



# HPE6-A68<sup>Q&As</sup>

Aruba Certified ClearPass Professional (ACCP) V6.7

## Pass HP HPE6-A68 Exam with 100% Guarantee

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

<https://www.geekcert.com/hpe6-a68.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.

Configuration » Enforcement » Policies » Edit - Vlan enforcement	
<b>Enforcement Policies - Vlan enforcement</b>	
Summary	Enforcement
Rules	
<b>Enforcement:</b>	
Name:	Vlan enforcement
Description:	
Enforcement Type:	RADIUS
Default Profile:	Internet VLAN
<b>Rules:</b>	
Rules Evaluation Algorithm:	First applicable
Conditions	Actions
1. (Tips: Role EQUALS Engineer AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Connection:Protocol EQUALS RADIUS)	Full Access VLAN
2. (Tips: Role EQUALS Manager) AND (Connection:Protocol BELONGS_TO RADIUS, TACACS, WEBAUTH, Application)	Full Access VLAN
3. (Tips: Role EQUALS Engineer AND (Connection:Protocol BELONGS_TO WEBAUTH)	Employee VLAN

Based on the Policy configuration shown, which VLAN will be assigned when a user with ClearPass role Engineer authenticates to the network successfully on Saturday using connection protocol WEBAUTH?

- A. Full Access VLAN
- B. Employee VLAN
- C. Internet VLAN
- D. Deny Access

Correct Answer: B



## QUESTION 2

A client's authentication is failing and there are no entries in the ClearPass Access tracker. What is a possible reason for the authentication failure?

- A. The user account has expired.
- B. The client used a wrong password.
- C. The shared secret between the NAD and ClearPass does not match.
- D. The user's certificate is invalid.
- E. The user is not found in the database.

Correct Answer: C

## QUESTION 3

Refer to the exhibit.

Configuration » Identity » Role Mappings » Edit - [Guest Roles]

### Role Mappings - [Guest Roles]

Summary Policy **Mapping Rules**

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Role Mapping Rules:

Conditions	Role Name
1. (GuestUser:Role ID EQUALS 1)	[Contractor]
2. (GuestUser:Role ID EQUALS 2)	[Guest]
3. (GuestUser:Role ID EQUALS 3)	[Employee]
4. (GuestUser:Role ID EQUALS 4)	Test guest role creation

Based on the Guest Role Mapping Policy shown, what is the purpose of the Role Mapping Policy?

- A. to display a role name on the Self-registration receipt page
- B. to send a firewall role back to the controller based on the Guest User's Role ID
- C. to assign Controller roles to guests
- D. to assign three roles of [Contractor], [Guest] and [Employee] to every guest user
- E. to create additional account roles for guest administrators to assign to guest accounts

Correct Answer: C



#### QUESTION 4

A ClearPass administrator wants to make Enforcement decisions during 802.1x authentication based on a client's Onguard posture token. Which Enforcement profile should be used on the health check service?

- A. RADIUS CoA
- B. Quarantine VLAN
- C. Full Access VLAN
- D. RADIUS Accept
- E. RADIUS Reject

Correct Answer: A

The Health Check Service requires a profile to terminate the session so that the RADIUS 802.1X authentication Service can use the posture token in a new authentication routine. The terminate session profile will utilize the Change of

Authorization feature to force a re-authentication.

See step 6) below.

1.

Navigate to the list of Enforcement Profiles by selecting, Configuration > Enforcement > Profiles.

2.

Click the + Add link in the upper right hand corner.

3.

From the Template dropdown menu, choose RADIUS Change of Authorization (CoA).

4.

Name the policy.

This example uses Dell Terminate Session as the profile name.

5.

Leave all the other settings as default, and click Next > to move to the Attributes tab.

6.

On the dropdown menu for Select RADIUS CoA Template, choose IETF-Terminate-Session-IETF.

7.

Click Next > and review the Summary tab (Figure 22).

8.

Click Save.



References: ClearPass NAC and Posture Assessment for Campus Networks Configuring ClearPass OnGuard, Switching, and Wireless (v1.0) (September 2015), page 22

[http://en.community.dell.com/cfs-file/\\_key/telligent-evolution-components-attachments/13-4629-00-00-20-44-16-18/ClearPass-NAC-and-Posture-Assessment-for-Campus-Networks.pdf?forcedownload=true](http://en.community.dell.com/cfs-file/_key/telligent-evolution-components-attachments/13-4629-00-00-20-44-16-18/ClearPass-NAC-and-Posture-Assessment-for-Campus-Networks.pdf?forcedownload=true)

## QUESTION 5

Refer to the exhibit.

Type	Name	Value
1. Radius:IETF	Session-Timeout (27)	= 600
2. Click to add...		

An Enforcement Profile has been created in the Policy Manager as shown. Which action will ClearPass take based on the Enforcement Profile? A. It will send the Session-Timeout attribute in the RADIUS Access-Request packet to the NAD and the NAD will end the user's session after 600 seconds.

B. It will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the User and the user's session will be terminated after 600 seconds.

C. It will count down 600 seconds and send a RADIUS CoA message to the NAD to end the user's session after this time is up.

D. It will count down 600 seconds and send a RADIUS CoA message to the user to end the user's session after this time is up.

E. It will send the session -Timeout attribute in the RADIUS Access-Accept packet to the NAD and the NAD will end the user's session after 600 seconds.

Correct Answer: E

[HPE6-A68 VCE Dumps](#)

[HPE6-A68 Study Guide](#)

[HPE6-A68 Exam Questions](#)