.
- Read this HPE Exam Preparation Guide and follow its recommendations.
- Visit HPE Press for additional reference materials, study guides, practice tests, and HPE books.

Supporting resources
These recommended resources help you prepare for the exam:

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource ID</th>
<th>Resource Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course</td>
<td>01114375</td>
<td>Aruba Advanced Mobility Troubleshooting and Solutions, Rev. 18.21</td>
</tr>
</tbody>
</table>

Objectives
This exam validates that you can:

Exam ID: HPE6-A48
Exam type: Proctored
Exam duration: 2 hours
Exam length: 60 questions
Passing score: 72%
Delivery languages: Japanese, English

Register for this Exam
You need an HPE Learner ID and a Pearson VUE login and password.

The HPE6-A48 ACMX Written Exam is required to be passed before the practical exam. Once the written is passed, you will only have 18 months to pass the ACMX Practical Exam. Candidates who do not pass the ACMX Practical Exam within 18 months will have to retake the ACMX Written Exam. HPE recommends that you register for the ACMX Practical Exam within 12 months of passing the written exam to ensure that you pass in the allotted 18-month timeframe.

No reference material is allowed at the testing site. This exam may contain beta test items for experimental purposes.

During the exam, you can make comments about the exam items. We welcome these comments as part of our continuous improvement process.
Sample questions

Sample questions are provided only as examples of question style, format and complexity/difficulty. They do not represent all question types and do not reflect all topic areas. These sample questions do not represent a practice test.

1. Refer to the exhibit.

**[MC2] [MCQ] #show user**

This operation can take a while depending on number of users. Please be patient.

<table>
<thead>
<tr>
<th>IP</th>
<th>Host Name</th>
<th>MAC</th>
<th>User Type</th>
<th>Name</th>
<th>Role</th>
<th>Age (d/h/m)</th>
<th>Auth</th>
<th>VPN Link</th>
<th>AP name</th>
<th>Roaming</th>
<th>Essid/Bssid/Phy</th>
<th>Profile</th>
<th>Forward mode</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.150 78:4d:7b:10:9e:c6</td>
<td>it</td>
<td>g000:00 881x-User</td>
<td>AP22 Wireless Corp-employee/78:3a:0e:50:Ba:d2/a-VHT Corp-Network tunnel</td>
<td>W</td>
<td>18</td>
<td>0</td>
<td>WIRELESS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User Entries: 1/1


**[MC2] [MCQ] #show user mac 70:4d:7b:10:9e:c6**

This operation can take a while depending on number of users. Please be patient.

Name: it, IP: 10.1.1.150, MAC: 70:4d:7b:10:9e:c6, Age: 00:00:00

Role: guest (how: ROLE_DERIVATION_DOTIX), ACL: 7/6


Role Derivation: ROLE_DERIVATION_DOTIX

---

A network administrator evaluates a deployment to validate that users are assigned to the proper roles. Based on the output shown in the exhibit, what can the network administrator conclude?
The MC assigned the role based on server derivation rules.

The MC assigned the machine authentication default user role.

The MC assigned the role based on user derivation rules.

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

A company offers guest access with an open SSID and an internal Mobility Controller (MC) captive portal. The network administrator needs to integrate a more scalable solution with a remote RADIUS and captive portal server.

The network administrator fully deploys a guest solution with self-registration in ClearPass, and defines the MC as a RADIUS client. Next, the network administrator defines ClearPass as a RADIUS server and adds it into a server group in the MC.

Which two configuration components must the network administrator modify in the MC to complete the deployment? (Select two.)

- AAA server profile
- Initial role firewall policies
- VAP profile
- Authentication server group
- Captive portal profile

Refer to the exhibit. (MC11) [sudo]# show ap database

<table>
<thead>
<tr>
<th>AP Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>70:3a:8e:cd:bb:a4</td>
</tr>
<tr>
<td>70:3d:7f:1c:13:3a</td>
</tr>
<tr>
<td>API1</td>
</tr>
</tbody>
</table>

Flags: I = 802.1x authenticated AP; P = 802.1x use PAP; L = 802.1x use CHAP; D = Dirty or no config

A company offers guest access with an open SSID and an internal Mobility Controller (MC) captive portal. The network administrator needs to integrate a more scalable solution with a remote RADIUS and captive portal server.

The network administrator fully deploys a guest solution with self-registration in ClearPass, and defines the MC as a RADIUS client. Next, the network administrator defines ClearPass as a RADIUS server and adds it into a server group in the MC.

Which two configuration components must the network administrator modify in the MC to complete the deployment? (Select two.)

- AAA server profile
- Initial role firewall policies
- VAP profile
- Authentication server group
- Captive portal profile

Refer to the exhibit. (MC11) [sudo]# show ap bss-table

<table>
<thead>
<tr>
<th>bss</th>
<th>ess</th>
<th>port</th>
<th>ip</th>
<th>phy</th>
<th>type</th>
<th>ch/IEEE</th>
<th>max-IIEEE</th>
<th>cur.cl</th>
<th>ap name</th>
<th>in-t(s)</th>
<th>tot-t</th>
<th>mtu</th>
<th>acl-state</th>
<th>acl</th>
<th>fn</th>
<th>cluster</th>
<th>datazone</th>
</tr>
</thead>
<tbody>
<tr>
<td>70:3a:8e:cd:bb:a4</td>
<td>Company Guest</td>
<td>N/A</td>
<td>10.1.146.150</td>
<td>g-HT</td>
<td>ap</td>
<td>6/8/0/25/6</td>
<td>0</td>
<td>API1</td>
<td>3m:40s</td>
<td>1500</td>
<td>T</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70:3a:8e:cd:bb:a4</td>
<td>Company Guest</td>
<td>N/A</td>
<td>10.1.146.150</td>
<td>e-WT</td>
<td>ap</td>
<td>153/19/8/28.5</td>
<td>0</td>
<td>API1</td>
<td>3m:40s</td>
<td>1500</td>
<td>T</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Channel followed by "*" indicates channel selected due to unsupported configured channel. Multiple channels followed by "**" indicates Local Spectrum Override in effect.

Num APs: 2
Num Associations: 8

Based on the output shown in the exhibit, what is the current relationship between API1 and MC11?

- API1 is a multzone AP, and MC11 is its primary zone.
- API1 is a CAP, and MC11 terminates its active tunnels.
- API1 is a CAP, and MC11 terminates its standby tunnels.

Refer to the exhibit. (MC11) [MON]# show aaa authentication dot1x DOT1X-EMP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA/WPA2 Key Message Retry Count</td>
<td>3</td>
</tr>
<tr>
<td>Multicast Key Rotation</td>
<td>Disabled</td>
</tr>
<tr>
<td>Unicast Key Rotation</td>
<td>Disabled</td>
</tr>
<tr>
<td>Reauthentication</td>
<td>Enabled</td>
</tr>
<tr>
<td>Opportunistic Key Caching</td>
<td>Enabled</td>
</tr>
<tr>
<td>Validate PMKD</td>
<td>Enabled</td>
</tr>
<tr>
<td>Use Session Key</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use Static Key</td>
<td>Disabled</td>
</tr>
<tr>
<td>xSec MTU</td>
<td>1500 bytes</td>
</tr>
<tr>
<td>Termination EAP-Type</td>
<td>N/A</td>
</tr>
<tr>
<td>Termination Inner EAP-Type</td>
<td>N/A</td>
</tr>
<tr>
<td>Enforce Suite-B 128 bit or more security level Authentication</td>
<td>128-DH</td>
</tr>
<tr>
<td>Enforce Suite-B 192 bit or more security level Authentication</td>
<td>128-DH</td>
</tr>
<tr>
<td>Enforce Suite-B</td>
<td>128-DH</td>
</tr>
<tr>
<td>Token Caching</td>
<td>Disabled</td>
</tr>
<tr>
<td>Token Caching Period</td>
<td>30 sec</td>
</tr>
<tr>
<td>CA-Certificate</td>
<td>N/A</td>
</tr>
<tr>
<td>Server-Certificate</td>
<td>default</td>
</tr>
<tr>
<td>TLS Guest Access</td>
<td>Disabled</td>
</tr>
<tr>
<td>TLS Guest Role</td>
<td>guest</td>
</tr>
<tr>
<td>Ignore EAPOL-START after authentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>Handle EAPOL-Logoff</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ignore EAP ID during negotiation</td>
<td>Disabled</td>
</tr>
<tr>
<td>WPA-Fast-Handover</td>
<td>Disabled</td>
</tr>
<tr>
<td>Check certificate common name against AAA server</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Based on the output shown in the exhibit, which configuration change is required to validate user credentials in a server group that includes LDAP and the internal database?

- aaa authentication dot1x DOT1X-EMP termination eap-type eap-peap
- aaa authentication dot1x DOT1X-EMP termination inner-eap-type eap-md5pwd
- aaa authentication dot1x DOT1X-EMP termination eap-type eap-md5pwd
- ca-cert AD.mycompany.com
server-cert AD-signed.mycompany
ca-cert AD.mycompany.com
server-cert AD-signed.mycompany.com
server serverretry 5

d. aaa authentication dot1x DOT1X-EMP
   termination enable
termination eap-type eap-peap
termination inner-eap-type eap-mschapv2

5. Refer to the exhibit.

(MC1) # show log security 56

Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2267] Sending radius request to ClearPass. 23.10.254.1.23:1812 Id=63, len=243
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] User Name: employe33
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] NAS IP Address: 10.254.10.214
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] NAS Port Id: 0
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] NAS-Identifier: 10.1.140.100
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] NAS-Port-Type: Wireless-IEEE802.11
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] Calling-Station-Id: 7040787896C6
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] Radius-Session-Id: 2940831865C0
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] Service-Type: Framed-User
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] Framed-MTU: 1100
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] EAP-Message: 0
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] State: ADDw/WA/AADB0yPsyXzXzZks8K4kys3Cue4Y9Y9kA==
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] Aruba-Ext-Id: Employee
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] Aruba-Location-Id: AP2
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] Aruba-Device-Type: (VSA with invalid length - Don't send it)
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_server.c:2283] [request c:95] First Request: id=43, server=Null, IP=10.254.1.23, server-group=Null f=646
Jun 26 15:27:46:121001: [3575] [DBG] [authmgr] [aaa] [rc_request.c:184] Current entry: server=Null, IP=10.254.1.23, server-group=Null, t=646

A network administrator deploys an employee WLAN and uses ClearPass as the authentication and policy server. Change of Authorization (CoA) is used to disconnect users once the client has been profiled. This permits a more granular control over connections prior to assigning the ultimate user role.

When users connect, the network administrator notices they always remain in the profiling firewall role and the CoA action does not occur. It has been confirmed that the ClearPass server configuration is correct. The network administrator debugs an authentication attempt and sees the output shown in the exhibits.

What must the network administrator do to successfully deploy this solution?

a. Change the RADIUS NAS-ID of the authentication server at the Managed Device group level.
b. Use an IP address for the calling station ID in the authentication server configuration at the MC device level.
c. Change the RADIUS Client NAS IPv4 address at the MC device level.
d. Enable interim accounting in the Managed Device group level.

Answers
This section provides answers to and references for the sample questions.

1. Refer to the exhibit.

(MC2) # show user

This operation can take a while depending on number of users. Please be patient ....

<table>
<thead>
<tr>
<th>Users</th>
<th>IP</th>
<th>MAC</th>
<th>User Type</th>
<th>Name</th>
<th>Role</th>
<th>Age(d:h:m)</th>
<th>Auth</th>
<th>VPN Link</th>
<th>AP name</th>
<th>Roaming</th>
<th>Essid/Bssid/Phy</th>
<th>Profile</th>
<th>Forward mode</th>
<th>Tj</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.141.150</td>
<td>70:4d:7b:10:9e:06</td>
<td>it</td>
<td></td>
<td>guest</td>
<td></td>
<td>00:00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User Entries: 1/1
corr/Cua Alloc: 3/42 Free:8/39 Dyn:3 AllocErr:0 FreeErr:0

(MC2) # show user mac 70:4d:7b:10:9e:06

This operation can take a while depending on number of users. Please be patient.

Name: it, IP: 10.1.141.150, MAC: 70:4d:7b:10:9e:06, Age: 00:00:00
Role: guest (how: ROLE_DERIVATION_DOT1X), ACL: 7/0
Authentication Servers: dotlx authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE_DERIVATION_DOT1X
A network administrator evaluates a deployment to validate that users are assigned to the proper roles. Based on the output shown in the exhibit, what can the network administrator conclude?

a. The MC assigned the role based on server derivation rules.
b. The MC assigned the machine authentication default user role.
c. The MC assigned the role based on user derivation rules.
d. The MC assigned the default role based on the authentication method.

2. A company offers guest access with an open SSID and an internal Mobility Controller (MC) captive portal. The network administrator needs to integrate a more scalable solution with a remote RADIUS and captive portal server. The network administrator successfully integrates a guest solution with self-registration in ClearPass, and defines the MC as a RADIUS client. Next, the network administrator defines ClearPass as a RADIUS server and adds it into a server group in the MC.

Which two configuration components must the network administrator modify in the MC to complete the deployment? (Select two.)

a. AAA server profile
b. Initial role firewall policies
c. VAP profile
d. Authentication server group
e. Captive portal profile

3. Refer to the exhibit.

<table>
<thead>
<tr>
<th>AP Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>AP11</td>
</tr>
</tbody>
</table>

Based on the output shown in the exhibit, what is the current relationship between AP11 and MC11?

a. AP11 is a multizone AP, and MC11 is its datazone.
b. AP11 is a multizone AP, and MC11 is its primary zone.
c. AP11 is a CAP, and MC11 terminates its active tunnels.
d. AP11 is a CAP, and MC11 terminates its standby tunnels.

4. Refer to the exhibit.
Based on the output shown in the exhibit, which configuration change is required to validate user credentials in a server group that includes LDAP and the internal database?

a. `aaa authentication dot1x DOT1X-EMP
termination eap-type eap-peap
termination inner-eap-type eap-mschapv2`

b. `aaa authentication dot1x DOT1X-EMP
termination eap-type eap-tls
cacert AD.mycompany.com
server-cert AD-signed.mycompany.com
server server-retry 5`

c. `aaa authentication dot1x DOT1X-EMP
cacert AD.mycompany.com
server-cert AD-signed.mycompany.com`

d. `aaa authentication dot1x DOT1X-EMP
termination enable
termination eap-type eap-peap
termination inner-eap-type eap-mschapv2`

A network administrator deploys an employee WLAN and uses ClearPass as the authentication and policy server. Change of Authorization (CoA) is used to disconnect users once the client has been profiled. This permits a more granular control over connections prior to assigning the ultimate user role.

When users connect, the network administrator notices they always remain in the profiling firewall role and the CoA action does not occur. It has been confirmed that the ClearPass server configuration is correct. The network administrator debugs an authentication attempt and sees the output shown in the exhibits.

What must the network administrator do to successfully deploy this solution?

a. Change the RADIUS NAS-ID of the authentication server at the Managed Device group level.

b. Use an IP address for the calling station ID in the authentication server configuration at the MC device level.

c. Change the RADIUS Client NAS IPv4 address at the MC device level.

d. Enable interim accounting in the Managed Device group level.