

HPE6-A15^{Q&As}

Aruba Certified Clearpass Professional 6.5

Pass HP HPE6-A15 Exam with 100% Guarantee

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

<https://www.pass2lead.com/hpe6-a15.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.

The screenshot displays a simulation configuration interface. At the top, there are three tabs: 'Simulation', 'Attributes', and 'Results'. The 'Simulation' tab is selected. Below the tabs, there are several input fields: 'Name' (test), 'Description' (empty), 'Type' (Role Mapping), 'Service' (Table6 Wireless Service hello), 'Role Mapping Policy' (AD Role mapping policy), 'Authentication Source' (remote lab AD), 'Username' (test1), and 'Test Date and Time' (empty). Below this is a 'Policy Simulation' section with three tabs: 'Simulation', 'Attributes', and 'Results'. The 'Results' tab is selected. Underneath, there is a 'Summary -' section with a 'Roles' field containing the text 'AD User, Engineering, Software Engineer, [User Authenticated]'.

Which statement accurately reflects the status of the Policy Simulation test figure shown?

- A. The test verifies that a client with username test1 can authenticate using EAP-PEAP.
- B. Role mapping simulation verifies if the remote lab AD has the ClearPass server certificate.
- C. Role mapping simulation verifies that the client certificate is valid during EAP-TLS authentication.
- D. The simulation test result shows the firewall roles assigned to the client by the Aruba Controller.
- E. The roles assigned in the results tab are based on rules matched in the AD Role Mapping Policy.

Correct Answer: E

QUESTION 2

Refer to the exhibit.

Summary	Input	Output
Session Identifier:		W00000024-01-515a5f14
Date and Time:		Apr 02, 2013 04:31:17 UTC
End-Host Identifier:		4c60def412ee
Username:		4c60def412ee
Access Device IP/Port:		-
System Posture Status:		HEALTHY (0)
Policies Used -		
Service:		Health Check for clients
Authentication Method:		Not applicable
Authentication Source:		-
Authorization Source:		-
Roles:		[Guest]
Enforcement Profiles:		[Aruba Terminate Session]
Service Monitor Mode:		Disabled

Based on the Access Tracker output for the user shown, which statement describes the status?

- A. The Aruba Terminate Session enforcement profile as applied because the posture check failed.
- B. A Healthy Posture Token was sent to the Policy Manager.
- C. A RADIUS-Access-Accept message is sent back to the Network Access Device.
- D. The authentication method used is EAP-PEAP.
- E. A NAP agent was used to obtain the posture token for the user.

Correct Answer: B

We see System Posture Status: HEALTHY(0)

End systems that pass all SHV tests receive a Healthy Posture Token, if they fail a single test they receive a Quarantine Posture Token.

References: CLEARPASS ONGUARD CONFIGURATION GUIDE (July 2015), page 13

<https://community.arubanetworks.com/aruba/attachments/aruba/aaa-nac-guest-access-byod/21122/1/OnGuard%20config%20Tech%20Note%20v1.pdf>

QUESTION 3

DRAG DROP

Use the arrows to sort the steps to request a Policy on the left into the order they are performed on the right.

Select and Place:

Steps to Request a Policy Service

- ClearPass tests the request against Service Rules to select a Policy Service
- ClearPass applies the Enforcement Policy
- ClearPass sends the Enforcement Profile attributes to the NAD
- NAD forwards authentication request to ClearPass

Order Performed

← ↑

→ ↓

Correct Answer:

Steps to Request a Policy Service

-
-
-
-

Order Performed

- NAD forwards authentication request to ClearPass
- ClearPass tests the request against Service Rules to select a Policy Service
- ClearPass applies the Enforcement Policy
- ClearPass sends the Enforcement Profile attributes to the NAD

← ↑

→ ↓

QUESTION 4

A customer wants all guests who access a company's guest network to have their accounts approved by the receptionist, before they are given access to the network. How should the network administrator set this up in ClearPass? (Select two.)

- A. Enable sponsor approval confirmation in Receipt actions.
- B. Configure SMTP messaging in the Policy Manager.
- C. Configure a MAC caching service in the Policy Manager.

- D. Configure a MAC auth service in the Policy Manager.
- E. Enable sponsor approval in the captive portal authentication profile on the NAD.

Correct Answer: AD

A: Sponsored self-registration is a means to allow guests to self-register, but not give them full access until a sponsor (could even be a central help desk) has approved the request. When the registration form is completed by the guest/user, an on screen message is displayed for the guest stating the account requires approval.

Guests are disabled upon registration and need to wait on the receipt page for the confirmation until the login button gets enabled.

D. Device Mac Authentication is designed for authenticating guest devices based on their MAC address.

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 94 <https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf>

QUESTION 5

A customer with an Aruba Controller wants it to work with ClearPass Guest.

How should the customer configure ClearPass as an authentication server in the controller so that guests are able to authenticate successfully?

- A. Add ClearPass as a RADIUS CoA server.
- B. Add ClearPass as a RADIUS authentication server.
- C. Add ClearPass as a TACACS+ authentication server.
- D. Add ClearPass as an HTTPS authentication server.

Correct Answer: B

5. Configuring the Aruba Controller

5.1 Add Clearpass as RADIUS Server

Navigate to Configuration > SECURITY > Authentication > Servers Click on RADIUS Server and enter the Name of your Clearpass Server: myClearpass Click Add Click on myClearpass in the Server List Etc.

References: <https://community.arubanetworks.com/t5/Security/Step-by-Step-Controller-CPPM-6-5-Captive-Portal-authentication/td-p/229740>