



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.geekcert.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

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 2

Refer to the exhibit: You are doing a ClearPass PoC at a customer site with a single Aruba Mobility Controller. The customer asked for a demonstration of a simple Web Login functionality. You used a service template to create the guest services. During testing, the user gets redirected back to the weblogin page with an Authentication failed message. The guest configurations on the Aruba Mobility Controller are configured correctly. Why would the guest fail to authenticate successfully?



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

Services - HPE-Aruba Wired Mac auth

Summary Service Authentication Authorization Roles **Enforcement** Profiler

Use Cached Results: 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) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Aruba)	Assign Aruba switch role AP-ACCESS

Configuration > Service Templates & Wizards

Service Templates - Guest Authentication with MAC Caching

General Wireless Network Settings MAC Caching Settings Posture Settings **Access Restrictions**

- Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields.
- Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired.
- At least one of Employee, Guest, and Contractor Access must be provided.

Enforcement Type*: Aruba Role Enforcement

Captive Portal Access*: gueaths-login

Days allowed for access*: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Maximum number of devices allowed per user*: 0

Maximum bandwidth allowed per user*: 0 MB (For unlimited bandwidth, set value to 0)

Employee Access:

Guest Access: Lab-Guest

Contractor Access:

Back to Service Templates & Wizards Delete Next Add Service Cancel

Configuration > Services > Edit - Guest User Authentication with MAC Caching

Services - Guest User Authentication with MAC Caching

Summary Service Authentication Authorization Roles **Enforcement**

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Guest User Authentication with MAC Caching Enforcement Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Allow Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 0)	[Deny Access Profile]
2. (Tips:Role EQUALS [Guest]) AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	Guest MAC Caching Session Timeout, Guest MAC Caching Bandwidth Limit, Guest MAC Caching Session Limit, Guest Guest MAC Caching, [Update Endpoint Known], Guest MAC Caching Do Expire, Guest MAC Caching Expire Post Login, Guest Guest Profile

A. The authentication source mapped in the service is incorrect, it should be mapped as (Guest Device Repository)



[Local SQL DB].

B. The username and/or password used for authentication is incorrect Re-enter the correct password on the weblogin page.

C. The username used for authentication does not exist in the Guest User Database Create a new user and authenticate again.

D. The Unique-Device-Count does not allow any Client devices. Update the Enforcement policy condition: Unique-Device-Count.

Correct Answer: A

QUESTION 3

Refer to the exhibit:

The screenshot displays a 'Request Details' window with a tabbed interface. The 'Summary' tab is active, showing the following details:

Field	Value
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)

Below the main details, there is a section titled 'Policies Used -' with the following information:

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

At the bottom of the window, there is a navigation bar with the text 'Showing 1 of 1-20 records' and several buttons: 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and '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)#
```



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 4

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

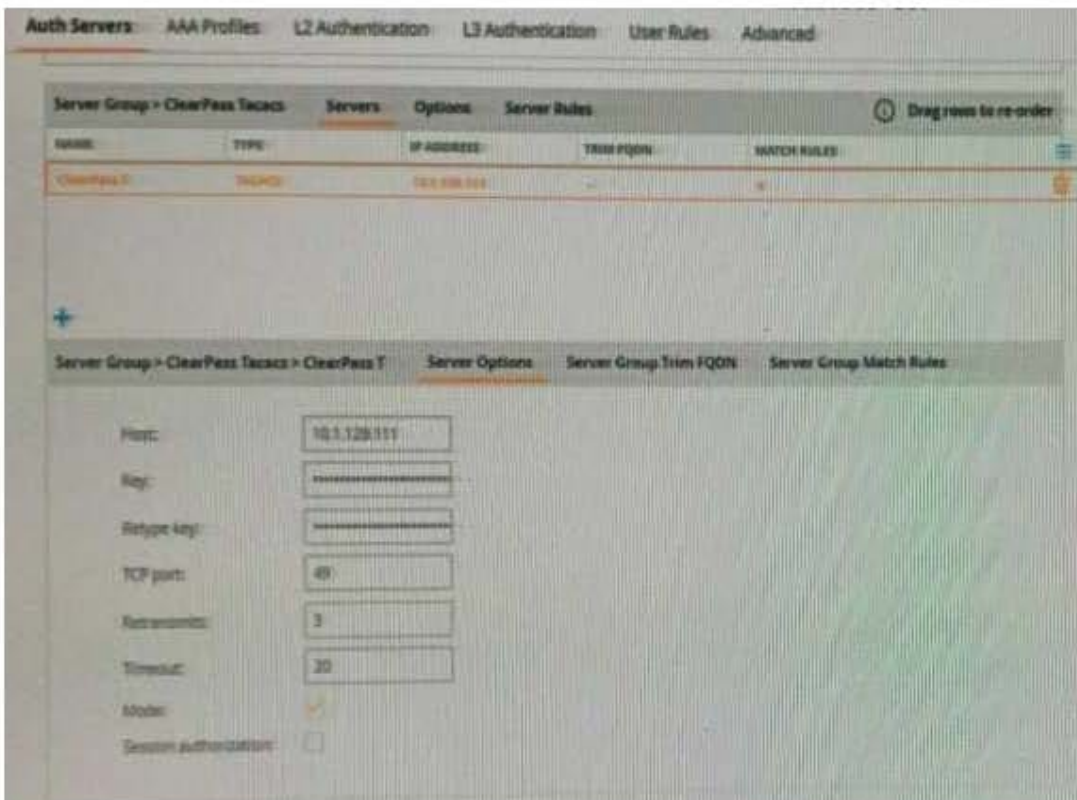
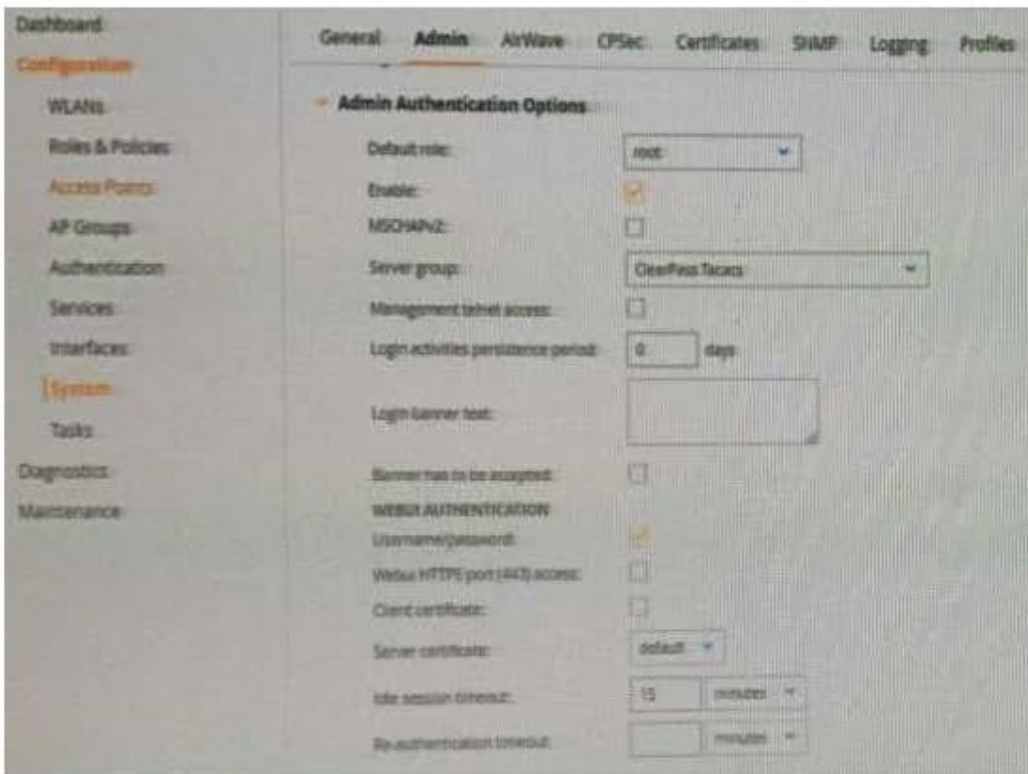
QUESTION 5

Refer to the exhibit:

The screenshot displays the 'TACACS+ Session Details' window with the 'Policies' tab selected. It shows a table of policies used for a session.

Policies Used -	
Service Name:	[Aruba Device Access Service]
Authentication Source:	[Local User Repository]
Role:	[User Authenticated], [Aruba TACACS read-only Admin]
Profiles:	[ArubaOS Wireless - TACACS Read-Only Access]

At the bottom of the window, there is a navigation bar with the text 'Showing 2 of 1-2 records' and three buttons: 'Export', 'Show Logs', and 'Close'.





```
10.1.29.100 - PuTTY
(HPE6-A81-MC) [admin@hpe6-a81:~]$ show sessions
Sessions Table
-----
ID   User Name  User Role  Connection From  Idle Time  Session Time  Path
-----
1    admin      root       10.1.29.90       00:00:10   00:00:42     /
2    read-only  root       10.1.29.90       00:00:39   00:00:45     /
3    admin      root       10.1.29.90       00:00:23   00:12:14     /
```

A customer has configured the Aruba Controller for administrative authentication using ClearPass as a TACACS server. During testing, the read-only user is getting the root access role. What could be a possible reason for this behavior? (Select two.)

- A. The Controller's Admin Authentication Options Default role is mapped to root.
- B. The ClearPass user role associated to the read-only user is wrong
- C. The Controller Server Group Match Rules are changing the user role
- D. The read-only enforcement profile is mapped to the root role
- E. On the Controller, the TACACS authentication server is not configured for Session authorization

Correct Answer: CE

[HPE6-A81 Practice Test](#)

[HPE6-A81 Study Guide](#)

[HPE6-A81 Exam Questions](#)