

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.pass2lead.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:

Request Details

Summary | Input | Output | Alerts

| | |
|------------------------|--|
| Login Status: | ACCEPT |
| Session Identifier: | R00000238-01-5d9dd0b2 |
| Date and Time: | Oct 09, 2019 08:21:07 EDT |
| End-Host Identifier: | 78D29437BD69 (Computer / Windows / Windows 10) |
| Username: | alex07 |
| Access Device IP/Port: | 10.1.70.100:0 (ArubaController / Aruba) |
| System Posture Status: | HEALTHY (0) |

Policies Used -

| | |
|------------------------|---|
| Service: | HS_Building Aruba 802.1x service |
| Authentication Method: | EAP-PEAP,EAP-MSCHAPv2 |
| Authentication Source: | AD:AD1.aruba1.local |
| Authorization Source: | [Endpoints Repository], AD1, Corp SQL |
| Roles: | [Machine Authenticated], [Other], [User Authenticated] |
| Enforcement Profiles: | Redirect to Aruba OnBoard Portal, Aruba Full Access 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: | Redirect to Aruba OnBoard Portal, Aruba Full Access Profile |
| System Posture Status: | HEALTHY (0) |
| Audit Posture Status: | UNKNOWN (100) |

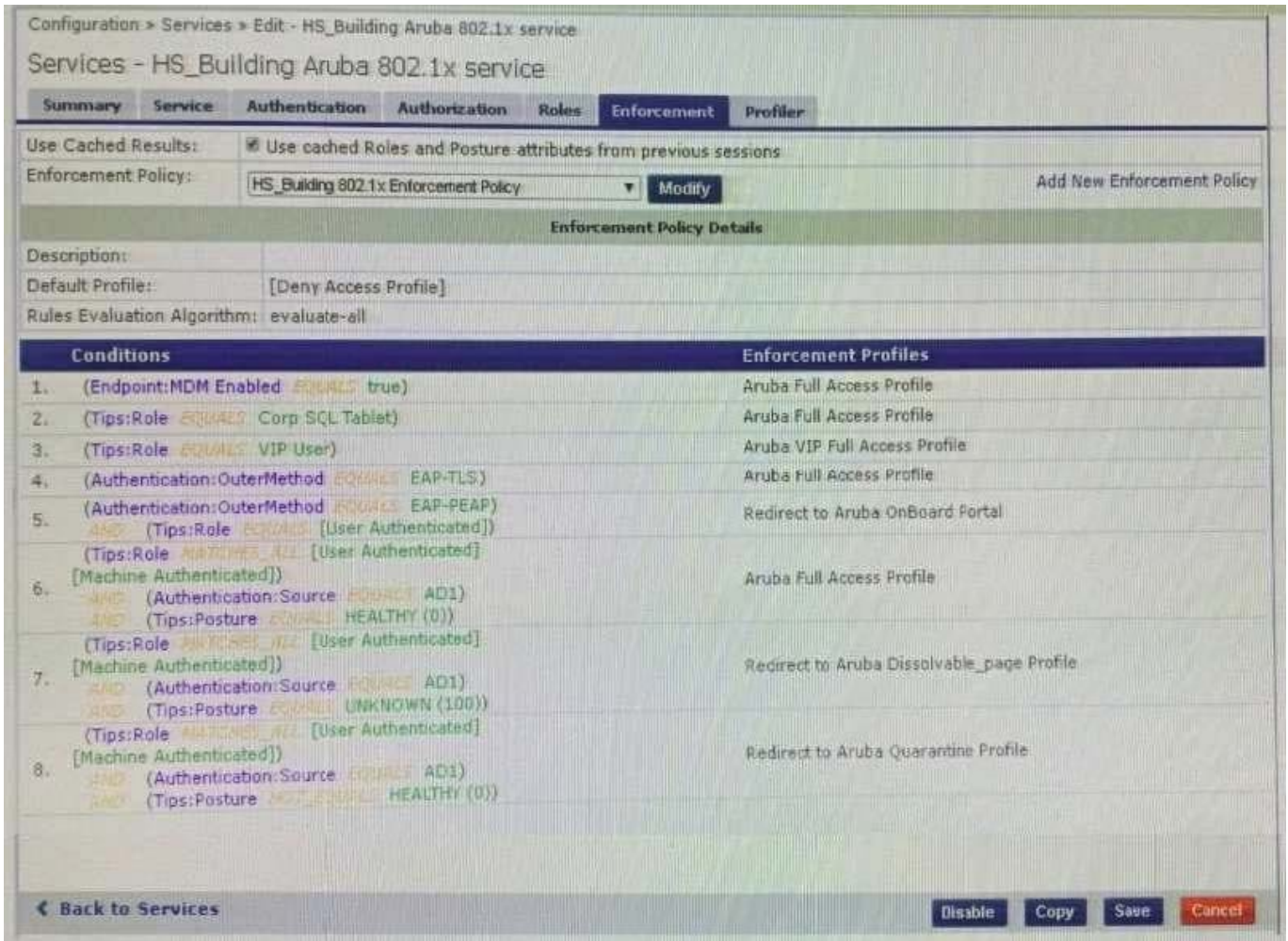
RADIUS Response

| |
|---|
| Radius:Aruba:Aruba-User-Role BYOD-Provision |
|---|

Posture Evaluation Results

Showing 1 of 1-20 records

Change Status Show Configuration Export Show Logs Close



The customer configured an 802.1x service with different enforcement actions for personal and corporate laptops. The corporate laptops are always being redirected to the BYOD Portal. The customer has sent you the above screenshots.

How would you resolve the issue? (Select two)

- A. Modify the enforcement policy and change the rule evaluation algorithm to select first match
- B. Modify the enforcement policy and re-order the condition with posture not_equals to healthy as the sixth condition
- C. Modify the enforcement policy and re-order the EAP-PEAP with [user authenticated] rule to the last condition.
- D. Modify the enforcement policy and re-order the condition with Posture - Unknown as the fifth condition
- E. Remove the EAP-PEAP with [user authenticated] condition for Onboard and create another service

Correct Answer: CD

QUESTION 2

A customer has a ClearPass cluster deployment with one Publisher and one Subscriber configured as a Standby

Publisher at the Headquarters DataCenter They also have a large remote site that is connected with an Aruba SD Branch solution over a two Mbps Internet connection. The Remote Site has two ClearPass servers acting as Subscribers. The solution implemented for the customer includes OnGuard, Guest Self Registration, and Employee 802.1x authentication. The client is complaining that users connecting to an IAP Clusters Guest SSID located at the Remote Site are experiencing a significant delay in accessing the Guest Captive Portal page. What could be a possible cause of this behavior?

- A. The configuration of the captive portal is pointing to a link located on one of the servers in the Headquarters
- B. The ClearPass Cluster has no zones defined and the guest captive portal request is being redirected to the Publisher
- C. The guest page is not optimized to work with the client browser and a proper theme should be applied
- D. The captive portal page was only created on the Publisher and requests are getting redirected to a Subscriber

Correct Answer: A

QUESTION 3

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 4

Refer to the exhibit: A customer has configured a Guest Self registration page for their Cisco Wireless network with the settings shown. What should be changed in order to successfully authenticate guests users?

Home > Configuration > Pages > Self-Registrations

Customize Self-Registration (Admin-GuestCiscoSelfReg)

Use this form to make changes to the self-registration instance Admin-GuestCiscoSelfReg.

Customize Self-Registration

Login
Options controlling logging in for self-registered guests.

Enabled: Enable guest login to a Network Access Server

* Vendor Settings: Cisco Systems
Select a predefined group of settings suitable for standard network configurations.

Login Method: Controller-initiated -- Guest browser performs HTTP form submit
Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

* IP Address: 1.1.1.1
Enter the IP address or hostname of the vendor's product here.

Secure Login: Use vendor default
Select a security option to apply to the web login process.

Dynamic Address: The controller will send the IP to submit credentials
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

Username Suffix:
The suffix is automatically appended to the username before logging into the NAC.

Default Destination
Options for controlling the destination clients will redirect to after login.

* Default URL:
Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.

Override Destination: Force default destination for all clients
If selected, the client's default destination will be overridden regardless of its value.



The screenshot shows the Cisco Management Console interface. At the top, there is a navigation bar with the Cisco logo and menu items: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The main content area is titled "HTTP-HTTPS Configuration" and contains several settings:

- HTTP Access: Enabled
- HTTPS Access: Enabled
- WebAuth SecureWeb: Disabled
- HTTPS Redirection: Disabled
- Web Session Timeout: 30 Minutes
- Current Certificate: (link)

On the left side, there is a "Management" sidebar with a tree view showing: Summary, SNMP, HTTP-HTTPS (selected), Telnet-SSH, Serial Port, Local Management, Users, and User Sessions.

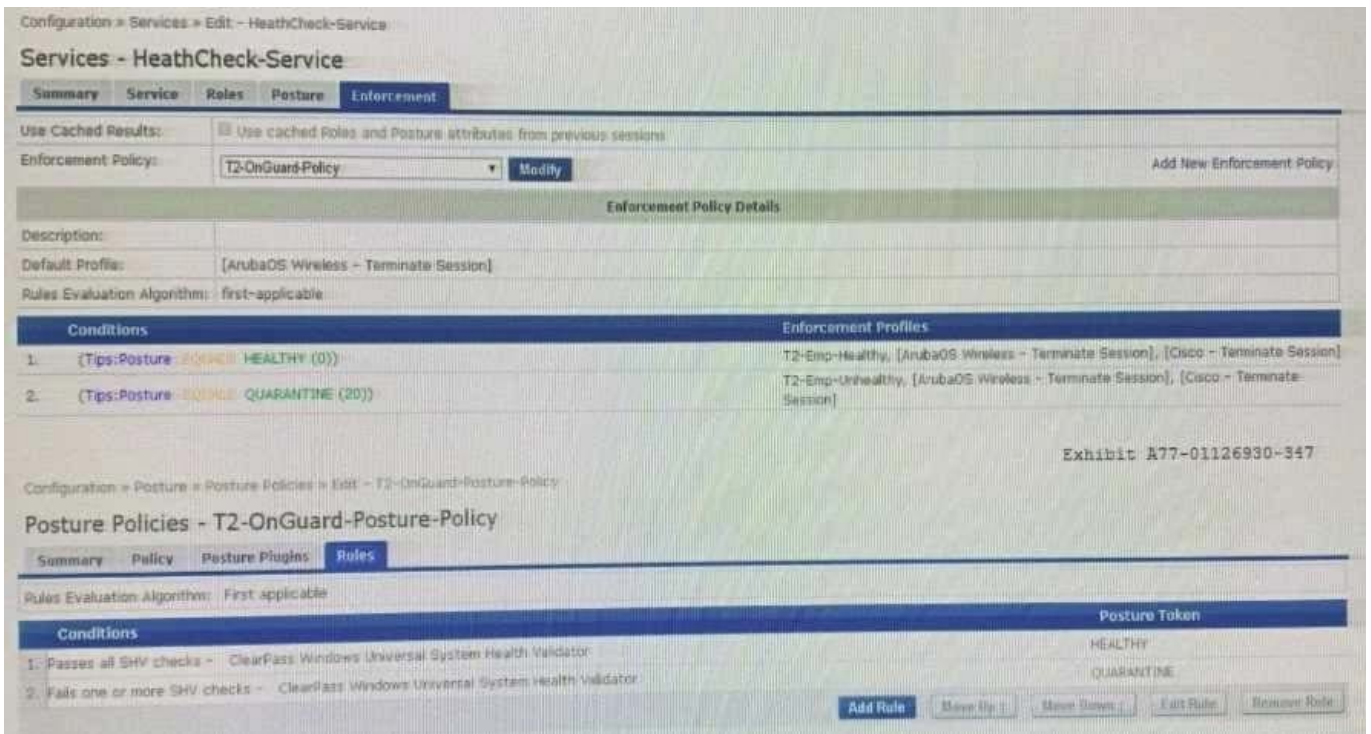
- A. Secure Login should use HTTP
- B. Change the Vendor Settings to Airespace Networks
- C. Change the IP Address to the Cisco Controller DNS name

D. Login Method should be Controller-initiated - using HTTPs form submit

Correct Answer: C

QUESTION 5

Refer to the Exhibit:



A customer wants to integrate posture validation into an Aruba Wireless 802.1X authentication service

During testing, the client connects to the Aruba Employee Secure SSID and is redirected to the Captive Portal page where the user can download the OnGuard Agent. After the Agent is installed, the client receives the Healthy token, the client remains connected to the Captive Portal page. ClearPass is assigning the endpoint the following roles: T2-Staff-User, (Machine Authenticated!) and T2-SOL-Device. What could cause this behavior?

- A. The Enforcement Policy conditions for rule 1 are not configured correctly.
- B. Used Cached Results: has not been enabled in the Aruba 802.1X Wireless Service
- C. RFC-3576 is not configured correctly on the Aruba Controller and does not update the role.
- D. The Enforcement Profile should bounce the connection instead of a Terminate session

Correct Answer: B

[HPE6-A81 Study Guide](#)

[HPE6-A81 Exam Questions](#)

[HPE6-A81 Braindumps](#)