

HPE6-A77<sup>Q&As</sup>

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:

Request Details	
Summary Input	Output Alerts
Login Status:	REJECT
Session Identifier:	R00000218-01-5d9db68b
Date and Time:	Oct 09, 2819 06:29:34 EDT
End-Host Identifier:	78D29437BD68 (Computer / Windows / Windows 10)
Usemame:	andy07
Access Device IP/Port:	18.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (160)
	Policies Used -
Service:	HS_Building Aruba 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPy2
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
He Showing 1 of 1-20 r	records 11 Show Configuration Export Show Logs Close
Request Details	
Summary Input	Output Alerts
Error Code: 206	
Error Category: Autheni	tication failure
Error Message: Access	denied by policy
Alerts for this Reque	st
RADIUS Applied 'Rejec	ť profile



Con	figuration > Services	> Edit - HS_Build	ing Aruba	802.1x service				
Ser	rvices - HS_Bui	ilding Aruba	802.1>	service				
Su	mmary Service	Authentication	Roles	Enforcement	Profiler			
Ser	vice:							
Nam	ie:	HS_Building An						
Desi	cription:	is complete		ervice authenticatin	g users prior to device provisio	ning with Onboard, and after	device provisionii	
Туре	et in the second second	Aruba 802.1X V	reless					
Stat	us:	Enabled						
Man	itor Mode:	Disabled						
More	e Options:	Profile Endpoint	5					
				5	ervice Rale			
Matc	h ALL of the following	conditions:						
_	Туре		Name		Operator	Yalue		
1.	Radius:IETF		NAS-Port-	Туре	EQUALS	Wireless-802.1	L (19)	
NE	Radius:IETF		Service-T	ype	BELONGS_TO	Login-User (1), Authenticate-Or	Framed-User (2), nly (8)	
3.	Radius:Aruba		Aruba-Essid-Name		EQUALS	secure-HS-500	secure-HS-5007	
Aut	hentication:							
Auti	hentication Mathods:		EAP TLS	With OCSP Enabled	P C C C C C C C C C C C C C C C C C C C			
Aut	hentication Sources:	1. [Onboard De 2. AD1 3. AD2	vices Rep	ository]				
Stri	p Username Rules:	/:user						
Ser	vice Certificate:	-						
Role	es:							
Role	e Mapping Policy:	HS_Building Ro	le Mappin	g Policy				
Enf	orcement							
Use	Cached Results:	Enabled						
Enfo	preement Policy:	HS_Building 80	2.1× Enfo	rcement Policy				
Pro	filer:							
End	point Classification:	ANY						
RAE	DIUS CoA Action:	[ArubaOS Wire	less - Terr	minate Session]				
1000	Back to Services					Disable Copy	Save Gu	



Confi	iguration	> Services	> Edit - HS_Buildi	ng Aruba I	302.1x serv	vice					
Ser	vices -	HS_Bu	ilding Aruba	802.1x	service						
Sur	mmary	Service	Authentication	Roles	Enforcem	ent	Profiler				
Role	Mapping	Policy:	HS_Building Role M	Apping Polic	Y		Aodify			Add New I	Role Mapping Policy
						Role M.	opping Policy	Details			
Desc	ription:										
Defa	ult Role:		[Other]								
Rules	s Evaluat	ion Algorith	m: first-applicabl	8:							
	Conditio	ons						Role			
1.0	(Connec	tion:Client	Mac-Address (BE)	XINGS_70	GROOM N	IP Use	r MAC)	VIP User			
2.	(Authoria	zation:Con	SQLIMAC EXTEN	- )				Corp SQL Table	et		
31	(Authoria	ation:[End	points Repository	]:Category	E EQXXADO	VOIP P	hone)	IP Phone			
4.	(Authori	ation [End	ipoints Repository	]:Categor	ECLIPALS	Smart	Device)	Personal Smar	Device		
5.	(Authoria	zation:[End	ipoints Repository	]:Categor	E E E E E E E E E E E E E E E E E E E	Points	if Sale devic	es) Vending Machin	ie:		
6. T	(Authori Inc.)	zation:[End Authorizati	points Repository on:[Endpoints Rep	]:Categor lository]:M	AC Vendor	Printer	CANON	Printer			
7.	(Authori	zation:[End Authorizati cations AB	ipoints Repository on:[Endpoints Rep )	]:Categor ository]:M	104511042		rk Camera) Accs	IP Camera			

		s > Edit - HS_Building Aruba 802.1x servic	
Service Authentication Roles Enforcement Profiler         Summary Service Authentication Roles Enforcement Profiler         Use Cached Results:       * Use cached Roles and Posture attributes from previous sessions         Enforcement Policy:       # Use cached Roles and Posture attributes from previous sessions         Enforcement Policy:       # S. Building 802.1x Enforcement Policy       Modify         Description:       Enforcement Policy Postals         Default Profile:       [Deny Access Profile]         Rules Evoluation Algorithm:       first-applicable         Eonditions       Enforcement Profiles         1.       (Endpoint:MDM Enabled counds: EAP-PEAP)       Redirect to Arube OnBoard Portal         3.       (Authentication:OuterMethod Science EAP-PEAP)       Redirect to Arube OnBoard Portal         3.       (Authentication:OuterMethod Science EAP-PEAP)       Aruba Full Access Profile         4.       (Tips:Role cound: Corp SQL Tablet)       Aruba Full Access Profile			
Summary         Service         Authentication         Roles         Enforcement         Poniler           Use Cached Results:         * Use cached Roles and Posture attributes from previous sessions         Add New Enforcement Policy:           Enforcement Policy:         HS_Building 602.11x Enforcement Policy         * Modify         Add New Enforcement Policy:           Description:         Enforcement Policy:         Inforcement Policy:         * Modify         Add New Enforcement Policy:           Default Profile:         [Deny Access Profile]         Enforcement Profiles         Inforcement Profiles         Inforcement Profiles           Rules Evaluation Algorithm:         first-applicable         Enforcement Profiles         Inforcement Profiles           1.         (Endpoint:MDM Enabled Foundation: OuterMethod Strue)         Aruba Full Access Profile         Inforcement Profiles           2.         Modify         Aruba Full Access Profile         Inforcement Profiles         Inforcement Profiles           3.         (Authentication: OuterMethod Strue)         Aruba Full Access Profile         Inforcement Policy           3.         (Authentication: OuterMethod Strue)         Aruba Full Access Profile         Inforcement Policy           4.         (Tips:Role Strue)         Aruba Full Access Profile         Inforcement Policy         Inforcess Profile           4.<			
Enfor	Cached Results:  Use cached Roles and Posture attributes from p  rement Policy: HS_Building 802.1x Enforcement Policy  forforcement  reription: ault Profile: [Deny Access Profile] ss Evaluation Algorithm: first-applicable  Conditions  (Endpoint:MDM Enabled Sciences EAP-PEAP)  Authentication:OuterMethod Science EAP-PEAP)  (Authentication:OuterMethod Science EAP-PEAP)  (Dense Science EAP	Contraction of the second s	
		1000 March 1	orcement Policy Details
Desc	cription:		
- the property of		A REAL PROPERTY AND A REAL	
Rules	s Evaluation Algorith	nm: first-applicable	
	Conditions		Enforcement Profiles
1.	(Endpoint:MDM Er	nabled FGMALS true)	Aruba Full Access Profile
2.			Redirect to Aruba OnBoard Portal
3.			Aruba Full Access Profile
4.			Aruba VIP Full Access Profile
5.	[Machine Authentic	ated]) ation:Source English AD1)	Aruba Full Access Profile
6,	[Machine Authentic 440 (Authentic		Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7.	[Machine Authentic	sation(Source ASMALS AD1)	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 2**

#### Refer to the Exhibit:

Use Cached Results: Enforcement Policy:	Use cached Poles and Posture attributes from previous sessions	
Enforcement Policy:	Personal sector in the sector is a sector in the sector is a sector is a sector in the sector is a sec	
	T2-OnGuard-Policy T Modify	Add New Enforcement Policy
	Enforcement	Policy Details
Description:		
Default Profile:	(ArubaOS Wiveless - Terminate Session)	
Rules Evaluation Algorithm:	first-applicable	
Conditions		Enforcement Profiles
1. (Tips:Posture 200	HEALTHY (0))	T2-Emp-Healthy, [Aruba0S Winkers - Terminate Session], [Cisco - Terminate Session]
2. (Tips:Posture II)	ULE QUARANTINE (20))	T2-Emp-Universitity, [ArubaOS Wereless - Terminate Session], [Cisco - Terminate Session]
		Exhibit &77-01126930-347
	Posture Policies > Edit - T2-OnGuard-Posture-Policy	
Posture Policies -	T2-OnGuard-Posture-Policy	
	asture Plughas Roles	
Pules Evaluation Algorithm	First applicable	and the second sec
Conditions	and the second	Posture Token
17 Passes all SHV checks -	ClearPass Windows Universal System Health Validator     hecks - ClearPass Windows Universal System vealth Validator	PEACHT



Summary Service	Authentication Authorization Roles Enforcement		
Use Cached Results:	Use cached Roles and Posture attributes from previous session		
Enforcement Policy:	secure1-2x Aruba 802.1X Wireless Enforcement Policy .	Modify	Add New Enforcement Policy
	Enforc	ement Policy Details	
Description			
Default Profile:	(Deny Access Profile)		
Rules Evaluation Algorith	m: first-epplicable		
Conditions		Enforcement Profiles	
(Tips:Role Mills (Machine Authent 1. T2-SQL-Device) Mills (Tips:Rol	icated) ture HEALTHY (0))	T2-Enskoyee-Auth	
(Tips:Role T2-SQL-Owvice) 2. (Tips:Rol (Tips:Rol	Uter Authenticated]	T2-Engloyee-Auth	
3. (Tips:Role Con		52-Employee-Auth	
4. (Tips:Role Clips:Pole		12-Quarantina-Profile	
(Tips:Role	Ruger Authenticated[) hure [] (minicipated[)	52 - Unknows - Profile	
in the			

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

#### **QUESTION 3**

A customer is planning to implement machine and user authentication on infrastructure with one Aruba

Controller and a single ClearPass Server.

What should the customer consider while designing this solution? (Select three.)

A. The Windows User must log off, restart or disconnect their machine to initiate a machine authentication before the cache expires.

B. The machine authentication status is written in the Multi-master cache on the ClearPass Server for 24 hrs.

C. Onboard must be used to install the Certificates on the personal devices to do the user and machine authentication.

D. The Customer should enable Multi-Master Cache Survivability as the Aruba Controller will not cache the machine state.



E. Machine Authentication only uses EAP TLS, as such a PKI infrastructure should be in place for machine authentication.

F. The customer does not need to worry about Multi-Master Cache Survivability because the Controller will also cache the machine state.

Correct Answer: BCE

## **QUESTION 4**

Refer to the exhibit:



Configuration = Services =	Edit - Health-Check	
Services - Health	1-Check	
Summary Service	Roles Enforcement	
Use Cached Results:	I use cached Roles and Posture attributes from previous re	store
Enforcament Policy:	T-3-Onguard Modify	Add New Enforcement Policy
	En	arcament Policy Details
Description:		
Default Profile:	[ArubaOS Wireless - Terminate Session]	
Pules Evaluation Algorithm	m: first-applicable	
Conditions		Enforcement Profiles
1. (Tips:Posture	MINE HEALTHY (0))	T4-Healthy, (Aruba05 Wireless - Terminate Sassion)
2. (Tips:Posture	QUARANTINE (20))	T-4-Unhealthy, [AndraOS Wireless - Terminate Session]

elect	one/more plugins:			
	Plugin Name	Plugin Config	uration	Status
×	ClearPass Windows Universal System Health Validator	Configure	View	Configured
B	Windows System Health Validator	Canfigure	View	1 1 1 1 ×
	Windows Security Health Validator	Carofigurar	Miene	
	ration » Posture » Posture Policies » Edit - Windows ure Policies - Windows		Exh	1b1t A77-01126930-351
	ure Policies - Windows	Barris I.	Exh	1bit A77-01126930-351
Summ	ure Policies - Windows		Exh	1bit A77-01126930-351
Summ des E	ure Policies - Windows nary Policy Posture Plugins Rules		Exh	ibit A77-01126930-351 Posture Token
Summ Summ Ules E	ure Policies - Windows nary Policy Posture Plugins Rules valuation Algorithm: First applicable		Exh	



Summary Input O	utput
Login Status:	ACCEPT
Session Identifier:	W0000002e-81-5d5ce4f4
Date and Time:	Aug 21, 2019 08:30:13 CEST
End-Host Identifier:	7c5cf8cb1f0b
Username:	7cScf8cb1f0b
Access Device IP/Port:	
System Posture Status:	UNKNOWN (100)
	Policies Used -
Service:	Health-Check
Authentication Method:	Not applicable
Authentication Source:	
Authorization Source:	
Roles:	the second s
Enforcement Profiles:	[AnubaOS Wireless - Terminate Session]
Service Monitor Mode:	Desabled



What could be causing the error message received on the OnGuard client?

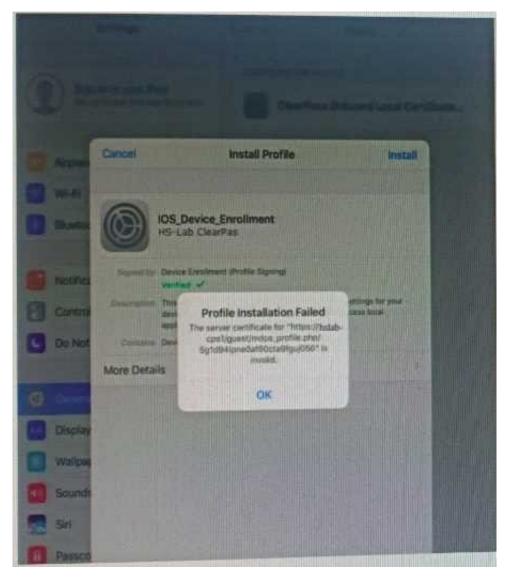
- A. The Service Selection Rules for the service are not configured correctly
- B. The Web-Based Health Check service needs to be configured to use the Posture Policy
- C. There is a firewall policy not allowing the OnGuard Agent to connect to ClearPass
- D. The client\\'s OnGuard Agent has not been configured with the correct Policy Manager Zone



Correct Answer: D

## **QUESTION 5**

Refer to the exhibit:



A customer has configured Onboard and Windows devices work as expected but cannot get the Apple iOS devices to Onboard successfully. Where would you look to troubleshoot the Issued (Select two)

A. Check if the ClearPass HTTPS server certificate installed in the server is issued by a trusted commercial certificate authority.

B. Check if the customer installed the internal PKI Root certificate presented by the ClearPass during the provisioning process.

C. Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client.

D. Check if the customer has Instated a custom HTTPS certificate for IDS and another internal PKI HTTPS certificate for



other devices.

E. Check if the customer has installed the same internal PKI signed RADIUS server certificate as the HTTPS server certificate.

Correct Answer: AC

#### **QUESTION 6**

Refer to the exhibit:

oruba		C	learPass Policy Manager	Henry
Dashboard 0	Config	uration = Toentity = Loca		
Honitoring 0	Loca	Users		📫 Add
Configuration		Edit Local User <ul> <li>Account Settings</li> <li>Export All</li> <li>Account Settings</li> <li>Stow (20 * records</li> <li>Stow (20 * records</li> <li>Status</li> <li>Enable User:</li> <li>Change Password:</li> <li>Change Password:</li></ul>		
Q Service Templates & Wizards				and the second se
- O Services	Clear	User ID:	Mon	
Authentication		Name:	Larry Fins	A CONTRACTOR OF A
A Methods	Filter	Password:		Show 20 Tecords
- Q Identity		Verify Password:		And the second se
Single Sign-On (SSO)	1.	Enable User:	(Check to enable user)	Statement Concerning of Landson Pro-
C Local Users	2.			And the second statement of the second statement of the
C Endpoints	Shaw	Collector State of the second state of the sec		Export Deters
C Static Host Lists		KÖre:	The first of the second s	
O Role Mappings		A DECEMBER OF PRESS		ENSEMPTION S
- B Posture		State of the second	Value	
Enforcement		CheR to add		
- Q Policies				
Q Profiles	10.04			A DESCRIPTION OF THE REAL OF T
Profile and Network Scan				
O Policy Simulation			Save Cancel	
	n an			
Administration 0				
© Copyright 2018 Hewlett Packard E	nterre	to Couplement 1.2	Aug 15, 2019 16:01:56 EDT ClearPass Policy Manager	6.7.9.109195 on C1000V platform
PERSONAL PROPERTY PACKATO E	SATING BEE		NAME OF TAXABLE PARTY AND ADDRESS OF TAXABLE PARTY.	

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 7**



Refer to the exhibit: You configured a new Wireless 802.1X service for a Cisco WLC broadcasting the Secure-ADM-5007 SSID. The client falls to connect to the SSID. Using the screenshots as a reference, how would you fix this issue? (Select two.)

Request Details		9
Summary 1	Input Output Alerts	
Error Code:	204	1
Error Category:	Authentication failure	
Error Message:	Failed to classify request to service	
Alerts for this	s Request	
RADIUS Servi	ce Categorization failed	

Su	ummary §	iervice.	Authentication	Authorization	Roles	Enforcement	Profiler	A CONTRACTOR OF A CONTRACTOR O	
Ser	vice:								
Nam	ne:		HS_Building Cisc	o 802.1x service					
Des	cription:		802.1X wireless a is complete	access service au	thenticat	ing users prior to	device provisioning	with Onboard, and after device provisi	IOFIIF
Туре	et		Aruba 802.1X Wi	reless					
Stat	tus:		Enabled						
Mon	itor Mode:		Disabled						
Mor	e Options:		1, Authorization 2. Profile Endpoin	nts					
						Service Rule			
Mate	ch ALL of the	following	conditions:						
	Туре		6	lame		Operat	ar	Value	
1.	Radius:IET	F	N	AS-Port-Type		EQUALS		Wireless-802.11 (19)	1H2 (*
2.	Radius:IET	Ŧ	s	ervice-Type		BELONG	S_TO	Login-User (1), Framed-User Authenticate-Only (8)	(2),
3.	Radius:IET	F	<	Called-Station-Id		EQUALS		secure-ADM-5007	
Aut	thentication	1:							
Aut	hentication M	1ethods:	1. [EAP PEAP] 2. HS_Branch_[E	AP TLS With OCS	P Enable	ed]			
Aut	hentication S	Sources:	1. [Onboard Dev 2. AD1 3. AD2	rices Repository]					

A. Update the service condition Radius:IETF Called-Station-Id CONTAINS secure-adm-5007

- B. Make sure that the Network Devices entry for the Cisco WLC has a vendor setting of "Airspace"
- C. Remove the service condition Radius:IETF Service-Type BELONGSJTO Login-User (1). 2. 8
- D. Change the service condition to Radius:IETF Calling-Station-Id EQUALS Secure-ADM-5007

Correct Answer: AC

# **QUESTION 8**



A customer has a ClearPass cluster deployment with four servers, two servers at the data center and two servers at a large remote site connected over an SD-WAN solution The customer would like to implement OnGuard, Guest Self-Registration, and 802.1x authentication across their entire environment. During testing the customer is complaining that users connecting to an Instant Cluster Employee SSID at the remote site, with the OnGuard Persistent Agent installed are randomly getting their health check missed. What could be a possible cause of this behavior?

A. The OnGuard Clients are automatically mapped to the Policy Manager Zone based on their IP range but an ACL on the switch could be blocking access.

B. The traffic on the TCP port 6658 is congested due to the fact that this port is also used by the IPsec keep-alive packets of the SD-WAN solution.

C. The ClearPass Policy Manager zones have been defined but the local IP sub-nets have not been property mapped to the zones and the OnGuard Agent might connect to any of the servers in the cluster.

D. The Aruba-user-role received by the IAP is filtering the TCP port 6658 to the ClearPass servers and after 10 seconds the SSL fallback gets activated and randomly generates the issue.

Correct Answer: D

#### **QUESTION 9**

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 ate 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 the same authority used for signing me final TLS certificate of the device.

B. Configure the identity certificate signer as Active Directory Certificate Services and enter the ADCS URL http://ADCSVVeoEnrollmentServemostname/certsrv in the OnBoard Provisioning settings.

C. Enable access to EST servers from the Certificate Authority to make ClearPass Onboard to use of 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 to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

Correct Answer: C

## **QUESTION 10**

Where is the following information stored in ClearPass?

1.

Roles and Posture for Connected Clients

2.

System Health for OnGuard



3.

# Machine authentication State

4.

CoA session info

5.

Mapping of connected clients to NAS/NAD

- A. Multi-Master cache
- B. Endpoint database
- C. insight database
- D. ClearPass system cache

Correct Answer: D

HPE6-A77 Practice Test

HPE6-A77 Study Guide

HPE6-A77 Braindumps