PassQueen
a.k.a dumpsqueen.com

Aruba Certified Edge Professional Exam

HP HPE6-A75

Version Demo

Total Demo Questions: 10

Total Premium Questions: 109

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Planning and Design	9
Topic 2, Installation and Configuration	76
Topic 3, Monitoring and Troubleshooting	24
Total	109

QUESTION NO: 1

Whichstatement is true about the Endpoint Profiler? (Select two.)

A. The Endpoint Profiler usesDHCP fingerprinting for device categorization.

B. Data obtained from the Endpoint Profiler can be used in Enforcement Policy.

C. Endpoint Profiler requires a profiling license.

D. The Endpoint Profiler requires the Onboard license to be enabled.

E. The Endpoint Profiler can only categorize laptops and desktops.

ANSWER: A B

Explanation:

The Endpoint Profiler uses DHCP fingerprinting for device categorization. ClearPass collects endpoint attributes from network activity and profiling probes, including DHCP information such as DHCP option values supplied by a client. These characteristics can be matched against profiling rules to identify or classify endpoint types. DHCP profiling is particularly useful because it can provide device-related context when an endpoint initially connects and before an agent-based posture assessment is available.

Data obtained from the Endpoint Profiler can be used in Enforcement Policy. ClearPass stores the resulting endpoint information in its endpoint repository and makes relevant endpoint attributes available during policy evaluation. Administrators can therefore build role and enforcement decisions based on a device's profiled category and attributes, applying the appropriate access controls as part of normal ClearPass Policy Manager authentication and authorization processing. This enables differentiated treatment of managed devices, printers, phones, IoT endpoints, and other categorized clients according to the organization's access policy. Aruba's ClearPass documentation describes endpoint profiling methods and endpoint attributes, while the Policy Manager documentation explains their use in enforcement-policy decisions. See Aruba ClearPass Endpoint Profiler documentation and Aruba ClearPass Enforcement Policies documentation.

QUESTION NO: 2 - (SIMULATION)

Which is a valid policy simulation types in ClearPass? (Select three.)

ANSWER: See the explanation for the answer

Explanation:

The three valid ClearPass Policy Simulation types are:

RADIUS
TACACS+
WebAuth

These simulation types let an administrator test how ClearPass service classification, role mapping, and enforcement policy rules would be processed without requiring a live authentication transaction.

QUESTION NO: 3

OSPF is configured on several routers connected to the same broadcast network. An administrator wants one router to participate in OSPF adjacency formation but never become the Designated Router (DR) or Backup Designated Router (BDR).

Which OSPF interface setting should the administrator configure on that router?

A. Set the OSPF interface cost to 0.

B. Set the OSPF interface priority to 0.

C. Configure the interface as passive.

D. Set the OSPF router ID to 0.0.0.0.

ANSWER: B

Explanation:

The administrator should configure an **OSPF priority of 0** on the interface. A router with interface priority 0 is ineligible for election as either the DR or BDR on a multi-access network. It can still form the required adjacencies and exchange link-state information with the DR and BDR.

OSPF interface priority affects only DR and BDR election eligibility; it does not prevent the router from participating in OSPF routing. The election behavior is defined in RFC 2328, section 9.4.

QUESTION NO: 4

Which statement is true about the Endpoint Profiler? (Select two.)

A. The Endpoint Profiler uses DHCP fingerprinting for device categorization.

B. Data obtained from the Endpoint Profiler can be used in Enforcement Policy.

C. Endpoint Profiler requires a profiling license.

D. The Endpoint Profiler requires the Onboard license to be enabled.

E. The Endpoint Profiler can only categorize laptops and desktops.

ANSWER: A B

Explanation:

The Endpoint Profiler uses DHCP fingerprinting for device categorization. ClearPass examines DHCP request characteristics, including the parameter request list and other DHCP attributes, to help identify and classify endpoint types. DHCP fingerprinting is one of several profiling data sources available to ClearPass, allowing it to build endpoint context from observed network behavior rather than relying only on a user-provided device description. This supports identification of a broad range of managed and unmanaged endpoints as they connect to the network.

Data obtained from the Endpoint Profiler can be used in Enforcement Policy. Profiling results are stored as endpoint attributes and can be referenced during policy evaluation. Administrators can therefore create enforcement decisions based on the endpoint category or other discovered endpoint properties, such as assigning an appropriate role, VLAN, downloadable user role, or access restriction for a recognized device class. This integration enables context-aware network access control, where authorization reflects both identity and the characteristics of the connecting device. Aruba documents Endpoint Profiler data collection and categorization in its ClearPass Endpoint Profiler documentation and explains policy actions in the Enforcement Policies documentation.

QUESTION NO: 5

Refer to the exhibit.

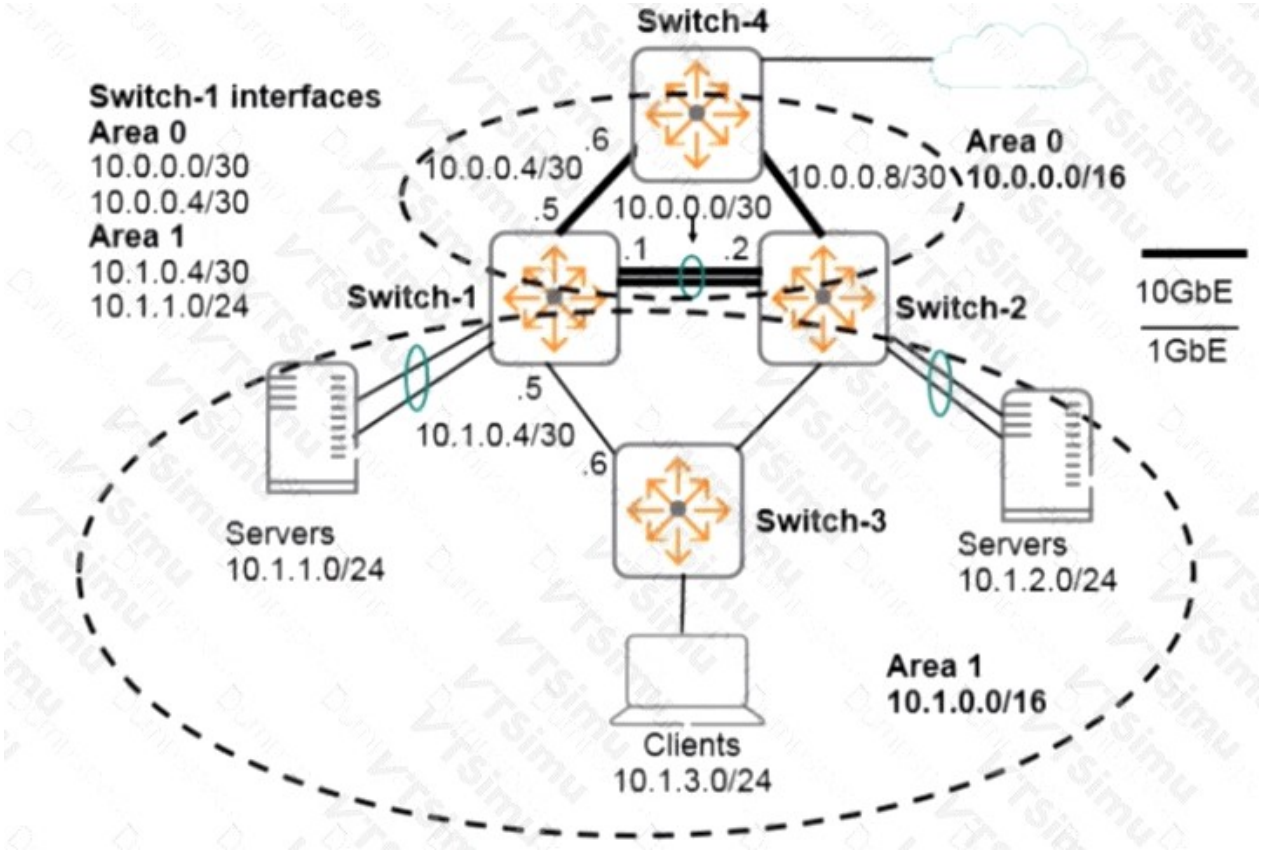

Exhibit 2

```
Switch-1# show ip route
IP Route Entries
Destination         Gateway          VLAN Type       Sub-Type     Metric     Dist.
------------------- ---------------- ---- ---------- ---------- ---------- -----
10.0.0.0/30         VLAN1000         1000 connected               5          0
10.0.0.4/30         VLAN1004         1004 connected               10         0
10.0.0.8/30         10.0.0.2         1000 ospf       IntraArea    15         110
10.1.0.4/30         VLAN104          104  connected               100        0
10.1.0.8/30         10.1.0.6         104  ospf       IntraArea    200        110
10.1.0.8/30         10.1.0.6         104  ospf       IntraArea    200        110
10.1.1.0/24         VLAN110          110  connected               50         0
10.1.2.0/24         10.1.0.6         104  ospf       IntraArea    250        110
10.1.3.0/24         10.1.0.6         104  ospf       IntraArea    200        110
10.2.0.0/16         10.0.0.6         1004 ospf       InterArea    110        110
10.3.0.0/16         10.0.0.6         1004 ospf       InterArea    110        110
127.0.0.0/8         reject                static                  0          0
127.0.0.1/32        lo0                   connected               1          0

Switch-1# show ip ospf neighbor
 OSPF Neighbor Information

Router ID       Pri IP Address      NbIfState State    QLen  Events Status
--------------- --- --------------- --------- -------- ----- ------ ------
2.2.2.2         1   10.0.0.2        BDR       FULL     0     6      None
3.3.3.3         1   10.1.0.6        BDR       FULL     0     6      None
4.4.4.4         1   10.0.0.6        BDR       FULL     0     6      None
```

Traffic between the servers m Area I takes a less optimal path rather than the link associated with VLAN I OOO, subnet 10.0.0.0/30. Based on the exhibits, why is this the case?

A. The metric on the VLAN 1000 interface is too low.

B. Switch-1 and Switch-2 cannot achieve adjacency on VLAN 1000 due to mismatches.

C. OSPF routing switches choose the best intra-area routes based on Area 1 links only.

D. The link between Switch-1 and Switch-2 has gone down.

ANSWER: C

Explanation:

OSPF gives preference to an intra-area route over an inter-area route, even when the inter-area path has a lower cumulative cost or appears physically more direct. For traffic between the servers in Area 1, the routing switches therefore use the available Area 1 topology to calculate and select an intra-area path. The VLAN 1000 link, subnet 10.0.0.0/30, does not become the preferred forwarding path for that Area 1 destination merely because it would provide a shorter route at the physical topology level.

This behavior follows OSPF's route-type preference order: intra-area routes are preferred before inter-area routes, and external route types are considered only afterward. Metrics are used to select among routes of the same route type; they do not override this fundamental preference between intra-area and inter-area OSPF routes. Consequently, the route through the Area 1 links is installed and used, producing the observed less-optimal path. This is specified in the OSPF route calculation and path-type preference rules in RFC 2328, OSPF route calculation. Aruba's OSPF implementation follows these standard OSPF area and route-selection behaviors, as documented in the AOS-CX OSPF documentation.

QUESTION NO: 6

Refer to the exhibit.

Exhibit:accp67-531

Based on the configuration for the client's certificate private key as shown, which statements accurately describe the settings? (Select two.)

A. More bits in the private key will increase security.

B. The private key for TLS client certificates is not created.

C. The private key is stored in the ClearPass server.

D. More bits in the private key will reduce security.

E. The private key is stored in the user device.

ANSWER: A E

Explanation:

"More bits in the private key will increase security." is accurate because the configured key size determines the cryptographic strength of an RSA private key. A larger RSA modulus makes the mathematical work required to derive the private key from its public key substantially more difficult. Key sizes must still be selected in accordance with the organization's security policy, certificate lifetime, device capabilities, and current cryptographic guidance. Aruba ClearPass Onboard supports configuring client-certificate key parameters as part of certificate enrollment and provisioning.

"The private key is stored in the user device." is also accurate for this configuration. The client device generates or receives and retains the private key in its local certificate/key store, while ClearPass acts as the onboarding and certificate-management service. Keeping the private key on the enrolled endpoint enables that endpoint to prove possession of the certificate during TLS-based authentication, such as EAP-TLS, without requiring the ClearPass server to hold the client's private credential. This endpoint-bound handling is a fundamental part of certificate-based client authentication and protects

the key through the operating system or available hardware-backed key storage. See the Aruba ClearPass Onboard documentation and NIST cryptographic key-strength guidance.

QUESTION NO: 7

An administrator configures a primary LMS IP address and a backup LMS IP address in an AP system profile.

When will an AP attempt to connect to the backup LMS?

A. When the primary LMS is unreachable

B. When the AP detects a new wireless client

C. When the AP radio changes channels

D. When the primary LMS reaches 50 percent CPU utilization

ANSWER: A

Explanation:

An AP attempts to connect to the **backup LMS when the primary LMS is unreachable**. The primary LMS identifies the preferred managed device for the AP's normal control-plane connection. The backup LMS provides an alternate managed-device address that the AP can use if it cannot establish or maintain connectivity to the primary LMS.

This configuration improves AP survivability during a managed-device failure or a network-path outage affecting the primary LMS. The backup LMS is not normally selected merely because it exists in the configuration; it is used when the AP cannot reach the primary LMS. Aruba documents LMS and backup-LMS configuration in the ArubaOS AP system-profile documentation.

QUESTION NO: 8

An administrator wants to use Airwave to manually add devices on the network. Where should the administrator perform this action?

A. in Device Setup

B. in Groups

C. in AMP Setup

D. in Devices

ANSWER: A

Explanation:

Manual device onboarding in Aruba AirWave is performed in **in Device Setup**. This area provides the workflow for adding individual network devices directly to AirWave rather than relying on discovery. From the Device Setup page, an administrator can select the device type, enter the device's management IP address or hostname, provide the required management credentials, and assign the device to the appropriate AirWave group. AirWave then contacts the device using the configured management protocol, validates access, and begins collecting inventory, configuration, status, and monitoring data. This workflow is especially useful when an administrator already knows the management address of an infrastructure device or wants to control exactly which devices are added and how they are initially grouped. Proper group assignment during onboarding is important because the group determines monitoring, configuration, and management settings that AirWave applies to the device. Aruba's AirWave documentation identifies the Device Setup workflow as the location for manually adding devices and describes the required device communication and credential settings. See the AirWave manual device-addition procedure and the AirWave Device Setup documentation.

QUESTION NO: 9

Refer to the exhibit.

	Conditions	Role Name
1.	(Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive
2.	(Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Windows)	Vendor
3.	(Authorization:[Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Apple)	iOS Device
4.	(Authorization:remotelab AD:UserDN EXISTS)	[Employee]
5.	(Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	HR Local
6.	(Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User
7.	(Connection:NAD-IP-Address BELONGS_TO_GROUP Remote NAD)	Remote Employee

Exhibit:aocp67-236

An AD user's department attribute is configured as *HR". The user connects on Monday using their Windows Laptop to a switch that belongs to the Device Group HQ. Which role is assigned to the user in ClearPass?

A. Executive

B. iOS Device

C. Vendor

D. Remote Employee

E. HR Local

ANSWER: D E

Explanation:

ClearPass evaluates every rule in the selected Role Mapping Policy during authentication and can assign more than one role when multiple rule conditions match. In the exhibited policy, the user's connection on Monday satisfies the condition defined for **Remote Employee**. This role is therefore included in the role list returned by role mapping for the session.

The user also matches **HR Local**. The Active Directory department value matches the configured HR pattern, and the authenticator is a switch in the **HQ** device group. Those attributes satisfy the HR-local mapping criteria shown in the exhibit. The Windows laptop characteristic does not prevent either matching role from being assigned.

The resulting role set contains both **Remote Employee** and **HR Local**. ClearPass can subsequently use either or both returned roles in Enforcement Policy rules, allowing authorization to be based on the complete set of identity, endpoint, connection, and contextual attributes rather than a single exclusive role. Aruba documents that role mapping derives roles from authentication and authorization attributes, and that matching role-mapping rules contribute roles for use by enforcement. See the ClearPass Policy Manager Role Mapping documentation and the ClearPass Enforcement Policy documentation.

QUESTION NO: 10

What is true about clustering and AP connections to cluster members?

A. The AP will always stay connected to the LMS IP address configured in the AP profile.

B. During rebalancing, the active load is redistributed first.

C. The default thresholds are 75% for the Rebalanced Threshold and 25% for the Unbalanced Threshold.

D. AP load balancing is disabled by default.

ANSWER: D

Explanation:

AP load balancing is disabled by default. In an ArubaOS cluster, cluster members can coordinate AP assignments, but automatic redistribution of APs is not enabled simply by forming the cluster. An administrator must explicitly enable the AP load-balancing feature in the cluster profile before the cluster automatically evaluates member load and moves eligible APs to achieve a more balanced distribution. This default is intentional: AP reassignment can briefly affect an AP's control-plane connection and should therefore be enabled only after the administrator has validated cluster capacity, controller reachability, and the desired balancing behavior.

When the feature is enabled, ArubaOS uses the cluster's AP load-balancing settings and thresholds to identify an imbalance and coordinate AP moves among members. This behavior is distinct from the AP's initial controller-discovery and LMS/redirection processes; clustering allows AP associations to be managed across the available cluster members rather than treating a configured LMS address as an unconditional permanent attachment. Aruba's clustering documentation describes AP load balancing as an optional cluster capability that must be configured, and the command reference documents the relevant cluster-profile configuration. See the ArubaOS AP load-balancing documentation and the ArubaOS cluster-profile CLI reference.