PassQueen
a.k.a dumpsqueen.com

Aruba Certified Mobility Expert Written Exam

HP HPE6-A79

Version Demo

Total Demo Questions: 9

Total Premium Questions: 98

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

A company uses ClearPass Policy Manager to authenticate employees on an Aruba Mobility Controller WLAN. Employees must receive a user role and VLAN assignment based on their Active Directory group membership.

Which two RADIUS attributes can ClearPass return in an Access-Accept message to provide these assignments? (Choose two.)

A. Aruba-User-Role

B. Tunnel-Private-Group-ID

C. Framed-MTU

D. NAS-Identifier

E. Called-Station-Id

ANSWER: A B

Explanation:

The Aruba-User-Role vendor-specific attribute assigns the authenticated client to an ArubaOS user role. The role determines the firewall policies, bandwidth controls, captive portal behavior, and other access controls enforced for the session.

Standard RADIUS tunnel attributes can assign the client to a VLAN. ClearPass can return Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID attributes to identify the VLAN that ArubaOS should assign to the client. Together, the role and VLAN assignment allow ClearPass to apply differentiated access based on directory membership. Aruba role assignment and RADIUS authentication concepts are described in the ArubaOS authentication documentation.

QUESTION NO: 2 - (SIMULATION)

A network administrator wants to receive a major alarm every time a controller or an Aruba switch goes down for either a local or an upstream device failure. Which alarm definition must the network administrator create to accomplish this?

ANSWER: Check the explanation for the answer

Explanation:

Create a **Device Down** alarm definition.

Set the alarm **severity** to **Major**.
Scope/filter the definition to both **Aruba Controllers** and **Aruba Switches** (or to the group containing those devices).
Configure the Device Down condition to include both a device's **local failure** and an **upstream-device failure**.

This alarm type is intended to report an infrastructure device as down regardless of whether the device itself fails locally or becomes unreachable because of an upstream failure.

QUESTION NO: 3

A network administrator wants to permit explicit SSH, FTP and HHTP(s) access to servers in the 10.100.20.5 to 10.100.20.31 range, all devices in 10.100.21.0/24 network, and a host with IP address 10.100.22.70. The services must work properly at all times.

Which configuration scripts accomplish this task with the fewer number of lines, while avoiding access to other devices not included in these ranges? (Choose two.)

A.

```
ip access-list session access2servers
    user alias file&web_servers svc-http permit
    user alias file&web_servers svc-https permit
    user alias file&web_servers svc-ssh permit
    user alias file&web_servers svc-ftp permit
```

B.

```
netdestination file&web_servers
    host 10.100.22.70
    range 10.100.20.5 to 10.100.20.21
    range 10.100.20.22 to 10.100.20.31
    network 10.100.21.0 255.255.255.0
```

C.

```
netdestination file&web_servers
host 10.100.22.70
network 10.100.20.0 255.255.255.0
network 10.100.21.0 255.255.255.0
```

D.

```
netdestination file&web_servers
    host 10.100.22.70
    network 10.100.20.0 255.255.255.0
    network 10.100.21.0 255.255.255.0
```

E.

```
ip access-list session access2servers
    user alias file&web_servers tcp 20 permit
    user alias file&web_servers tcp 21 permit
    user alias file&web_servers tcp 22 permit
    user alias file&web_servers tcp 80 permit
    user alias file&web_servers tcp 443 permit
```

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

ANSWER: A B

Explanation:

The two correct configuration scripts are the ones that define the required destinations as an exact combination of address objects or network specifications and then apply service rules for SSH, FTP, HTTP, and HTTPS. The server range from 10.100.20.5 through 10.100.20.31 must be represented without expanding access to adjacent addresses; the full 10.100.21.0/24 subnet can be summarized as one network; and 10.100.22.70 must remain a single-host destination. This approach minimizes configuration lines by reusing grouped destination and service definitions while retaining the required precision.

FTP requires particular attention because it uses a control connection and dynamically negotiated data connections. On Aruba stateful firewall platforms, permitting the FTP service through the appropriate service/application-aware policy allows the firewall to track the FTP control session and permit its related data traffic, so the service continues to work reliably. Stateful policy handling also permits return traffic for established client sessions without creating broad, unnecessary

inbound rules. ArubaOS policy configuration uses address aliases, service aliases, and firewall policies to make such rules concise and maintainable. See the ArubaOS firewall policy documentation and the ArubaOS service alias documentation.

QUESTION NO: 4

A network administrator must provide RADIUS accounting records from a WPA2-Enterprise WLAN to ClearPass Policy Manager. ClearPass must receive accounting start and stop messages for authenticated client sessions.

Which two configuration steps are required on the Mobility Controller? (Choose two.)

A. Define ClearPass as a RADIUS accounting server.

B. Reference an accounting server group in the WLAN AAA profile.

C. Enable MAC authentication in the virtual AP profile.

D. Configure ClearPass only as the RADIUS authentication server.

E. Enable DHCP relay on the client VLAN.

ANSWER: A B

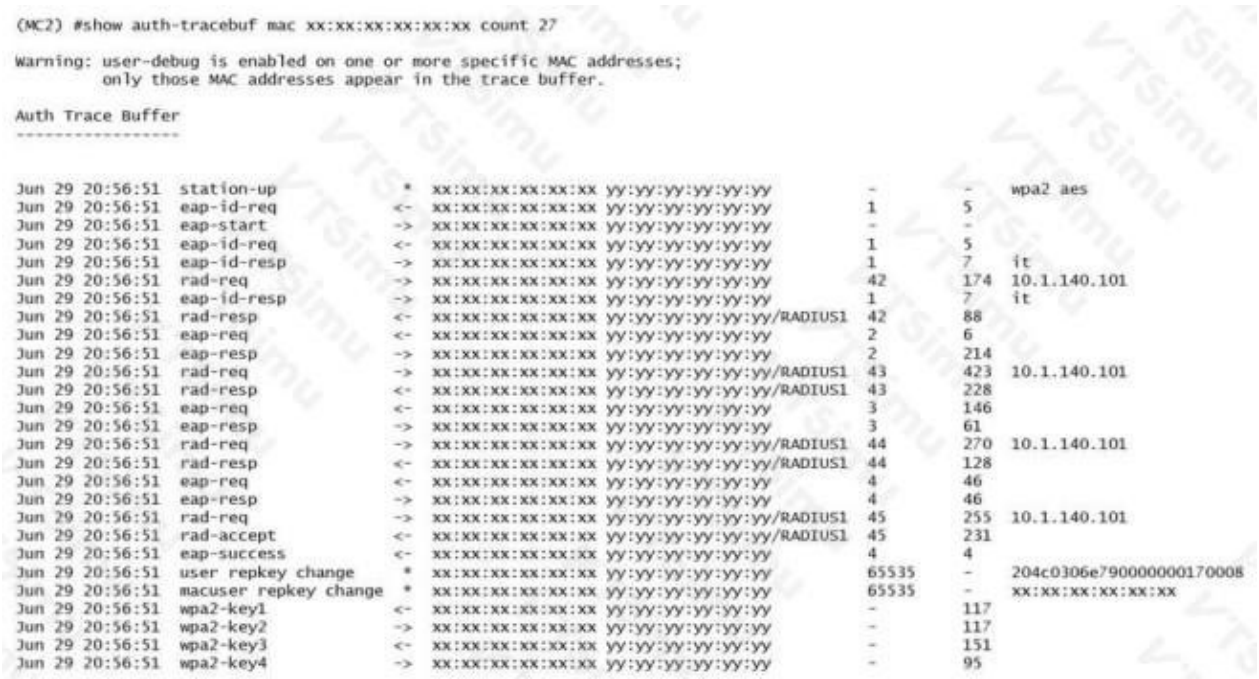
Explanation:

The administrator must define the ClearPass server as a RADIUS accounting server. This configuration establishes the destination and shared secret used by ArubaOS when sending RADIUS accounting messages.

The accounting server must then be placed in an accounting server group and that group must be referenced by the AAA profile used by the WLAN. Referencing the group in the active AAA profile applies accounting to client sessions authenticated through that WLAN. Configuring only an authentication server does not cause accounting start and stop records to be sent. Aruba RADIUS configuration concepts are covered in the ArubaOS RADIUS documentation.

QUESTION NO: 5

Refer to the exhibit.



```
(MC2) #show auth-tracebuf mac xx:xx:xx:xx:xx:xx count 27

Warning: user-debug is enabled on one or more specific MAC addresses;
         only those MAC addresses appear in the trace buffer.

Auth Trace Buffer
-----------------

Jun 29 20:56:51  station-up            *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      -    wpa2 aes
Jun 29 20:56:51  eap-id-req           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1      5
Jun 29 20:56:51  eap-start             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      -
Jun 29 20:56:51  eap-id-req           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1      5
Jun 29 20:56:51  eap-id-resp            ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1      7    it
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          42     174  10.1.140.101
Jun 29 20:56:51  eap-id-resp            ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          1      7    it
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  42     88
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          2      6
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          2      214
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  43     423  10.1.140.101
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  43     228
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          3      146
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          3      61
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  44     270  10.1.140.101
Jun 29 20:56:51  rad-resp              <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  44     128
Jun 29 20:56:51  eap-req               <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4      46
Jun 29 20:56:51  eap-resp              ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4      46
Jun 29 20:56:51  rad-req               ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  45     255  10.1.140.101
Jun 29 20:56:51  rad-accept            <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy/RADIUS1  45     231
Jun 29 20:56:51  eap-success           <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          4      4
Jun 29 20:56:51  user repkey change     *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          65535  -    204c0306e790000000170008
Jun 29 20:56:51  macuser repkey change   *  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          65535  -    xx:xx:xx:xx:xx:xx
Jun 29 20:56:51  wpa2-key1             <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      117
Jun 29 20:56:51  wpa2-key2             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      117
Jun 29 20:56:51  wpa2-key3             <-  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      151
Jun 29 20:56:51  wpa2-key4             ->  xx:xx:xx:xx:xx:xx yy:yy:yy:yy:yy:yy          -      95
```

Based on the output shown in the exhibit, which wireless connection phase has just completed?

A. L3 authentication and encryption

B. MAC Authentication and 4-way handshake

C. 802.11 enhanced open association

D. L2 authentication and encryption

ANSWER: A

Explanation:

L3 authentication and encryption has just completed. Aruba describes a client connection as progressing through distinct stages: initial 802.11 discovery and association, Layer 2 security establishment, and Layer 3 authentication/security processing. The exhibit's completed client-state information indicates that the station has already moved beyond radio association and Layer 2 link establishment and has reached the point at which the controller has finalized the higher-layer authentication result and applied the client's access policy. At this stage, the controller can place the client into its assigned role, enforce any applicable firewall or access rules, and permit normal data connectivity according to the authentication outcome. "L3 authentication" commonly encompasses captive-portal or web-based authentication and other controller-mediated user authentication processes that occur after the wireless link is established. The completion status shown in the output therefore corresponds to the final Layer 3 authentication and encryption phase rather than an earlier connection step. Aruba's authentication documentation explains the controller's role in authenticating clients and assigning authorization policies, while its WLAN security guidance describes the separation of wireless link security from later user-access controls. See ArubaOS Authentication and ArubaOS Security.

QUESTION NO: 6

A company uses an Aruba Mobility Controller WLAN with ClearPass Policy Manager. ClearPass returns multiple attributes for users in different directory groups, and the controller uses server-derived role rules to assign Aruba user roles.

Two server-derived role rules can match the same Access-Accept response. Which role does the controller assign?

A. The role associated with the first matching rule.

B. The role associated with the last matching rule.

C. A combination of all matching roles.

D. The role with the most restrictive firewall policy.

ANSWER: A

Explanation:

The controller assigns the role associated with the first matching server-derived role rule. Server-derived role rules are evaluated in their configured order, so more specific rules should be placed before broader rules that could also match the returned RADIUS attributes.

The controller does not merge all matching roles into a single role, nor does it automatically select the most restrictive or alphabetically first role. Proper rule ordering is therefore important when authorization attributes overlap. Aruba describes server-derived role assignment in the ArubaOS derivation rules documentation.

QUESTION NO: 7

Refer to the exhibit.

A network administrator has recently enabled WMM on the VAP's SSID profile and enabled UCC Skype4B ALG at the Mobility Master level. During testing, some voice and video conference calls were made, and it was concluded that the call quality has dramatically improved. However, end to end information isn't displayed in the call's details. Also, Skype4B app-sharing's performance is poor at times.

What must the administrator do next in order to enable end to end call visibility and QoS correction to app-sharing service?

A. Deploy the SDN API Software in the Skype4B Solution and point to the MM.

B. Increase the app-sharing DSCP value in the Skype4B ALG profile.

C. Enable UCC monitoring on the "default-controller" mgmt.-server profile.

D. Enable the App-sharing ALG profile at both MM and MD hierarchy levels.

ANSWER: A

Explanation:

Deploy the SDN API Software in the Skype4B Solution and point to the MM. The Skype for Business SDN interface supplies the Mobility Master with call metadata and quality telemetry from the Skype for Business environment. This data supplements the information that the controller can observe directly on the WLAN, enabling correlated end-to-end call details rather than visibility limited to the wireless portion of a media flow.

It is also important for application sharing because this traffic can use dynamically negotiated media characteristics that are not sufficiently classified by basic wireless QoS settings alone. The SDN integration communicates the application and media-flow context to Aruba's UCC services, allowing the Mobility Master to identify the application-sharing flow appropriately and apply the intended QoS treatment. WMM remains necessary for wireless prioritization, but the SDN deployment provides the Skype for Business context required for end-to-end reporting and application-aware QoS correction.

Microsoft describes how the Skype for Business Software-Defined Networking interface exposes network and media-quality information in its SDN interface documentation. Aruba UCC configuration and feature documentation is available through the Aruba technical documentation portal.

QUESTION NO: 8 - (HOTSPOT)

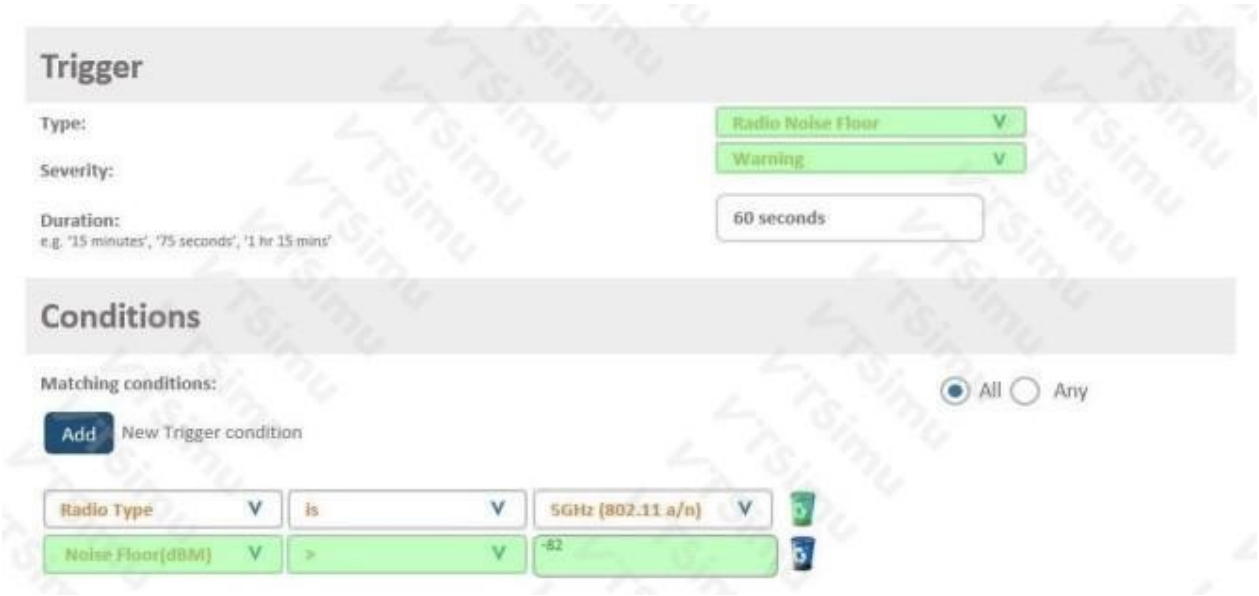
HOTSPOT

A network administrator wants to receive a warning level alarm every time the noise floor rises above -82 dBm on any of the AP radios.

Which alarm definition must the network administrator create to accomplish this?

Hot Area:

ANSWER:



Explanation:

The correct alarm definition uses the **Radio Noise Floor** trigger type, sets the severity to **Warning**, and evaluates the condition **Noise Floor(dBm) > -82**. Noise floor is the measured background RF energy at a radio. When that value rises above the selected threshold, it indicates increased ambient interference or RF noise that can reduce the signal-to-noise ratio and affect wireless client performance. A warning-severity alarm is appropriate because the administrator specifically requests a warning-level notification rather than a critical event.

The matching-condition list must contain the noise-floor threshold condition without a radio-band restriction. Leaving the condition applicable to all radio types allows the same definition to evaluate every AP radio covered by the management system. Consequently, the definition can generate the requested notification regardless of whether the affected radio operates in the 2.4 GHz or 5 GHz band. The configured duration controls how long the threshold must be met before the event is raised; the displayed 60-second duration can remain if the intended policy is to alarm after one minute of sustained elevated noise. Aruba's AirWave documentation describes configurable alerts and triggers for monitoring managed-device conditions: Aruba AirWave documentation. Aruba also provides RF-management guidance explaining the importance of monitoring RF conditions such as interference and noise: Aruba RF health documentation.

QUESTION NO: 9

Refer to the exhibits.

A user reports slow response time to a network administrator and suggests that there might be a problem with the WLAN. The userâ€™s phone supports 802.11ac in the 5 GHz band. The network administrator finds the user in the Mobility Master (MM) and reviews the output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

A. The low SNR forces the client to back off to low MCs. therefore speed is low and retransmits are high.

B. Client health is poor, but SNR is fair. TX power must be increased in both the client and the AP.

C. Since SNR is good, then the high retransmit rate must be due a hidden node scenario or high interference.

D. High Successful frame count and high Max Speed is an indication of a healthy client. Connection will improve at anytime.

ANSWER: C

Explanation:

“Since SNR is good, then the high retransmit rate must be due a hidden node scenario or high interference.” is the best conclusion from the reported client statistics. Signal-to-noise ratio measures the strength of the received Wi-Fi signal relative to the ambient noise floor. A good SNR indicates that the client has sufficient RF signal quality to use efficient 802.11ac modulation and coding rates; therefore, weak received signal is not the primary explanation for poor responsiveness. However, a high retransmission rate means that frames frequently require another transmission before they are successfully acknowledged. This condition consumes airtime, reduces effective throughput, and can create the slow application response observed by the user even where the client has a strong signal. Common RF causes include hidden clients that cannot hear one another and transmit simultaneously, as well as interference or contention that corrupts frames. The administrator should investigate channel utilization, co-channel contention, non-Wi-Fi interference, and nearby client/AP placement to identify the source of the retries. Aruba’s client-monitoring guidance and WLAN troubleshooting material provide the relevant client statistics and RF context for this analysis: ArubaOS 8.10 Documentation and Aruba Central Client Monitoring Documentation.