

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.certbus.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

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 2

Refer to the exhibit:

Summary Request	Policies				
	Policies Used -				
Service Name:	[Aruba Device Access Service]				
Authentication Source:	[Local User Repository]				
Role:	[User Authenticated], [Aruba TACACS read-only Admin]				
Profiles:	[ArubaOS Wireless - TACACS Read-Only Access]				



Deshboard	General Admin AkWave C	PSec Certificates SHAP Logging Profiles	
WLANE	Admin Authentication Options		
Roles & Policies	Default mie:	Trace w	
Access Points	Entite	R	
AP Groups	MSDHAVZ:	a	
Authentication	Server group:	Geor@uss Tacacs	
Services	Management tablet access	0	
tranfaces	Login activities persidence period:	C dags	
(Symam Tasks	Login Lanver text:		
Dorgnosticz	Server has to be accepted.	CI	
Mantenance	MEBUR AUTHENTICATION Utermann-Quebenorth		
	Wardson HYTTPS yourt (4443) accesss:		
	Cient certificate:		
	Server contriticate:	ortan *	
	tale session timenze.	15 montes 4	
	Re-suffernosisin trimous		

Server Scaup > ClearPas	in Tacaca Serve	rs Options Serv	uer Rubes		Drag room to re ord
Spinster.	7195	IP ADDRESS	TRuss Piljons	NATCH HULES	
Constraint D. S.	THERE	144 8 M 100			
+					
Server Group > ClearPe	na Taxana > Cient?en	a T Server Options	Server Group Trim	QON Server Croup N	datch Bules
Plant	10.1.120	ANT .			
Rep:					
Key: Retype keyt	-				
	and the second second	Concession and the second second			
Retype key: TCP port:	0	Concession and the second second			
Hatype Lega TCP parts Retransmitti	0	Concession and the second second			
Retype key: TCP port:	er 3				



# 10.1.120.100 - PuTTY			- 0	×
				î
		Seaturn Timt		
rinin rico Fead-only root				

A customer has configured the Aruba Controller for administrative authentication using ClearPass as a TACACS server. During testing, the read-only user is getting the root access role. What could be a possible reason for this behavior? (Select two.)

A. The Controllers Admin Authentication Options Default role is mapped to toot.

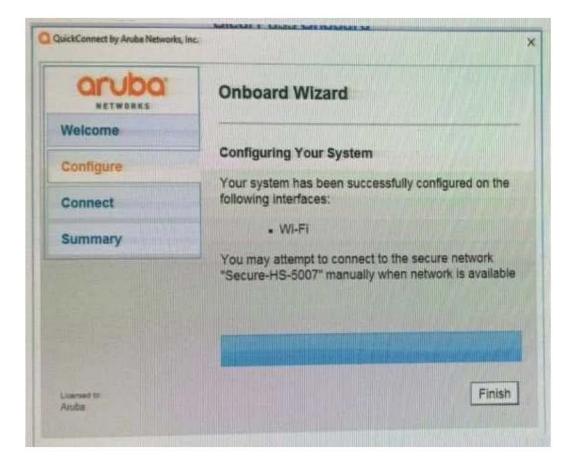
- B. The ClearPass user role associated to the read-only user is wrong
- C. The Controller Server Group Match Rules are changing the user role
- D. The read-only enforcement profile is mapped to the root role
- E. On the Controller, the TACAC\$ authentication server Is not configured for Session authorization

Correct Answer: CE

QUESTION 3

Refer to the exhibit:





Servic	es - HS_Bra	nch Onboard Provisi	oning			
Summi		Authentication Authoriza	Constitution and and and an inclusion of the owner of the owner of the			
Service:						
Name:		HS_Branch Onboard Provisi	oning			
Description: 802.1X wireless access service authenticating users prior		ice authenticating users prior to	device provisioning with Onboard, and after dev	vice provisioning is complete		
Type: Aruba 802.1X Wireless						
Status: Enabled		Enabled				
Monitor M	Aode:	Disabled				
More Opt	tions:	Authorization				
				Service Rule		
Match AL	L of the following	conditions:				
T	(pe		Name	Operator	Value	
1. Ra	edius:IETF		NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
2. R.	adiustIETF		Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	
3. R.	idius:Aruba		Aruba-Essid-Name	EQUALS	secure-HS+S007	
Authent	ication:					
Authenti	cation Methods	1. HS_Branch_[EAP TLS W 2. [EAP PEAP]	th OCSP Enabled]			
Authenti	cation Sources:	1. [Onboard Devices Report 2. ADI 3. AD2	itory]			
Strip Use	ername Rules:	J:USEF				
Service	Certificate:					
Authori	zation:					
Authoriz	ation Details:	1. A01 2. AD2				
Roles:						
Role Ma	pping Palicy:	2				
Enforce	ment:					
Use Cad	hed Results:	Disabled				
	nent Policy:		ioning Enforcement Policy			



There are arrows with the case	ver certificate configuration that will prevent device	Fride support and the support of the		
50-t07-cp1: The ClearPas	s HTTPS server root certificate is not trusted by Ap s HTTPS server root certificate is not trusted by Ap	ple. This will cause enrollment over HTTPS to	a fail on IOS devices. a fail on IOS devices.	
How do I fix this probler	nž			
this list to manage certif		Status Expiry		OCSP URL
HS_Branch		Valid: 2029-09-25T03-19147-0410	0 http://p50	-t07-cp1/guest/mdps_ocsp.php/2
Local Certificate Author	ty root 🖌	Valid 2029-06-25T21-25:44-04:0	0 http://p50	t07-cp1/guest/mdps_ocsp.php/1
This is the default cartificat	e authority.			
Refresh				
N	ame Mode	Status Expiry		OCSP URL
HS_Branch		Valid 2029-09-25703:19:47-04:0		t07-cp1/guest/mdps_ocsp.php/2
Hide Details 3 Edit .	Duplicate 🐂 Show Usage 💾 Trust Chain	Cartificator B Renew D Delete	Client Certificates	
	Contribute Authority Settings		Contraction of the local division of the loc	
	H5_Branch			
Description	Root CA			
Certificate Issuing				
	Specify an OCSP Responder URL			
OCSP URL:	http://p50-t07-cp1/guest/mdps_ocsp.php/2			
Validity Period:	and the second se			
Clock Skey Allovances	The second			
ubject Alternative Name:	Enabled			
tworks	uration = Network Settings server cartificate configuration that will prevent ass HTTPS server root cartificate is not trouted ass HTTPS server root cartificate is not trouted	But Sentis This will calle appallment supp	SETTERS TO TAIL ON TOTS DEVICES.	
atworks There are errors with the p30+07-op2: The Clear p50+07-op1: The Clear	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted ass HTTPS server root certificate is not trusted	But Sentis This will calle appallment supp	SETTERS TO TAIL ON TOTS DEVICES.	
atworks There are arrors with the p30-t07-cp2: The Clear p50-t07-cp1: The Clear How do I fix this prob	erver certificate configuration that will prevent ass HTTDS server root certificate is not trusted ass HTTDS server root certificate is not trusted em?	But Sentis This will calle appallment supp	SETTERS TO TAIL ON TOTS DEVICES.	
atworks There are arrors with the p30-t07-cp2: The Clear p50-t07-cp1: The Clear How do I fix this prob	erver certificate configuration that will prevent ass HTTDS server root certificate is not trusted ass HTTDS server root certificate is not trusted em?	But Sentis This will calle appallment supp	SETTERS TO TAIL ON TOTS DEVICES.	
There are errors with the p50+07-cp2: The Clear p50+07-cp1: The Clear How do I fix this prob e this list to manage re-	erver cartificate configuration that will prevent ass HTTDS server root cartificate is not trusted ass HTTDS server root cartificate is not trusted em? tworks. Name	i by Appla. This will cause enrollment over I by Appla. This will cause enrollment over	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices.	Example-TAS
There are errors with the p30-t07-cp2t The Clear p50-t07-cp1t The Clear between the first this prob e this list to manage ner Example Network Connectto the example	erver cartificate configuration that will prevent ass HTTDS server root cartificate is not trusted ass HTTDS server root cartificate is not trusted em? tworks. Name	i by Appla. This will cause enrollment over I by Appla. This will cause enrollment over	HTTPS to tall on IOS devices. HTTPS to fail on IOS devices. Network: Type	Example-TLS Secure-HS-5007
There are errors with the p30-r07-cp21 The Clear p50-r07-cp11 The Clear How do I fix this prob e this list to manage no Example Network Connect to the example Secure :H5-5007	erver certificate configuration that will prevent ass HTTDS server root certificate is not trusted ass HTTDS arver root certificate is not trusted em? works Name	by Apple. This will cause enrollment sour I by Apple. This will cause enrollment sour T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
There are errors with the p30-r07-cp21 The Clear p50-r07-cp11 The Clear How do I fix this prob e this list to manage no Example Network Connect to the example Secure :H5-5007	anver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted ess HTTPS anver root certificate is not trusted em? works Name hervork	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
Atworks There are errors with the p30-t07-cp2: The Clear p30-t07-cp1: The Clear How do I fix this prob e this list to manage no Example Network Connect to the example Secure H5-5007 Hide Details C Edit	erver certificate configuration that will prevent ass HTTDS server root certificate is not trusted ass HTTDS arver root certificate is not trusted em? works Name	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
Atworks There are errors with the pS0+07-cp21 The Clear pS0+07-cp11 The Clear How do I fix this prob a this list to manage nor Example Network Connect to the example Secure H5-5007 Hide Details 2 Edit Network Access	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted ess HTTPS arver root certificate is not trusted em? works Name network Duplicate Show Litings	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
Atworks There are errors with the pS0+07-cp21 The Clear pS0+07-cp11 The Clear How do I fix this prob a this list to manage nor Example Network Connect to the example Secure H5-5007 Hide Details 2 Edit Network Access	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted ess HTTPS arver root certificate is not trusted em? works Duplicate Show Litings Notwork Settings	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
etworks There are errors with the pS0+07-op21 The Clear pS0+07-op11 The Clear How do I fix this prob this list to manage ne Example Network Connect to the example Secure H5:5007 Hide Details get Edit Network Access Name Description	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted ess HTTPS arver root certificate is not trusted em? works Duplicate Show Litings Notwork Settings	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
etworks There are errors with the pS0+07-op21 The Clear pS0+07-op11 The Clear How do I fix this prob this list to manage ne Example Network Connectto the example Secure H5-5007 Hide Details Fidt Network Access Name Description Network Type	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted ess HTTPS server root certificate is not trusted em? works Name network Duplicate Show Litings Network Settings	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
Atworks There are errors with the p50+07-op21 The Clear p50+07-op21 The Clear How do I fix this prob a this list to manage ne Example Network Connect to the example Secure H5-5007 Hide Details Edit Network Access Name Description Network Type	erver certificate configuration that will prevent ass HTTPS server root certificate is not trusted ess HTTPS server root certificate is not trusted em? works Name network Dupleate Show Litings Network Settings Secure-HS-5007 H H Wireless only Enterprise (802:1X)	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
Atworks There are errors with the p50+07-op21 The Clear p50+07-op21 The Clear How do I fix this prob a <i>this list to manage ne</i> Example Network Connect to the example Secure H5-5007 Hide Details fight Network Access Name Description Network Type Security Type Wireless Network Setti Security Version	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted ess HTTPS server root certificate is not trusted em? works Name network Dupleate Show Usage Notwork Settings Secure-HS-5007 Secure-HS-5007 Herterprise (802:1X) ISSN 100000000000000000000000000000000000	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
etworks There are errors with the pS0+07-op21 The Clear pS0+07-op21 The Clear How do I fix this prob e this list to manage no Example Network Connectto the example Secure H5-5007 Hide Details Edit Network Access Name Description Network Type Security Type Wireless Network Setti Security Version SSII	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted eem? works Name network Dupleate Show Usage Notwork Settings Secure-HS-5007 Wireless only Enterprise (802:1X) 95 14 Wireless (recommended) 15 Secure-HS-5007	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
etworks There are errors with the pS0+07-op21 The Clear pS0+07-op21 The Clear How do I fix this prob obse fist to manage rea Example Network Connectto the example Secure H5-5007 Hide Details Fidt Network Access Name Description Network Setti Security Version Security Version	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted eem? works Name network Dupleate Show Usage Network Settings Secure-HS-5007 Wireless only Enterprise (802:1x) 9 9 10 11 12 13 14 14 15 15 15 15 15 15 15 15 15 15	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
etworks There are errors with the pS0+07-op21 The Clear pS0+07-op21 The Clear How do I fix this prob e this list to manage ne Example Network Connectto the example Secure H5-5007 Hide Details Edit Network Access Name Description Network Settis Security Version Security Version Securi	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted eem? works Name network Dupleate Show Usage Notwork Settings Secure-HS-5007 Wireless only Enterprise (802:1X) 95 14 Wireless (recommended) 15 Secure-HS-5007	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
Atworks There are errors with the p30+07-op2: The Clear p30+07-op2: The Clear How do I fix this prob e this list to manage no Example Network Connect to the simple Secure H5-5007 Hide Details Edit Network Access Name Description Network Setti Security Version Security Version	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted eem? works Name network pupileais Show Urage Network Settings Secure-HS-5007 Wineless.only Enterprise (802.1%) Secure-HS-5007 Wineless.only Enterprise (802.1%) Secure-HS-5007 Wineless.only Enterprise (802.1%) Secure-HS-5007 Wineless.only Enterprise (802.1%)	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
etworks There are errors with the p30-c07-cp2: The Clear p30-c07-cp2: The Clear p30-c07-cp1: The Clear How do I fix this prob e this list to manage no Example Network Connect to the example Secure H5-5007 Hide Details field Network Access Name Description Network Access Name Description Network Settis Security Version SSII Security Version SSII Wireless Auto Joi Enterprise Protocols (OS & macOS EA	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted eem? works Name network pupileais Show Urage Network Settings Secure-HS-5007 Wineless.only Enterprise (802.1%) Secure-HS-5007 Wineless.only Enterprise (802.1%) Secure-HS-5007 Wineless.only Enterprise (802.1%) Secure-HS-5007 Wineless.only Enterprise (802.1%)	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
etworks There are errors with the p30-c07-cp2: The Clear p30-c07-cp2: The Clear p30-c07-cp1: The Clear How do I fix this prob e this list to manage no Example Network Connect to the example Secure H5-5007 Hide Details field Network Access Name Description Network Access Name Description Network Settis Security Version SSII Security Version SSII Wireless Auto Joi Enterprise Protocols (OS & macOS EA	erver certificate configuration that vill prevent ass HTTPS Server root certificate is not trusted eem? works Name network pupileais Show Usings Notwork Settings Secure-HS-5007 Wineless.only Enterprise (802.1%) Secure-HS-5007 Wineless.only Enterprise (802.1%) Secure-HS-5007 Visible network Enabled Yisible network Enabled	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	
etworks There are errors with the p30-c07-cp2: The Clear p30-c07-cp2: The Clear How do I fix this prob e this list to manage no Example Network Connect to the example Secure H5-5007 Hide Details field Network Access Name Description Network Access Name Description Network Settis Security Version SSII Security Version SSII Wireless Auto Joi Enterprise Protocols (OS & macOS EA Legacy OS X EA	erver certificate configuration that will prevent ass HTTPS Server root certificate is not trusted eem? works Name Name Notwork Settings Secure-HS-5007 Wireless.only Enterprise (802.1%) Wireless.only Secure-HS-5007 Wireless.only Enterprise (802.1%) Secure-HS-5007 Wireless.only Enterprise (802.1%) Secure-HS-5007 Wisble network Enabled FLS PEAP with MSCHAPy2 TLS	by Apple. This will cause enrollment over I by Apple. This will cause enrollment over T	HTTPS to tail on IOS devices. HTTPS to fail on IOS devices. Network Type Wireless	



aruba	ClearPass Onboard	
Guest	Home = Onboard = Deployment and Provisioning = Provisioning Settings	
Onboard	G Provisioning Settings	
Start Here Certificate Authorities Management and Control Start Here View by Device View by Username View by Certificate	There are enors with the server certificate configuration that will prevent devices from provisioning or p50-t07-cp1: The ChairPass HTTPS server root certificate is not trusted by Apple. This will cause a p50-t07-cp2: The ChairPass HTTPS server root certificate is not trusted by Apple. This will cause a How do I fix this problem? Use this list to manage provisioning settings.	nrollment over HTTPS to fill on iOS devices.
🦛 Usage	Name	
Configuration	HS_Branch	HS_Branch
Start Here	Hide Detail: Fdit Duplicate 2 Delets Launch Device Provisioning Settings	
ios Settings	Name: HS Branch	
Windows Applications	Description	The second s
Deployment and Provisioning	Organization: Aruba	
Start Here Configuration Profiles	Identity	
Provisioning Settings	Cestificate Authority: HS_Branch	
	Signeri Onboard Certificate Authority	
- Self-Service Portal	TLS Certificate Authority: HS_Branch	
	Key Type: 2048-bit RSA - created by device	and a state of the second
	Unique Device Credentials: Enabled	
	Authorization	
	Authorization Method: App Authentication - check using Aruba Application Authe	ntication
	Use SSO1 Disabled	and the second second
	Configuration Profile: secure-HS-5007	the second s
	Maximum Devices: 0	
	Actions	The second s
	Certificate Expiny: Disabled	
Eonfiguration	Revoke Inactive: Disabled	
Administration	O Delete Duplicates: Disabled	

You have configured an Onboard portal for single SSID provision. During testing you notice that the QuickConnect Application did not display the "Connect" button, only the finish button. To get connected the test user had to manually connect to the secure-HS-5007 SSID but was prompted for a username and password. Using the screenshots as a reference, how would you fix this issue?

- A. Check the network settings for the correct SSID name spelling.
- B. Change the network settings to use EAP-TLS for the authentication protocol.
- C. Install a public signed HTTPs web server certificate on the ClearPass server.
- D. Configure the SSID to support both EAP-PEAP and EAP-TLS authentication method.

Correct Answer: A

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

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 Wirelessi - Terminate Session]
Status Code	0
Status Message	Radius [ArubaOS Wireless - Terminate Session] failed for client 78d29437bd69
RADIUS CoA Attributes	Calling-Station-Id = 78D29437BD69



	No response from network device
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:	10.1.70.100:6 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (180)
	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

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 6

You have recently implemented a serf-registration portal in ClearPass Guest to be used on a Guest SSID broadcast from an Aruba controller. Your customer has started complaining that the users are not able to reliably access the internet after clicking the login button on the receipt page. They tell you that the users will click the login button multiple times and alter about a minute they gain access. What could be causing this issue?

A. The self-registration page is configured with a 1 minute login delay.

- B. The guest client is delayed getting an IP address from the DHCP server.
- C. The guest users are assigned a firewall user role that has a rate limit.
- D. The enforcement profile on ClearPass is set up with an IETF:session delay.



Correct Answer: A

QUESTION 7

Refer to the exhibit: You are doing a ClearPass PoC at a customer site with a single Aruba Mobility Controller. The customer asked for a demonstration of a simple Web Login functionality. You used a service template to create the guest services. During testing, the user gets redirected back to the weblogin page with an Authentication failed message. The guest configurations on the Aruba Mobility Controller are configured correctly. Why would the guest fail to authenticate successfully?

		* Edit - HPE-Arubi Aruba Wired				
Summ	nary Service	Authentication	Authorization Roles	Enforcement	Profiler	
Use Ca	ched Results:	Use cached R	toles and Posture attributes	from previous s	Issions	
Enforce	ement Policy:	HPE-ArubaOS N	lac auth policy		Modify	Add New Enforcement Policy
			En	forcement Policy	Details	
Descrip	ition:					
Default	Profile:	[Deny Access	Profile]		The second s	
Rules E	Valuation Algorith	m: first-applicable				
C	onditions				Enforcement Profiles	
1.	(Authorization:[E	ndpoints Repositor]:Category NOT_EUSTS	0	Assign Switch role PROFILE	
2.		ndpoints Repositor ition: [Endpoints Re	y]:Category EQUALS Acce pository]:OS Family EQUA	ss Points) Aruba)	Assign Aruba switch role AP-ACCESS	

General Wireless Network Settings MA	C Caching Settings	Posture Settings	Access Restrictions
 Enforcement Type applies to the Ca Captive Portal Access is used for un At least one of Employee, Guest, and 	authenticated user	's and after the M	ss, Guest Access, and Contractor Access fields. AC caching duration has expired. ed.
Enforcement Type::	Aruba Role Enforcer	nent v	
BALLING BALLING AND	quesths-login		
Lapuve Portal Access	Gaeans-indu		
		iesday 🗑 Wednes	day 🖉 Thursday 🖉 Friday 🖉 Saturday 📽 Sunday
Days allowed for access	🕷 Monday 🕷 Tu	iesday 🕅 Wednes	day 🖉 Thursday 🖉 Friday 🖉 Saturday 📽 Sunday
Days allowed for access <mark>e</mark> : Maximum number of devices allowed per use	🕷 Monday 🕷 Tu		day 📽 Thursday 📽 Friday 🕷 Saturday 🕷 Sunday
Days allowed for access": Maximum number of devices allowed per user Maximum bandwidth allowed per user":	🕷 Monday 🕷 Tu		
Captive Portal Access*: Days allowed for access*: Maximum number of devices allowed per user Maximum bandwidth allowed per user*: Employee Access: Guest Access:	🕷 Monday 🕷 Tu		



Configuration » Services »	Edit - Guest User Authentication with MAC Cacl	aing	
Services - Guest I	User Authentication with MAC C	aching	
Summary Service	Authentication Authorization Roles En	forcement	
Use Cached Results:	Use cached Roles and Posture attributes fro	om previous sessions	
Enforcement Policy:	Guest User Authentication with MAC Caching Enfor	cement Policy T Modify	Add New Enforcement Policy
	Enf	orcement Policy Details	
Description:			
Default Profile:	[Allow Access Profile]		
Rules Evaluation Algorithm	first-applicable		
Conditions		Enforcement Profiles	
1. (Authorization:[End	Ipaints Repository]:Unique-Device-Count (19654)	ER THEW 0) [Deny Access Profile]	
(Tips:Role Conce 2. Alto (Date:Day-o Monday,Tuesday,Wee	[Guest]) of-Week SELOVOS TO dnesday, Thursday, Finday, Saturday, Sunday)	Limit, Guest MAC Caching !	n Timeout, Guest MAC Caching Bandwidth Session Limit, Guest Guest MAC Caching, Guest MAC Caching Do Expire, Guest MAC Guest Guest Profile

A. The authentication source mapped in the service is incorrect, it should be mapped as (Guest Device Repository] [Local SQL DB].

B. The username and/or password used for authentication is incorrect Re-enter the correct password on the weblogin page.

C. The username used for authentication does not exist in the Guest User Database Create a new user and authenticate again.

D. The Unique-Device-Count does not allow any Client devices. Update the Enforcement policy condition: Unique-Device-Count.

Correct Answer: A

QUESTION 8

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

QUESTION 9

What is the Open SSID (otherwise referred to as Dual SSID) Onboard deployment service workflow?

A. OnBoard Pre-Auth Application service, OnBoard Authorization Application service. OnBoard Provisioning RADIUS service

B. OnBoard Pre-Auth RADIUS service. OnBoard Authorization Application service. OnBoard Provisioning RADIUS service

C. OnBoard Authorization Application service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

D. OnBoard Authorization RADIUS service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

Correct Answer: C

QUESTION 10

Refer to the exhibit:



aruba		C	learPass Policy Manager	*****
Dashboard 0 Honitoring 0		aration + Identity + Loca Il Users	Add	
So Configuration	Chear Filter 1. 2. Shaw	Edit Local User		A Import Export All
C Service Templates & Wizards Services Authentication C Methods Sources C Sources C Identity C Single Sign-On (SSO) C Identity C Identity C Single Sign-On (SSO) C Identity C		User ID:	ifm	Show 20 • records Status Enabled only Admin] Enabled
		Name:	Lany Fins	
		Password:		
		Verify Password:		
		Enable User:	Check to enable user)	
		Change Password:	(Check to force change password on next TACACS+ login)	Export Delete
		Role:	Super Admin *	Contraction of the local division of the loc
			Attributes	
		Attribute	Value	
		Li Click to add		
Q Profiles	Side a			
Network Profile and Network Scan	FILL!			Ser Standard Bank
© Policy Simulation	NA D		and a fighter and the second state of the seco	tal I
			and the second	CONTRACT OF A
Administration 0				
Copyright 2018 Hawlett Packard	Enter	the Country and LD	Aug 15, 2019 16:01:50 EDT ClearPass Policy Mana	eger 6.7.9.109195 on C1000V platfor

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

Latest HPE6-A77 Dumps

HPE6-A77 Practice Test

HPE6-A77 Study Guide