



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: You have configured Onboard but me customer could not onboard one of his devices and has sent you the above screenshots. How could you resolve the issue?

-	already provisioned the maximu	
	Oruba NETWORKS	Onboard Wizard
	Welcome Configure Connect	ERROR The current Onboard configuration contains errors preventing you from enrolling. Please contact your network administrator.
	Summary	The log for your configuration session can be found here

A. Instruct the user to delete the profile on one of their other BYOD devices.

B. Instruct the user to run the Quick connect application in Sponsor Mode.

- C. Increase the maximum number of devices allowed by the individual user account.
- D. Increase the maximum number of devices that all users can provision to 3.

Correct Answer: D

# **QUESTION 2**

You are integrating a Postgres SQL server with the ClearPass Policy Manager. What steps will you follow to complete the integration process? (Select three)



- A. Click on the default filter name with pre-defined filter queries and check box to enable as role.
- B. Specify a new filter with filter queries to fetch authentication and authorization attributes.
- C. Attribute Name under filter configuration must match one of the columns being requested from the database table.
- D. Create a new Endpoint context server and add the SQL server IP, credentilas and the database name.
- E. Alias Name under filter configuration must match one of the columns being requested from the database table.
- F. Create a new authentication source and add the SQL server IP, credentials and the database name.

## Correct Answer: BDF

## **QUESTION 3**

A customer would like to allow only the AD users with the "Manager" title from the "HQ" location to

Onboard their personal devices. Any other AD users should not be authorized to pass beyond the initial

device provisioning page.

Which Onboard service will you use to implement this requirement?

- A. Onboard CP login service
- B. Onboard Authorization service
- C. Onboard Provisioning service
- D. Onboard Pre-Auth service

Correct Answer: A

## **QUESTION 4**

Refer to the exhibit: A customer has configured a service with the Onboard Devices Repository as an Authentication Source and an Active Directory Domain Server as an Authorization Source. What will happen if the client certificate is still valid and the user account associated with the certificate is disabled in Active Directory?



	ces » Edit - My_organization_ On			1
Services - My_	_organization_ Onboa	rd Provisioning		
Summary Servic	e Authentication Authoriza	ntion Roles Enforcement		
Service:				
Name:	My_organization_ Onboard	d Provisioning		
Description:	802.1X wireless access s	ervice authenticating users prior to device pro	visioning with Onboard, and after device provisionin	g is complete
Type: Aruba 802.1X Wireless				
Status: Enabled				
Monitor Mode: Disabled				
More Options:	Authorization			
			Service Rule	
Match ALL of the follo	wing conditions:			
Туре		Name	Operator	Value
1. Radius:IETF		NAS-Port-Type	EQUALS	Wireless-802.11 (19) Login-User (1), Framed-User (2), Authenticate-Only
2. Radius:IETF		Service-Type	BELONGS_T0	(8)
3. Radius: Aruba		Aruba-Essid-Name	EQUALS	Home_SSID
Authentication:				
Authentication Metho	ods: [EAP TLS With OCSP Ena	bled]		
Authentication medic				the second s

Authentication Methods:	[EAP TLS With OCSP Enabled]
Authentication Sources:	[Onboard Devices Repository]
Strip Username Rules:	/:user
Service Certificate:	
Authorization:	
Authorization Details:	AD1
Roles:	
Role Mapping Policy:	
Enforcement:	
Use Cached Results:	Disabled
Enforcement Policy:	My_organization_ Onboard Provisioning Enforcement Policy
Back to Services	Disable Copy Save Cano

- A. ClearPass will not process the request
- B. Enforcement will apply the [Deny Access Profile]
- C. ClearPass will redirect the client to Onboard again
- D. ClearPass will block network access to the device
- E. ClearPass will allow the device to access the network.

Correct Answer: D

# **QUESTION 5**

Refer to the exhibit:



Summary Input (	Dutput Alerta				
Login Status:	ACCEPT				
Session Identifier:	R000001ae-01-5d9cb453				
Date and Time:	Oct 08, 2019 12:07:47 EDT				
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)				
Usemame:	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,EAP-MSCHAPv2				
Authentication Source:	AD:AD1.aruba1.local				
Authorization Source:	[Endpoints Repository], AD1, AD2, Corp SQL				
Roles:	VIP User, [Machine Authenticated], [User Authenticated]				
Enforcement Profiles:	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile				
Service Monitor Mode:	Disabled				
Online Status:	Not Available				

			* Edit - HS_Buildi					
	ummaiy	Service	Authentication	Authorization	Roles	Enforcement	Profiler	
Rol	e Mapping	Policys	HS_Building Role M	lapping Policy		Modify		Add New Role Mapping Policy
					Role	tapping Policy D	etails	THE REPORT OF LAND
Des	scription:		est per la manager,					
Def	fault Role:		[Other]					
Rul	es Evaluat	tion Algorith	im: first-applicabl	e				
	Conditi	ons					Role	
1	(Connet	tion: Client	Mac-Address	SHASLING UNASU	VIP Us	er MAC)	VIP User	
2.	(Authori	ization:Cor	SQLIMAC MILL	5 3			Corp SQL Tablet	
э.	(Authori	ization:[End	points Repository	Category BOOM	UT VOIP	Phone)	IP Phone	
41	(Author	zation:[End	points Repository	Category House	C. Smar	tDevice)	Personal SmartDevice	
5.	Authon	ization:[End	ipoints Repository	Category 201/	OS Point	of Sale devices)	Vending Machine	
6.			points Repository on:[Endpoints Rep		dor est	ANDRAS CANON	Printar	
7.	(Author	ization:[End (Authorizations AB	ipoints Repository, on:[Endpoints Rep )	[:Category ository]:MAC Ver		ork Camera) MLS Axis	IP Camera	



Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler	
Ise Cached	Results:	Vise cached R	oles and Posture a	ttributes	from previous se	essions	
Enforcement Policy : HS_Branch Onboard Provisioning Enforcement Policy *				cement Po	ley T Modify	Add New Enforcement Pol	
				Enfor	cement Policy De	etails	
Description:							
Default Profi	le:	[Deny Access	Profile]				
Rules Evalua	tion Algoriti	nm: first-applicabl	8				
Condit	ions		40.000			Enforcement Profiles	
1. (Auth	orization:[Er	ndpoints Repositor	y]:OS Family	江朝期的方	)	Aruba Limited Access for Profiling	
2. (Endp	oint:MDM E	habled SQUALS to	'Ue)			Aruba Full Access Profile	
3. (Authentication: DuterMethod Corp. SQL Tablet)						Redirect to Aruba Oceoard Portal	
4. (Auth	The second s	uterMethod equin	EAP-TLS)			Acuba Full Access Profile	
(Tips:Role Authenticated) [Machine Authenticated]) 5. (Authentication:Source AD1) (Tips:Posture Conduct HEALTHY (0))					Windows)	Aruba Full Access Profile	
(Authorization:[User Authenticated] [Machine Authenticated]) 6. (Authenticated]) 6. (Authentication:Source UNKNOWN (100)) (Tips:Posture UNKNOWN (100)) (Authorization:[Endpoints Repository]:OS Family Content Windows)					windows)	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_pag Profile	
(Tips: [Machin 7.	Role Authentic (Authentic (Tinc-Post	[User Av ated]) ation: Source	thenticated] HEALTHY (0))		Windows)	Redirect to Aruba Quarantine Profile	
	CAUTIONIZ3	DOUR ENDPOINTS NO	Property and the second s	And Colored Lines Incom		Aruba VIP Full Access Profile	

The customer created a new enforcement policy condition to allow VIP Users access without additional security compliance checks hut cannot gel it working. The customer has sent you the above screenshots. How would you resolve the issue?

A. Ask the VIP user to complete the one time web health check to get the VIP profile.

- B. Set the Enforcement Policy rules evaluation algorithm to evaluate all.
- C. Include VIP User role along with the Healthy posture enforcement condition.
- D. Modify the Enforcement Policy and re-order the VIP user condition to the lop.

Correct Answer: C

#### **QUESTION 6**

You have configured a Guest SSID with Captive-portal Web Authentication and MAC authentication The MAC caching expiry time set to 12 hours and the Guest Account expiration time is set to 8 hours. What will happen if the guest were to disconnect from the SSID and re-connect 9 hours later?

A. The client will tail the MAC authentication and be denied access to the Guest SSID.



- B. The client will successfully pass the mac authentication until the mac caching time expires.
- C. The client will successfully pass the MAC authentication but still be redirected to captive portal page.
- D. The client will fail the MAC authentication and will be redirected to the Captive-portal login page.

Correct Answer: C

## **QUESTION 7**

When is it recommended to use a certificate with multiple entries on the Subject Alternative Name?

- A. The ClearPass servers are placed in different OnGuard zones to allow the client agent to send SHV updates.
- B. Using the same certificate to Onboard clients and the Guest Captive Portal on a single ClearPass server.
- C. The primary authentication server Is not available to authenticate the users.
- D. The ClearPass server will be hosting captive portal pages for multiple FQDN entries

Correct Answer: A

## **QUESTION 8**

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 (168) Policies Used HS\_Building Aruba 802.1x service Service: EAP-PEAP, EAP-MSCHAPy2 Authentication Method: AD:AD1.aruba1.local Authentication Source: Authorization Source: AD1 [Other], [User Authenticated] Roles: [Deny Access Profile] Enforcement Profiles: Disabled Service Monitor Mode: Not Available Online Status: Show Logs Export Show Configuration M Showing 1 of 1-20 records > > **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



54	ammary Service	Authentication	Roles Enforcement	t Profiler	The second se
Ser	vice:			The Market Property in	
			ba 802.1x service		
Description: 802.1X wireless a is complete		access service authentio	ating users prior to device provisionin	g with Onboard, and after device provisionini	
Тур	e:	Aruba 802.1X W	ireless		
Stat	tus:	Enabled			
Man	itor Mode:	Disabled			
Mor	e Options:	Profile Endpoints	5		
				Service Role	
Mate	h ALL of the following	conditions:			
	Туре		Name	Operator	Value
1.	Radius:IETF		NAS-Port-Type	EQUALS	Wireless-802.11 (19)
1975	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
Aut	thentication:				
Aut	hentication Methods:		EAP TLS With OCSP Ena	bied]	
Aut	hentication Sources:	1. [Onboard De 2. AD1 3. AD2	vices Repository]		
Stri	p Username Rules:	liuser			
Ser	vice Certificate:	÷			
Rol	es:				
Rol	e Mapping Policy:	HS_Building Rol	le Mapping Policy		
Enf	orcement:				
Use	Cached Results:	Enabled			
Enf	orcement Policy:	HS_Building 802	2.1: Enforcement Policy		
Pro	filer:				
Enc	point Classification:	ANY			
	DIUS CoA Action:	[ArubaOS Wirel	ess - Terminate Session	1	
100,044	and the second se	and the first in the second state of the state of the second state			Disable Copy Save Gm



Configur	ation > Services	=> Edit - HS_Building An	iba 802.1x sarv	rice		
		ilding Aruba 802.				
Summa		Authentication Rol	The second second second second			
Role Map	ping Policy:		COntractory Constants			Add New Role Mapping Policy
		HS_Building Role Mapping	PORCY	Modify		Add New Kole Mapping Folicy
				Role Mapping Pe	olicy Details	
Descripti	ion:		ili Martin Califi	alet de president		
Default P	Role:	[Other]				
Rules Ev	aluation Algoriti	nm: first-applicable				
Cor	nditions				Rale	
1. (Co	onnection: Client	-Mac-Address (BELCMIS)	TO GROUP V	IP User MAC)	VIP User	
2. (Au	thorization:Con	P SQL:MAC EXTERN )			Corp SQL Tablet	
3. (Au	thorization:[End	dpoints Repository]:Cate	gory Equination	VoiP Phone)	IP Phone.	
4. (Au	thorization [End	points Repository]:Cate	gory BOLLALN	SmartDevice)	Personal SmartDevice	
5. (Au	thorization:[En	dpoints Repository]:Cate	gory EDMALL	Point of Sale de	evices) Vending Machine	
6. (Au 1NC.	(Authorizat	dpoints Repository]:Cate ion:[Endpoints Repositor	The second s	Printer) CAN	ON Printer	
7. (AL	thorization: End	fpoints Repository]:Cate ion:[Endpoints Repositor )		Network Came Acts	the second se	

	ces * Edit - HS_Building Aruba 802.1x service Building Aruba 802.1x service e Authentication Roles Enforcement Pr	ofiler		
Use Cached Results: Enforcement Policy:	Use cached Roles and Posture attributes from     HS_Building 602.1x Enforcement Policy     Enforcement	m previous sessions  Modify Add New Enforcement Policy ent Policy Details		
Description: Default Profile: Rules Evaluation Algo	[Deny Access Profile] rithm: first-applicable			
Conditions		Enforcement Profiles		
1. (Endpoint:MDM	Enabled FOMALS true)	Aruba Full Access Profile		
Z AND (Tips:R	OuterMethod EQUALS EAP-PEAP) ole EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal		
	nOuterMethod BOKALS EAP-TLS) ole BOKALS Corp SQL Tablet)	Aruba Full Access Profile		
4. (Tips:Role EQ	VIP User)	Aruba VIP Full Access Profile		
5. [Machine Author (Author	77/25.44. [User Authenticated] vicated]) vication:Source 2500400 AD1) osture 2500400 HEALTHY (0))	Aruba Full Access Profile		
6. [Machine Auther (Auther	TOMOS du [User Authenticated] nticated]) ntication:Source (TROL AD1) osture (Control UNKNOWN (180))	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile		
Machine Auther	ntication:Source ASMALS AD1)	Redirect to Arube Quarentine 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 9**

Refer to the exhibit:



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)
Jsername:	alex07
Access Device IP/Port:	10.1.70.198:0 (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

Summary	Input	Output	Alerts
inforcement P System Posture S Audit Posture S	e Status:	HEALTHY	to Aruba OnBoard Portal, Aruba Full Access Profile (0) (N (100)
RADIUS Resp	onse		0
RadiustAruba	::Aruba-I	Jser-Role	BYOD-Provision
Posture Eval	uation Re	sults	



And a state of the	Authentication Authorization	Roles	Enforcement	Profiler		
se Cached Results:	S Use cached Roles and Posture	attributes	from previous se	ssions		
nforcement Policy:	HS_Building 802.1x Enforcement Pole	W.	Modify		Add New Enforcement Polic	
		Enfor	cement Policy De	tails		
escription						
efault Profile:	[Deny Access Profile]					
ules Evaluation Algorith	m: evaluate-all					
Conditions		and the second		Enforcement Profiles		
L. (Endpoint:MDM En	abled stands true)			Aruba Full Access Profile		
2. (Tips:Role State	Corp SQL Tablet)			Aruba Full Access Profile		
1. (Tips:Role StatAL	VIP User)			Aruba VIP Full Access Profile		
A REAL PROPERTY AND A REAL	terMethod EQUALS EAP-TLS.)			Aruba Full Access Profile		
Tips:Role	uterMethod (DGGACS EAP-PEAP) (Egg/Add [User Authenticated])			Redirect to Aruba OnBoard Portal		
5. [Machine Authentics (Authentics (Tips:Post	ation: Source HEALTHY (0))			Aruba Full Access Profile		
(Tips:Role [Machine Authentic (Authentic (Tips:Post)	ation:Source Filling AD1) ation:Source Filling AD1) ure Filling UNKNOWN (100))	Redirect to Aruba Dissolvable_page	Profile			
(Tips:Role [Machine Authentio 8. (Authentio	[User Authenticated]			Redirect to Aruba Quarantine Profil	•	

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 10**

Under Onboard management and control, which option will deny the user from re-provisioning the device a second



#### time?

- A. Revoke and Delete certificate
- B. Delete user
- C. Revoke certificate
- D. Delete certificate
- Correct Answer: D

HPE6-A81 PDF Dumps

HPE6-A81 VCE Dumps

HPE6-A81 Practice Test