

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.pass2lead.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: 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.)





- 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 2

Refer to the exhibit:

Request Details

Summary | Input | Output | Alerts

Login Status:	REJECT
Session Identifier:	R00000218-01-5d9db68b
Date and Time:	Oct 09, 2019 06:29:34 EDT
End-Host Identifier:	78D29437BD68 (Computer / Windows / Windows 10)
Username:	andy07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	HS_Building Aruba 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	AD1
Roles:	[Other], [User Authenticated]
Enforcement Profiles:	[Deny Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-20 records | Show Configuration | Export | Show Logs | Close

Request Details

Summary | Input | Output | Alerts

Error Code:	206
Error Category:	Authentication failure
Error Message:	Access denied by policy

Alerts for this Request

RADIUS	Applied 'Reject' profile
--------	--------------------------

Configuration > Services > Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary Service Authentication Roles Enforcement Profiler

Service:

Name: HS_Building Aruba 802.1x service
 Description: 802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete
 Type: Aruba 802.1X Wireless
 Status: Enabled
 Monitor Mode: Disabled
 More Options: Profile Endpoints

Service Role

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-5007

Authentication:

Authentication Methods: 1. [EAP PEAP]
 2. HS_Branch_[EAP TLS With OCSP Enabled]
 Authentication Sources: 1. [Onboard Devices Repository]
 2. AD1
 3. AD2
 Strip Username Rules: /:user
 Service Certificate: -

Roles:

Role Mapping Policy: HS_Building Role Mapping Policy

Enforcement:

Use Cached Results: Enabled
 Enforcement Policy: HS_Building 802.1x Enforcement Policy

Profiler:

Endpoint Classifications: ANY
 RADIUS CoA Action: [ArubaOS Wireless - Terminate Session]

[← Back to Services](#) [Disable](#) [Copy](#) [Save](#) [Cancel](#)

Configuration > Services > Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary Service Authentication Roles Enforcement Profiler

Role Mapping Policy: HS_Building Role Mapping Policy Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: [Other]

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Connection:Client-Mac-Address BELONGS_TO_GROUP VIP User MAC)	VIP User
2. (Authorization:Corp SQL:MAC EXISTS)	Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category EQUALS VoIP Phone)	IP Phone
4. (Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)	Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category EQUALS Point of Sale devices)	Vending Machine
6. AND (Authorization:[Endpoints Repository]:Category EQUALS Printer)	Printer
AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS CANON INC.)	
7. AND (Authorization:[Endpoints Repository]:Category EQUALS Network Camera)	IP Camera
AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS Axis Communications AB)	

Configuration > Services > Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary Service Authentication Roles Enforcement Profiler

Use Cached Results: Use cached Roles and Posture attributes from previous sessions Add New Enforcement Policy

Enforcement Policy: HS_Building 802.1x Enforcement Policy Modify

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
2. (Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
3. (Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
4. (Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile
(Tips:Role MATCHES ALL [User Authenticated]) [Machine Authenticated])	Aruba Full Access Profile
5. AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0))	Aruba Full Access Profile
(Tips:Role MATCHES ALL [User Authenticated]) [Machine Authenticated])	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
6. AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100))	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
(Tips:Role MATCHES ALL [User Authenticated]) [Machine Authenticated])	Redirect to Aruba Quarantine Profile
7. AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	Redirect to Aruba Quarantine Profile

Your company has a postgres SQL database with the MAC addresses of the company-owned tablets. You have configured a role mapping condition to tag the SQL devices. When one of the tablets connects to the network, it does not get the correct role and receives a deny access profile.

How would you resolve the issue?

- A. Remove SQL condition from role mapping policy and add it under the enforcement policy conditions.
- B. Edit the SQL authentication source niter attributes and modify the SQL server filter query.
- C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.
- D. Enable authorization tab in the service and add the SQL server as an authorization source.

Correct Answer: B

QUESTION 3

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:
Select a predefined group of settings suitable for standard network configurations.

Login Method:
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:
Enter the IP address or hostname of the vendor's product here.

Secure Login:
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.

| | | | |
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

Management

- Summary
- SNMP
- HTTP-HTTPS
- Telnet-SSH
- Serial Port
- Local Management
- Users
- User Sessions

HTTP-HTTPS Configuration

HTTP Access	<input type="text" value="Enabled"/>
HTTPS Access	<input type="text" value="Enabled"/>
WebAuth SecureWeb	<input type="text" value="Disabled"/>
HTTPS Redirection	<input type="text" value="Disabled"/>
Web Session Timeout	<input type="text" value="30"/> Minutes
Current Certificate	

- 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 4

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

Correct Answer: ACF

QUESTION 5

There is an Aruba Controller configured to send Guest AAA requests to ClearPass. If the customer would like the most effective way to ensure the lowest license usage counts, how should the controller be configured?

- A. Aruba Controller will send stop messages only if EAP termination and Interim accounting are enabled.
- B. Aruba Controller will send stop messages if RADIUS Accounting Server Group is defined in the authentication profile.
- C. Aruba Controller will send stop messages only if both accounting and interim accounting are enabled.
- D. Configure EAP Termination on the Aruba Controller and the client will send a stop message.

Correct Answer: D

[Latest HPE6-A77 Dumps](#)

[HPE6-A77 Practice Test](#)

[HPE6-A77 Exam Questions](#)