



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.pass4itsure.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.)

CoA Action# 1	
Date and Time	Oct 07, 2019 12:56:12 EDT
Application Name	Policy Manager
RADIUS CoA Action Type	Disconnect
RADIUS CoA Action Name	[ArubaOS Wireless - Terminate Session]
Status Code	0
Status Message	Radius [ArubaOS Wireless - Terminate Session] failed for client 78d29437bd69
RADIUS CoA Attributes	Calling-Station-Id = 78D29437BD69



The screenshot shows a 'Request Details' window with a status message 'No response from network device'. It contains a table with the following data:

Summary	Input	Output	Alerts
Login Status:	ACCEPT		
Session Identifier:	R00000180-01-5d9b61af		
Date and Time:	Oct 07, 2019 12:02:55 EDT		
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)		
Username:	alex07		
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	HS_Building 802.1x service		
Authentication Method:	EAP-PEAP		
Authentication Source:	AD:AD1.aruba1.local		
Authorization Source:	[Endpoints Repository], AD1, AD2, Corp SQL		
Roles:	[User Authenticated]		
Enforcement Profiles:	Aruba Limited Access for Profiling		
Service Monitor Mode:	Disabled		
Online Status:	Not Available		

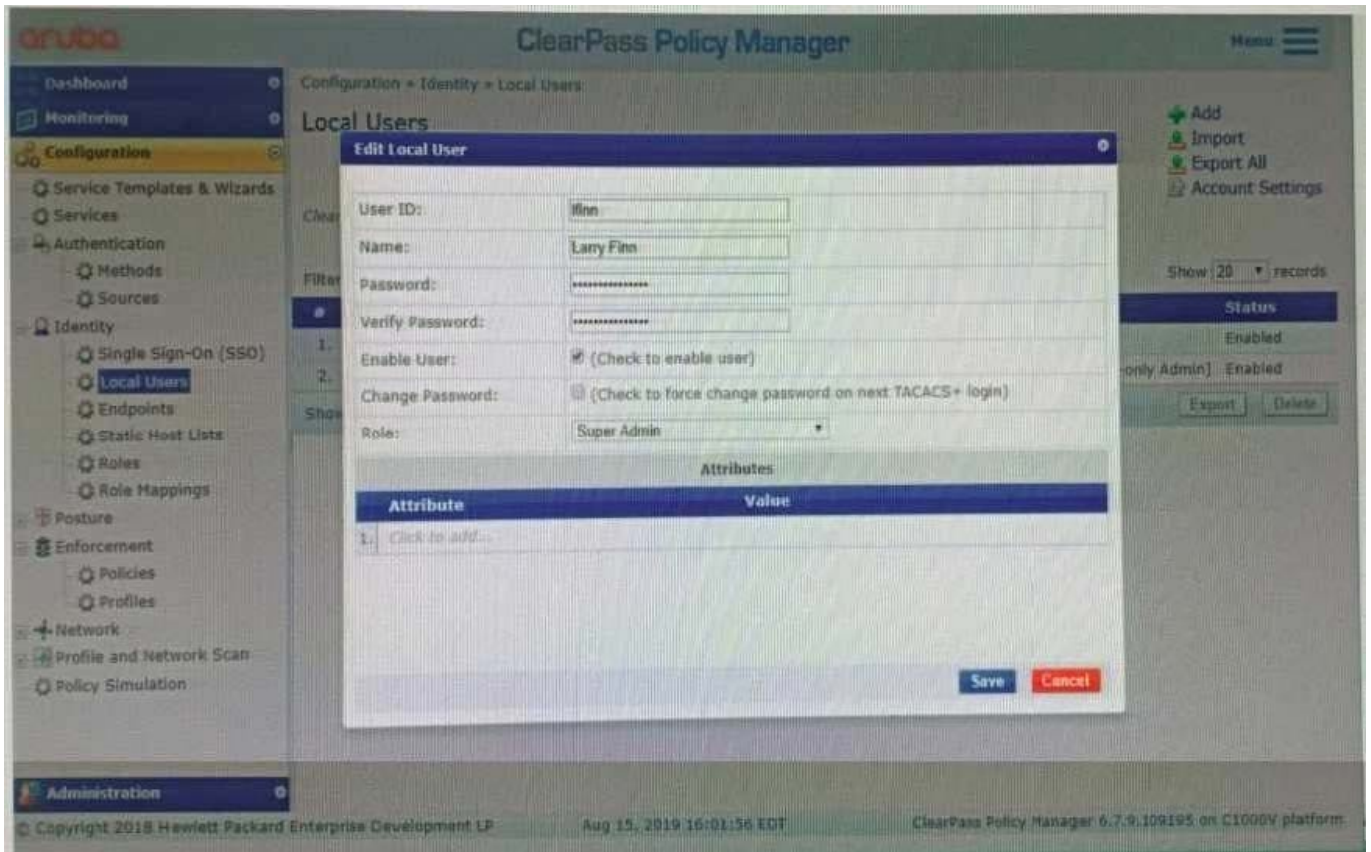
At the bottom, there are navigation buttons: 'Showing 1 of 1-6 records', 'Change Status' (highlighted with a red box), 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

- 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:



The customer complains that the user shown cannot log into the ClearPass Server as an administrator using the [Policy Manager Admin Network Login Service]. What could be the reason for this?

- A. The user might be used for a TACACS authentication
- B. The account created does not fit this purpose.
- C. The mapping on the role should be changed to [RADIUS Super Admin]
- D. The local user authentication might be disabled

Correct Answer: B

QUESTION 3

You have Integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment to sign the Anal device TLS certificates The Onboard provisioning process completes successfully but when the user finally clicks connect, the user falls to connect to the network with an unknown_ca certificate error. What steps will you follow to complete the requirement?

- A. Make sure that the ClearPass servers are using the default self-signed certificates for both SSL and RADIUS server identity
- B. Add the ADCS root certificate to both the CPPM Certificate trust list and to the Onboard Certificate Store trust list
- C. Make sure both the ClearPass servers have different certificates used for both SSL and RADIUS server identity.



D. Export the self-signed certificate from the ClearPass servers and manually add them as trusted certificates in clients

Correct Answer: A

QUESTION 4

Refer to the exhibit:



Configuration » Services » Edit - ACCX Aruba Device Access Service

Services - ACCX Aruba Device Access Service

- Summary
- Service
- Authentication
- Roles
- Enforcement**

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

Enforcement Policy: Aruba NAD Tacacs Modify

Enforcement Policy Details

Description:

Default Profile: [TACACS Deny Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Tips:Role READONLY [Aruba TACACS read-only Admin])	[TACACS Read-only Admin]
2. (Tips:Role ADMIN [Aruba TACACS root Admin])	[TACACS Network Admin]

#	Server	Source	Username	Service	Login Status
1.	10.1.129.1	TACACS	read-only	ACCX Aruba Device Access Service	REJECT

TACACS+ Session Details

- Summary
- Request
- Policies
- Alerts

Session ID: T00000006-01-5d55aba6

Username: read-only

Time: Aug 15, 2019 14:59:50 EDT

Status: AUTHEN_STATUS_FAIL

Authorizations: 0

Showing 1 of 1-6 records

Export Show Logs Close



#	Server	Source	Username	Service	Login Status
1	10.2.129.1	TACACS	read-only	AGC/ Aruba Device Access Service	REJECT

TACACS+ Session Details

Summary Request Policies Alerts

Authentication Request Messages

Error Category:	Tacacs authentication
Error Code:	Authentication privilege level mismatch

Alerts for this Request:

Tacacs server	Requested priv_level=□ greater than Max Allowed priv_level=□
---------------	--

Showing 1 of 1-6 records

Export Show Logs Close



Configuration » Enforcement » Profiles » Edit Enforcement Profile - [TACACS Read-only Admin]

Enforcement Profiles - [TACACS Read-only Admin]

Summary Profile **Services**

Privilege Level: 1 (Normal)

Selected Services: cpass:HTTP Remove Export All TACACS+ Services Dictionaries

Authorize Attribute Status: ADD

Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary.xml - Update TACACS+ Services Dictionary

Service Attributes			
Type	Name	=	Value
1. cpass:HTTP	AdminPrivilege	=	Read-only Administrator
2. Click to add...			

A customer is trying to configure a TACACS Authentication Service for administrative access to the Aruba Controller, During testing the authentication is not successful.

Given the screen shot what could be the reason for the Login status REJECT?

- A. The password used by the administrative user, user is wrong.
- B. The Enforcement profile is not designed to be used on Aruba Controller.
- C. The Read-only Administrator role does not exist on the Controller.
- D. The Enforcement profile used is not a TACACS profile.

Correct Answer: A

QUESTION 5

A corporate ClearPass Cluster with two servers located at a single site, has both Management and Data port IP addresses configured. The Management port IPs are in the DataCenter networks subnet, while the Data port IPs are in the DMZ. What is the difference between using one Virtual IP for the AAA traffic versus sending AAA requests to the physical IPs for each server? (Select two.)

- A. The failover can be accomplished only by using Virtual IP.
- B. The Individual IPs can provide failover and load balancing.
- C. One Virtual IP can be used together with the individual server IPs for load balancing.
- D. By using the Virtual IP, the failover convergence is faster than using individual server IPs.
- E. Using the one Virtual IP can provide failover and load balancing.

Correct Answer: BE



VCE & PDF

Pass4itSure.com

<https://www.pass4itsure.com/hpe6-a77.html>

2024 Latest pass4itsure HPE6-A77 PDF and VCE dumps Download

[HPE6-A77 VCE Dumps](#)

[HPE6-A77 Study Guide](#)

[HPE6-A77 Exam Questions](#)