

# HPE6-A77<sup>Q&As</sup>

Aruba Certified ClearPass Expert Written

## Pass HP HPE6-A77 Exam with 100% Guarantee

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

<https://www.leads4pass.com/hpe6-a77.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

When is it recommended to use a certificate with multiple entries on the Subject Alternative Name?

- A. The ClearPass servers are placed in different OnGuard zones to allow the client agent to send SHV updates.
- B. Using the same certificate to Onboard clients and the Guest Captive Portal on a single ClearPass server.
- C. The primary authentication server is not available to authenticate the users.
- D. The ClearPass server will be hosting captive portal pages for multiple FQDN entries

Correct Answer: A

**QUESTION 2**

Refer to the exhibit: You are configuring an 802.1x service endpoint profiling. When the client connects to the network, ClearPass successfully profiles the client and sends Radius Change of Authorization (RCoA) but Radius Change of Authorization (RCoA) fails for the client. You manually clicked on the Change Status button in the access tracker to force an RCoA but that failed too. What must you check to ensure that the RCoA will work? (Select two.)

The screenshot shows the 'Request Details' window in ClearPass, with the 'RADIUS CoA' tab selected. The 'CoA Action# 1' section displays the following details:

Date and Time	Oct 07, 2019 12:56:12 EDT
Application Name	Policy Manager
RADIUS CoA Action Type	Disconnect
RADIUS CoA Action Name	[ArubaOS Wireless - Terminate Session]
Status Code	0
Status Message	Radius [ArubaOS Wireless - Terminate Session] failed for client 78d29437bd69.
RADIUS CoA Attributes	Calling-Station-Id = 78D29437BD69

At the bottom of the window, there are several buttons: 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'. A status bar at the bottom left indicates 'Showing 1 of 1-20 records'.



- A. RFC 3576 option is enabled for Aruba Controller under Network device in ClearPass.
- B. RFC 3576 server should be mapped in the server group on the Aruba Controller
- C. The RFC 3576 shared secret on ClearPass should match the Authentication Server shared secret
- D. RFC 3576 server IPs and the Authentication server IPs should be same in the AAA profile

Correct Answer: AC

**QUESTION 3**

A customer is looking to implement a Web-Based Health Check solution with the following requirements:

for the HR user's client devices, check if a USB stick is mounted.

for the RandD user's client devices, check if the hard disk is fully encrypted.

The Web-Based Health Check service has been configured but the customer it is not sure how to design the Profile Policy.

How can be accomplished this customer request?

- A. create two Posture Policies and customize the OnGuard Agent (Persistent or Dissolvable) to select the correct SHV

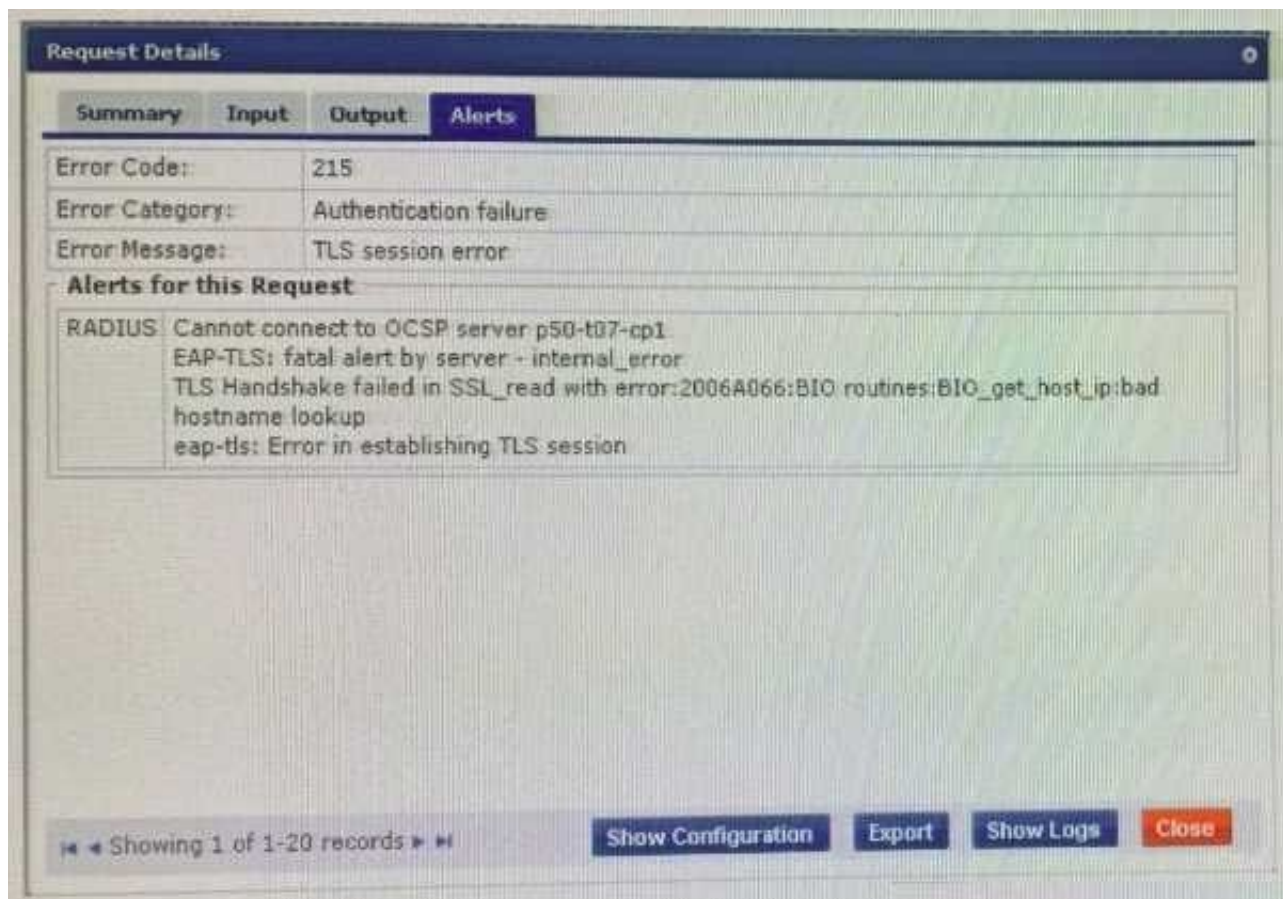
checks

- B. create one Posture Policy and define Rules Conditions that will apply different Tokens for each SHV check condition
- C. create two Posture Policies and use the Restrict by Roles option to filter for HR and RandD user roles and apply the correct SHV checks
- D. create one Posture Policy to check the HR users client devices and use the NAP Agent to check RandD users client devices

Correct Answer: A

#### QUESTION 4

Refer to the exhibit: A customer has configured Onboard in a cluster. After the Primary server's failure, the BYOD devices fail to connect to the network. What would you do to troubleshoot?



- A. Verify the OSCP URL under TLS authentication method is mapped to [http://localhost/guestmdps\\_ocsp.php/2](http://localhost/guestmdps_ocsp.php/2)
- B. Reboot the active ClearPass server and reconnect the client to the SSID by selecting the correct certificate when prompted
- C. Check EAP certificate on the secondary node is issued by the same common root Certificate Authority (CA)
- D. Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client

Correct Answer: B

---

## QUESTION 5

You are integrating a Postgres SQL server with the ClearPass Policy Manager. What steps will you follow to complete the integration process? (Select three)

- A. Click on the default filter name with pre-defined filter queries and check box to enable as role.
- B. Specify a new filter with filter queries to fetch authentication and authorization attributes.
- C. Attribute Name under filter configuration must match one of the columns being requested from the database table.
- D. Create a new Endpoint context server and add the SQL server IP, credentials and the database name.
- E. Alias Name under filter configuration must match one of the columns being requested from the database table.
- F. Create a new authentication source and add the SQL server IP, credentials and the database name.

Correct Answer: BDF

---

## QUESTION 6

Where is the following information stored in ClearPass?

1.

Roles and Posture for Connected Clients

2.

System Health for OnGuard

3.

Machine authentication State

4.

CoA session info

5.

Mapping of connected clients to NAS/NAD

A. Multi-Master cache

B. Endpoint database

C. insight database

D. ClearPass system cache

Correct Answer: D

---

**QUESTION 7**

You are deploying ClearPass Policy Manager with Guest functionality for a customer with multiple Aruba Networks Mobility Controllers. The customer wants to avoid SSL errors during guest access but due to company security policy cannot use a wildcard certificate on ClearPass or the Controllers. What is the most efficient way to configure the customer's guest solution? (Select two.)

- A. Build multiple Web Login pages with vendor settings configured for each controller
- B. Install the same public certificate on all Controllers with the common name "controller {company domain}"
- C. Build one Web Login page with vendor settings for controller {company domain}
- D. Install multiple public certificates with a different Common Name on each controller

Correct Answer: AB

---

**QUESTION 8**

Refer to the exhibit: A customer has configured a Guest Self registration page for their Cisco Wireless network with the settings shown. What should be changed in order to successfully authenticate guests users?

Home > Configuration > Pages > Self-Registrations

### Customize Self-Registration (Admin-GuestCiscoSelfReg)

Use this form to make changes to the self-registration instance Admin-GuestCiscoSelfReg.

Customize Self-Registration

**Login**  
Options controlling logging in for self-registered guests.

Enabled:  Enable guest login to a Network Access Server ▼

\* Vendor Settings: Cisco Systems ▼  
Select a predefined group of settings suitable for standard network configurations.

Login Method: Controller-initiated -- Guest browser performs HTTP form submit ▼  
Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

\* IP Address: 1.1.1.1  
Enter the IP address or hostname of the vendor's product here.

Secure Login: Use vendor default ▼  
Select a security option to apply to the web login process.

Dynamic Address:  The controller will send the IP to submit credentials.  
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

Username Suffix:   
The suffix is automatically appended to the username before logging into the NAC.

**Default Destination**  
Options for controlling the destination clients will redirect to after login.

\* Default URL:   
Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.

Override Destination:  Force default destination for all clients  
If selected, the client's default destination will be overridden regardless of its value.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

**Management**

- Summary
- SNMP
- HTTP-HTTPS
- Telnet-SSH
- Serial Port
- Local Management
- Users
- User Sessions

**HTTP-HTTPS Configuration**

HTTP Access:

HTTPS Access:

WebAuth SecureWeb:

HTTPS Redirection:

Web Session Timeout:  Minutes

Current Certificate

- A. Secure Login should use HTTP
- B. Change the Vendor Settings to Airespace Networks
- C. Change the IP Address to the Cisco Controller DNS name

D. Login Method should be Controller-initiated - using HTTPs form submit

Correct Answer: C

---

### QUESTION 9

A Customer has these requirements:

\*

2,000 IoT endpoints that use MAC authentication

\*

6,000 endpoints using a mix of username/password and certificate (Corporate/BYOD) based authentication

\*

1,000 guest endpoints at peak usage that use guest self-registration

\*

1,500 BYOD devices estimated as 3 devices per User (500 users)

\*

2,500 endpoints that have OnGuard installed and connect on a daily basis

What licenses should be installed to meet customer requirements?

- A. 11,500 Access, 500 Onboard, 2,500 OnGuard
- B. 13,000 Access, 1,500 Onboard, 2,500 OnGuard
- C. 11,500 Access, 1,500 Onboard, 2,500 OnGuard
- D. 9,000 Access, 500 Onboard, 2,500 OnGuard

Correct Answer: C

---

### QUESTION 10

A customer would like to allow only the AD users with the "Manager" title from the "HQ" location to Onboard their personal devices. Any other AD users should not be authorized to pass beyond the initial device provisioning page.

Which Onboard service will you use to implement this requirement?

- A. Onboard CP login service
- B. Onboard Authorization service



C. Onboard Provisioning service

D. Onboard Pre-Auth service

Correct Answer: A

[HPE6-A77 PDF Dumps](#)

[HPE6-A77 Exam Questions](#)

[HPE6-A77 Braindumps](#)