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 Aruba WLAN configuration, administration, and troubleshooting experience. 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:
<table>
<thead>
<tr>
<th>Percentage of Exam</th>
<th>Sections/Objectives</th>
</tr>
</thead>
</table>
| 24%                | - Analyze functional requirements to create a solution design and implementation plan.  
|                    | - Analyze a complex multisite highly available network to determine the physical infrastructure connectivity requirements.  
|                    | - Analyze an entire WLAN infrastructure to determine the licensing requirements.  
|                    | - Analyze an entire WLAN infrastructure to determine the architectural requirements.  
|                    | - Analyze a complex multisite highly available network to determine the need for QoS.  
|                    | - Analyze customer requirements to determine the need for a multizone deployment.  
|                    | - Analyze customer requirements to determine roles, firewall policies, and rule requirements.  
|                    | - Configure and validate a multizone solution. |

| 21%                | - Configure and validate Aruba WLAN solutions.  
|                    | - Configure and validate a WLAN to support voice and video optimization.  
|                    | - Configure and verify tunnels endpoint to endpoint.  
|                    | - Configure and validate MAC authentication for role derivation.  
|                    | - Configure and validate a complex multisite high availability mobility environment.  
|                    | - Configure a guest WLAN and validate client connectivity.  
|                    | - Configure and validate remote connectivity using RAP or a branch office solution. |

| 17%                | - Configure and validate Aruba WLAN solutions.  
|                    | - Use AirWave and a Mobility Master to gather information about client health.  
|                    | - Create triggers and custom reports in AirWave.  
|                    | - Monitor the Spectrum Analyzer dashboard on the Mobility Controller.  
|                    | - Monitor and analyze controller health.  
|                    | - Monitor and optimize the RF environment.  
|                    | - Integrate and monitor devices with AirWave. |

| 18%                | - Implement advanced services and security solutions.  
|                    | - Configure and validate a WLAN to support voice and video optimization.  
|                    | - Configure a secure WLAN and integrate it with an existing infrastructure.  
|                    | - Validate client connectivity to a secure WLAN.  
|                    | - Configure and validate a complex multisite high availability mobility environment.  
|                    | - Configure a guest WLAN and validate client connectivity.  
|                    | - Configure and validate remote connectivity using RAP or a branch office solution. |

**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 (day:hour)</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>10.1.1.150</td>
<td>78:4d:67:10:9e:c6</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>
</tbody>
</table>

**User Entries:**


(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 (new: ROLE_DERIVATION_DOTIX), ACL: 7/0

**Authentication:** Yes, status: successful, method: 8021x-user, protocol: EAP-PEAP, server: ClearPass.23

**Authentication Servers:** dotlx authserver: ClearPass.23, mac authserver: ClearPass.23

**Bandwidth:** No Limit

**Role Derivation:** ROLE_DERIVATION_DOTIX

(MC2) [MCQ] #show log security 55

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?
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.

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 (MC11) [privmode] #show ap database

AP Database

<table>
<thead>
<tr>
<th>Name</th>
<th>Group</th>
<th>AP Type</th>
<th>IP Address</th>
<th>Status</th>
<th>Flags</th>
<th>Switch IP</th>
<th>Standby IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>70:3a:6e:cd:61:54</td>
<td>Default</td>
<td>335</td>
<td>10.1.145.350</td>
<td>Down</td>
<td>18.254.13.14</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>70:17:2f:5c:73:da</td>
<td>default</td>
<td>335</td>
<td>10.1.147.2</td>
<td>Down</td>
<td>18.254.13.14</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>API1</td>
<td>CAMPUS</td>
<td>335</td>
<td>10.1.146.158</td>
<td>Up 6m35s</td>
<td>3s</td>
<td>18.254.13.14</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

Flags: 1 = Built-in AP; C = Cellular MAP; D = Dirty or no config
B = Regulatory Domain Disallowed; F = AP failed 802.1x authentication
G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed
M = Multi-mode
N = Duplicate name; P = PPPoe AP; R = Remote AP; T = Remote AP requires Auth;
S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
Y = Mesh Recovery
C = DCH-based MAP; E = Custom EST cert; F = No Spectrum PPT support
I = Indoor; O = Outdoor; b = LACP stripping; u = Custom-Cert MAP; v = Datazone AP

Total APs: 3

(MC11) [privmode] #show ap bss-table

fn (forward mode): T-Tunnel, S-Split, D-Decrypt Tunnel, B-Bridge (s-standard, p-persistent, b-backup, a-always), n-anyset

Cluster (cluster role): U=UAC, A=AAC, s=Standby UAC, S=Standby AAC

Aruba 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</th>
<th>EIRP</th>
<th>max EIRP</th>
<th>cur ch</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></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></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70:3a:6e:5b:6a:4c</td>
<td>MC11</td>
<td>Guest</td>
<td>N/A</td>
<td>10.1.146</td>
<td>150</td>
<td>g-HT</td>
<td>6/8,6/25.6</td>
<td>0</td>
<td>AP11</td>
<td>0</td>
<td>1500</td>
<td>79</td>
<td>T</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70:3a:6e:5b:6a:4c</td>
<td>Company</td>
<td>Guest</td>
<td>N/A</td>
<td>10.1.146,150</td>
<td>a-WNT</td>
<td>ap</td>
<td>1533,9,028.5</td>
<td>0</td>
<td>AP11</td>
<td>0</td>
<td>1500</td>
<td>79</td>
<td>T</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Channel followed by "*" indicates channel selected due to unsupported configured channel.

"Spectrum" 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?

a. API1 is a multizone AP, and MC11 is its datazone.
b. API1 is a multizone AP, and MC11 is its primary zone.
c. API1 is a CAP, and MC11 terminates its active tunnels.
d. API1 is a CAP, and MC11 terminates its standby tunnels.

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

802.1X Authentication Profile "DOT1X-EMP"

Parameter | Value
-----------|--------
WPA/WPA2 Key Message Retry Count | 3
Multicast Key Rotation | Disabled
Unicast Key Rotation | Disabled
Reauthentication | Enabled
Opportunistic Key Caching | Enabled
Validate PMKID | Enabled
Use Session Key | Disabled
Use Static Key | Disabled
xSec MTU | 1900 bytes
Termination EAP-Type | N/A
Termination Inner EAP-Type | N/A
Enforce Suite-B 128 bit or more security level Authentication | Disabled
Enforce Suite-B 192 bit security level Authentication | Disabled
Token Caching | Disabled
Token Caching Period | 24 hr(s)
CA-Certificate | N/A
Server-Certificate | default
TLS Guest Access | Disabled
TLS Guest Role | guest
Ignore EAPOL-START after authentication | Disabled
Handle EAPOL-Logoff | Disabled
Ignore EAP ID during negotiation. | Disabled
WPA-Fast-Handover | Disabled
Check certificate common name against AAA server | Enabled

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-peap
cert AD.mycompany.com
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?

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

---

**Answers**

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

<table>
<thead>
<tr>
<th>IP</th>
<th>Host Name</th>
<th>MAC Address</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>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.141.150</td>
<td>7b:4d:7b:10:9e:0c</td>
<td>It</td>
<td>guest</td>
<td>00:00:00</td>
<td>802.1X-User</td>
<td>AP22</td>
<td>Wireless Corp-employee/7b:3a:0e:5b:ba:2d/-vht</td>
<td>Corp-Network tunnel</td>
<td>0 W</td>
<td>10 WIRELESS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User Entries: 1/1


**[MC2] #show mac 7b:4d:7b:10:9e:0c**

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

Name: It, IP: 10.1.141.150, MAC: 7b:4d:7b:10:9e:0c, Age: 00:00:00
Role: guest (how: ROLE DERIVATION DOTTIX), ACL: 7/b
Authentication Servers: dotlx authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE DERIVATION DOTTIX
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 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.)

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.

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 ca-cert AD.mycompany.com server-cert AD-signed.mycompany.com server server-retry 5`

c. `aaa authentication dot1x DOT1X-EMP ca-cert AD.mycompany.com server-cert AD-signed.mycompany.com check certificate common name against AAA server`  

5. Refer to the exhibit.

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.