



HPE6-A77^{Q&As}

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.geekcert.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

Refer to the exhibit:

Request Details

Summary Input Output Alerts

Login Status:	ACCEPT
Session Identifier:	R0000001e-01-5d9ef61c
Date and Time:	Oct 10, 2019 05:13:00 EDT
End-Host Identifier:	20-4c-03-5b-4a-d2
Username:	204c035b4ad2
Access Device IP/Port:	10.1.70.5:3 (HPE Aruba switch / Hewlett-Packard-Enterprise)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	HPE-Aruba Wired Mac auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Endpoints Repository]
Roles:	[User Authenticated]
Enforcement Profiles:	Assign Switch role PROFILE
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-20 records

Change Status Show Configuration Export Show Logs Close

Request Details

Summary Input Output Alerts

Enforcement Profiles:	Assign Switch role PROFILE
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Hewlett-Packard-Enterprise:HPE-User-Role Profile



```
P50-T7-2930(config)# sho port-access clients
```

```
Port Access Client Status
```

Port	Client Name	MAC Address	IP Address	User Role	Type

VLAN					

3	204c035b4ad2	204c03-5b4ad2	n/a	denyall	MAC
70					

```
P50-T7-2930(config)# show user-role
```

```
User Roles
```

```
Enabled      : Yes  
Initial Role : denyall
```

Type	Name
local	PROFILE
predefined	denyall
local	AP-ACCESS

```
P50-T7-2930(config)#
```

Configuration > Services > Edit - HPE-Aruba Wired Mac auth

Services - HPE-Aruba Wired Mac auth

Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler
Use Cached Results:	<input checked="" type="checkbox"/> Use cached Roles and Posture attributes from previous sessions					
Enforcement Policy:	HPE-ArubaOS Mac auth policy					Modify
Add New Enforcement Policy						
Enforcement Policy Details						
Description:						
Default Profile:	[Deny Access Profile]					
Rules Evaluation Algorithm:	first-applicable					
Conditions			Enforcement Profiles			
1. {Authorization:[Endpoints Repository]:Category NOT_EXISTS }			Assign Switch role PROFILE			
2. {Authorization:[Endpoints Repository]:Category EQUALS Access Points}			Assign Aruba switch role AP-ACCESS			
AND {Authorization:[Endpoints Repository]:OS Family EQUALS Aruba}						

You have been asked to help a Customer troubleshoot an issue. They have configured an Aruba OS switch (Aruba 2930 with 16.09) to do MAC authentication with profiling using ClearPass as the authentication source. They cannot get it working.

Using the screenshots as a reference, how will you fix the issue?

A. Delete the initial role in the Aruba OS switch to force the device to get the server derived user roles



- B. Use a CoA to bounce the switch port to force the port to change to the correct Aruba user role
- C. Change the Vendor settings for the Aruba OS switch to "Aruba" so that the enforcement will use the correct VSAs
- D. Modify the enforcement profile conditions with Aruba Vendor specific attributes and Aruba-user- roles
- E. User-roles are case sensitive, update the correct role with correct case in the enforcement profile

Correct Answer: D

QUESTION 2

Refer to the exhibit:

Monitoring » Live Monitoring » Access Tracker

Access Tracker Aug 21, 2019 20:03:29 CEST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] default (2 servers) Last 1 day before Today

Filter: Source contains Webauth Go Clear Filter

#	Server	Source	Username	Service	Login Status	Request Timestamp
21.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:18:03
22.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:15:06
23.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:12:11
24.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:09:14
25.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:06:19
26.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:03:23
27.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:00:28
28.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:57:31
29.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:54:36
30.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:51:41
31.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:48:44
32.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:45:49
33.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:42:54
34.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:39:56
35.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:37:00
36.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:34:05
37.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:31:10
38.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:28:15
39.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:25:19
40.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:22:23



A customer has just configured a Posture Policy and the T2-Healthcheck Service. Next they installed the OnGuard Agent on Secure_Employee SSID. When they check Access Tracker they see many WEBAUTH requests are being triggered.

What could be the reason?

- A. OnGuard Web-Based Health Check interval has been wrongly configured to three minutes.
- B. The OnGuard Agent trigger the events based on changing the Health Status
- C. TCP port 6658 is not allowed between the client and the ClearPass server
- D. The OnGuard Agent is connecting to the Data Port interface on ClearPass

Correct Answer: A

QUESTION 3

You have configured a Guest SSID with Captive-portal Web Authentication and MAC authentication The MAC caching expiry time 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 captive portal page.
- D. The client will fail the MAC authentication and will be redirected to the Captive-portal login page.

Correct Answer: C

QUESTION 4

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 5

What is used to validate the EAP Certificate? (Select three.)

- A. Common Name
- B. Date
- C. Key usage
- D. Server Identity
- E. SAN entries
- F. Trust chain



VCE & PDF

GeekCert.com

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

2024 Latest geekcert HPE6-A77 PDF and VCE dumps Download

Correct Answer: ACF

[Latest HPE6-A77 Dumps](#)

[HPE6-A77 Practice Test](#)

[HPE6-A77 Braindumps](#)