



HPE6-A81^{Q&As}

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

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

<https://www.passapply.com/hpe6-a81.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**

Refer to the exhibit: You 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.)

Request Details

Summary Input Output Alerts **RADIUS CoA**

CoA Action# 1

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

Showing 1 of 1-20 records

Change Status Show Configuration Export Show Logs Close



Request Details

No response from network device

Summary Input Output Alerts

Login Status:	ACCEPT
Session Identifier:	R00000180-01-5d9b61af
Date and Time:	Oct 07, 2019 12:02:55 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	HS_Building-802.1x service
Authentication Method:	EAP-PEAP
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	[Endpoints Repository], AD1, AD2, Corp SQL
Roles:	[User Authenticated]
Enforcement Profiles:	Aruba Limited Access for Profiling
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-6 records

Change Status Show Configuration Export Show Logs Close

- 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 2

What is the Open SSID (otherwise referred to as Dual SSID) Onboard deployment service workflow?

- A. OnBoard Pre-Auth Application service, OnBoard Authorization Application service. OnBoard Provisioning RADIUS service
- B. OnBoard Pre-Auth RADIUS service. OnBoard Authorization Application service. OnBoard Provisioning RADIUS service
- C. OnBoard Authorization Application service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service
- D. OnBoard Authorization RADIUS service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service



Correct Answer: C

QUESTION 3

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 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?

The screenshot shows a 'Request Details' window with tabs for Summary, Input, Output, and Alerts. The Alerts tab is selected, displaying the following information:

Error Code:	215
Error Category:	Authentication failure
Error Message:	TLS session error

Alerts for this Request

```
RADIUS: Cannot connect to OCSP server p50-t07-cp1  
EAP-TLS: fatal alert by server - internal_error  
TLS Handshake failed in SSL_read with error:2006A066:BIO routines:BIO_get_host_ip:bad  
hostname lookup  
eap-tls: Error in establishing TLS session
```

At the bottom of the window, there is a status bar indicating 'Showing 1 of 1-20 records' and buttons for 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

- A. Verify the OCSP URL under TLS authentication method is mapped to `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 have configured a Guest SSID with Captive-portal Web Authentication and MAC authentication. The MAC caching expiry time is set to 12 hours and the Guest Account expiration time is set to 8 hours. What will happen if the guest were to disconnect from the SSID and re-connect 9 hours later?

A. The client will fail the MAC authentication and be denied access to the Guest SSID.

B. The client will successfully pass the MAC authentication until the MAC caching time expires.

C. The client will successfully pass the MAC authentication but still be redirected to the captive portal page.

D. The client will fail the MAC authentication and will be redirected to the Captive-portal login page.

Correct Answer: C

[Latest HPE6-A81 Dumps](#)

[HPE6-A81 PDF Dumps](#)

[HPE6-A81 Braindumps](#)