



# HPE6-A81<sup>Q&As</sup>

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.passapply.com/hpe6-a81.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

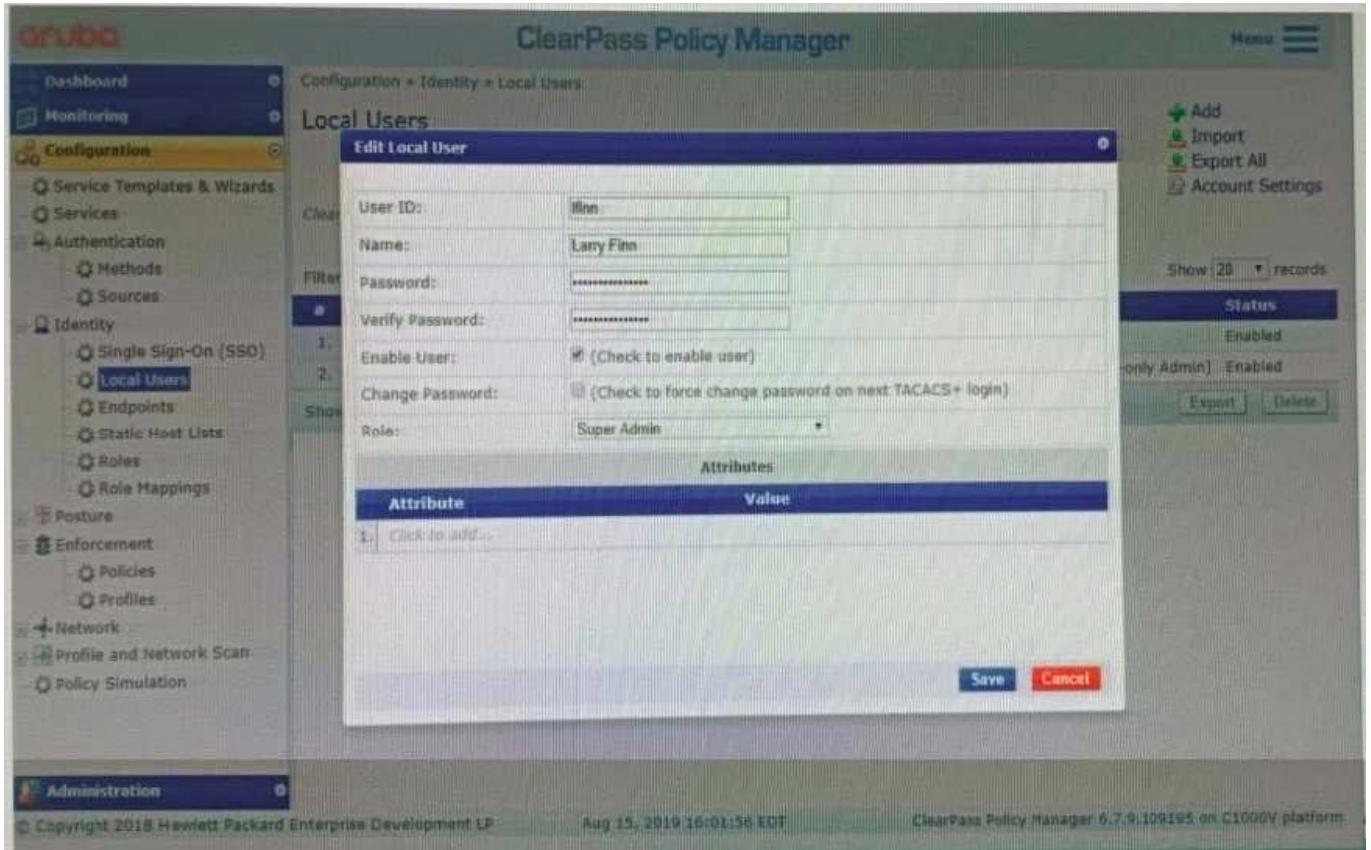
-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

Refer to the exhibit:



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 2

Refer to the exhibit:



aruba

Please login to the network using your username and password.  
To create a new account click [Create Account](#).

**Login**

Username:   
Invalid username or password

Password:

Terms:  I accept the terms of use

**Log In**

Contact a staff member if you are experiencing difficulty logging in.

Exhibit: A77-01126930-058

Request Details

Summary Input Output Alerts

Login Status:	REJECT
Session Identifier:	W0000000c-01-5d88e82b
Date and Time:	Sep 23, 2019 11:43:40 EDT
End-Host Identifier:	-
Username:	accx@exam.com
Access Device IP/Port:	*:*
System Posture Status:	-

Policies Used -

Service:	-
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	-
Enforcement Profiles:	-
Service Monitor Mode:	-
Online Status:	Not Available

Showing 1 of 1-18 records

Show Configuration Export Show Logs Close

Request Details

Summary Input Output Alerts

Error Code:	204
Error Category:	Authentication failure
Error Message:	Failed to classify request to service

Alerts for this Request

WebAuthService:	ServiceClassification failed (No service matched)
-----------------	---





Configuration > Services > Edit - ACCX Guest Access

### Services - ACCX Guest Access

Summary | Service | Authentication | Roles | Enforcement

**Service:**

Name: ACCX Guest Access  
 Description: To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.  
 Type: RADIUS Enforcement ( Generic )  
 Status: Enabled  
 Monitor Mode: Disabled  
 More Options: -

**Service Rule**

Match ALL of the following conditions:

	Type	Name	Operator
1.	Radius:IETF	Calling-Station-Id	EXISTS
2.	Connection	Client-Mac-Address	NOT_EQUALS
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS

**Authentication:**

Authentication Methods: 1. [PAP]  
 2. [MSCHAP]  
 3. [CHAP]  
 Authentication Sources: [Guest User Repository]  
 Strip Username Rules: -  
 Service Certificate: -

**Roles:**

Role Mapping Policy: [Guest Roles]

**Enforcement:**

Use Cached Results: Disabled



Home > Configuration > Pages > Web Logins  
Web Login (ACCX\_LabTest)

Use this form to make changes to the Web Login ACCX\_LabTest.

Web Login Editor	
* Name:	ACCX_LabTest <small>Enter a name for this web login page.</small>
Page Name:	ACCX_TestPage <small>Enter a page name for this web login. The web login will be accessible from "/guestpage_name.php".</small>
Description:	<input type="text"/> <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	Aruba Networks <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	Controller-initiated — Guest browser performs HTTP form submit <small>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.</small>
* Address:	securelogin.arubanetworks.com <small>Enter the IP address or hostname of the vendor's product base.</small>
Secure Login:	Use vendor default <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials. <small>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.</small>
<b>Page Redirect</b> <small>Options for specifying parameters passed in the initial redirect.</small>	
Security Hash:	Do not check — login will always be permitted <small>Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.</small>
<b>Login Form</b> <small>Options for specifying the behaviour and content of the login form.</small>	
Authentication:	Credentials — Require a username and password <small>Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted.</small>

Security Hash:	Do not check — login will always be permitted <small>Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.</small>
<b>Login Form</b> <small>Options for specifying the behaviour and content of the login form.</small>	
Authentication:	Credentials — Require a username and password <small>Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.</small>
Prevent CNA:	<input checked="" type="checkbox"/> Enable bypassing the Apple Captive Network Assistant <small>The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.</small>
Custom Form:	<input type="checkbox"/> Provide a custom login form <small>If selected, you must supply your own HTML login form in the Header or Footer HTML areas.</small>
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages <small>If selected, you will be able to alter labels and error messages for the current login form.</small>
* Pre-Auth Check:	App Authentication — check using Aruba Application Authentication <small>Select how the username and password should be checked before proceeding to the RADIUS authentication.</small>
Terms:	<input checked="" type="checkbox"/> Require a Terms and Conditions confirmation <small>If checked, the user will be forced to accept a Terms and Conditions checkbox.</small>

A year ago, your customer deployed an Aruba ClearPass Policy Manager Server for a Guest SSID hosted in an IAP Cluster. The customer just created a new Web Login Page for the Guest SSID. Even though the previous Web Login



page worked test with the new Web Login Page are falling and the customer has forwarded you the above screenshots.

What recommendation would you give the customer to fix the issue?

- A. The service type configured is not correct. The Guest authentication should be an Application authentication type of service.
- B. The customer should reset the password for the username accx@exam.com using Guest Manage Accounts
- C. The Address filed under the WebLogin Vendor settings is not configured correctly, it should be set to instant.arubanetworks.com
- D. The WebLogin Pre-Auth Check is set to Aruba Application Authentication which requires a separate application service on the policy manager

Correct Answer: A

---

### QUESTION 3

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

---

### QUESTION 4

Refer to the exhibit:





**Request Details**

Summary | Input | Output | Alerts

Login Status:	<b>REJECT</b>
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 Classification: 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 <b>BELONGS_TO_GROUP</b> VIP User MAC)	VIP User
2. (Authorization:Corp SQL:MAC <b>EXISTS</b> )	Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> VoIP Phone)	IP Phone
4. (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> SmartDevice)	Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> Point of Sale devices)	Vending Machine
6. <b>AND</b> (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> Printer)	Printer
<b>AND</b> (Authorization:[Endpoints Repository]:MAC Vendor <b>EQUALS</b> CANON INC.)	
7. <b>AND</b> (Authorization:[Endpoints Repository]:Category <b>EQUALS</b> Network Camera)	IP Camera
<b>AND</b> (Authorization:[Endpoints Repository]:MAC Vendor <b>EQUALS</b> 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 <b>EQUALS</b> true)	Aruba Full Access Profile
2. (Authentication:OuterMethod <b>EQUALS</b> EAP-PEAP) <b>AND</b> (Tips:Role <b>EQUALS</b> Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
3. (Authentication:OuterMethod <b>EQUALS</b> EAP-TLS) <b>AND</b> (Tips:Role <b>EQUALS</b> Corp SQL Tablet)	Aruba Full Access Profile
4. (Tips:Role <b>EQUALS</b> VIP User)	Aruba VIP Full Access Profile
(Tips:Role <b>MATCHES</b> ALL [User Authenticated]) [Machine Authenticated])	Aruba Full Access Profile
5. <b>AND</b> (Authentication:Source <b>EQUALS</b> AD1) <b>AND</b> (Tips:Posture <b>EQUALS</b> HEALTHY (0))	Aruba Full Access Profile
(Tips:Role <b>MATCHES</b> ALL [User Authenticated]) [Machine Authenticated])	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
6. <b>AND</b> (Authentication:Source <b>EQUALS</b> AD1) <b>AND</b> (Tips:Posture <b>EQUALS</b> UNKNOWN (100))	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
(Tips:Role <b>MATCHES</b> ALL [User Authenticated]) [Machine Authenticated])	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7. <b>AND</b> (Authentication:Source <b>EQUALS</b> AD1) <b>AND</b> (Tips:Posture <b>NOT_EQUALS</b> 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 5

A customer has completed all the required configurations in the Windows server in order for Active Directory Certificate Services (ADCS) to sign Onboard device TLS certificates. The Onboard portal and the Onboard services are also configured. Testing shows that the Client certificates are still signed by the Onboard Certificate Authority and not ADCS. How can you help the customer with the situation?

- A. Educate the customer that, when integrating with Active Directory Certificate Services (ADCS) the Onboard CA will be the same authority used for signing the final TLS certificate of the device.
- B. Configure the identity certificate signer as Active Directory Certificate Services and enter the ADCS URL `http://ADCSVVeolEnrollmentServemostname/certsrv` in the OnBoard Provisioning settings.
- C. Enable access to EST servers from the Certificate Authority to make ClearPass Onboard use the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.
- D. Enable access to SCEP servers from the Certificate Authority to make ClearPass Onboard use the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

Correct Answer: C

[HPE6-A81 Study Guide](#)

[HPE6-A81 Exam Questions](#)

[HPE6-A81 Braindumps](#)