

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.geekcert.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 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 2

Refer to the exhibit:



Summary Input (Output Alerts	
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)	
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,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 Lumited 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 OWNER OF THE OWNER
Des	scription:							
Def	fault Role:		[Other]					
Rul	es Evaluat	tion Algorith	im: first-applicabl	6				
	Conditi	ons					Role	
1	(Connet	tion: Client	Mac-Address	ONASU NO LONGO	VIP Us	er MAC)	VIP User	
2.	(Authorization:Corp SQL:MAC (1777))					Corp SQL Tablet		
э.	(Authorization:[Endpoints Repository]:Category (Routing VolP Phone)					IP Phone		
41							Personal SmartDevice	
5.	Authon	ization:[End	ipoints Repository	Category 601/	os: Point	of Sale devices)	Vending Machine	
61			points Repository on:[Endpoints Rep		dor est	er) LS CANON	Printar	
7.	(Author	ization:[End (Authorizations AB	ipoints Repository, on:[Endpoints Rep)	(:Category ository]:MAC Ver		ork Camera) MLS Axis	IP Camera	



https://www.geekcert.com/hpe6-a77.html 2024 Latest geekcert HPE6-A77 PDF and VCE dumps Download

Jun	mary	Service	Authentication	Authorization	Roles E	nforcement	Profiler		
	achied R		Vise cached Ro	oles and Posture	attributes from	m previous se	essions		
Enford	ement	Policy:	HS_Branch Onboa	rd Provisioning Entor	coment Policy	• Modify	Add New Enforcement Policy		
					Enforcen	nent Policy De	stails		
Descr	iption:								
	It Profile		[Deny Access						
lules	Evaluat	ion Algoriti	nm: first-applicabl	•					
1	Conditi	ons		All Phillip and			Enforcement Profiles		
İ.	(Autherization:[Endpoints Repository]:OS Family M07_ENDF3)				T_800575)		Aruba Limited Access for Profiling		
2.	2. (Endpoint:MDM Enabled #Caractic true)						Aruba Full Access Profile		
3. (Authentication: OuterMethod Corp SQL Tablet)							Redirect to Aruba OrBoard Portal		
4.	(Authe		uterMethod Corp St	EAP-TLS) (L Tablet)			Aruba Full Access Profile		
5.		e Authentic (Authentic (Tips:Post		THY (0))	ally Loward	Windows)	Aruba Full Access Profile		
(Tips:Role [User Authenticated]) [Machine Authenticated]) 6. (Authentication:Source ACI1) (Tips:Pocture UNKNOW(N (100))					windows)	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_pag Profile			
7-	(Tips:Role [Liser Authenticated] [Mechine Authenticated]) (Authentication:Source AU1) (Tips:Porture HEAUTHY (0))					Windows)	Redirect to Aruba Quarantine Profile		
			VIP User)	And a state of the state	and the second se		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 3

Refer to the exhibit:



ALANA	a :	Onboard W	izard		
Welcome					
Configure		Securely Conn Authentication in			
Connect	Qui	ckConnect	Constant of the second second	×	
Summary		Could not authenticate	with wareless network.	Contraction of the second	
			OK	1	



Request Details Seary. Input **Output** Alerts Login Status: REFET Sezzion Identifieri R0000002-01-5d0b2731 Date and Time: Sep 25, 2019 04:37:06 EDT End-Host Identifier: 780294992613 (Computer / Windows / Windows 10) Usemamer mike07 Access Device IP/Parts 10.1.70.100:0 (ArubaController / Aruba) System Posture Status: UNKNOWN (100) Palities Used Services HS_Branch Onboard Provisioning Authentication Method: EAP-TLE Authentication Sources AD(AD1. arubat. local Authorization Sources AD1. AD2 Roless Enforcement Profiles: [Allow Access Profile], HS_Branch Onboard Post-Provisioning Service Monitor Moden Disabled Configuration Export is a Showing 1 of 1-7 reports - M Request Details Summary Input Output Alerts 215 Error Code: Authentication failure Error Category: TLS session error Error Message: Alerts for this Request RADSUS Certificate Status unknown, Reason (UlakNOWN) EAD-TLE: fatal alert by zerver - internal_error TLE Handshahe failed in SSL read with emprid science iss. routinesissi3_get_client_certificate/sertificate verify failed exp-this Error in establishing TLS session



Ser	vices - HS_Bra	nch Onboard Pro	wisioning		
	and the second second second		sization Roles Enforcement		
Servi	cei				
Name: HS_Branch Onboard Provis		Provisioning			
Deso	iption	802.1X wireless acces	s service authenticating users prior to devic	e provisioning with Onboard, and after device	provisioning is complete
Туре		Aruba 802.1X Wireles			
Statu	#1:	Enabled			
Manif	tor Mode:	Dirabled			
More	Options	Authorization			
				Service Bale	
March	ALL of the followin	a conditioner		PRIVACE PRIVACE	
- Children	Туре		Name	Operator	Value
1	RadiustIETF		NAS-Port-Type	EQUALS	Wireless-892.11 (19)
1	RadiustIETF		Service-Type	BELONISS_TO	Login-User (1), Framed-User (2), Authentica Only (8)
31	Radius:Aruba		Aruba-Essid-Name	EQUALS	recure:HS-5007
Auth	entication:				
Auth	entication Methods	1. [EAP TLS WITH OC 2. [EAP PEAP]	SP Enabled]		
Auth	entication Sourcest	1. [Onboard Devices 2. AD1 3. AD2	Repository]		
Strip	Lisemame Rules	/iuser			
Sary	ce Certificate:	-			
Auth	orization:				
Auth	onzation Details:	1. AD1 2. AD2			
Role	92				
	Manning Policy				

	22.2				and the second se
ertificate Authoriti	es				🔅 Create ne
pourcurreptions clearpas	iver certificate configuration th is HTTPS server root certificat is HTTPS server rout certificat	til not trutted	the Annia, This w	izioning or authenticating: Ill cause enrollment over HTTPS to fail on iO Ill cause enrollment over HTTPS to fail on iO	5 devices. S devices.
How do I fix this problem	m2				
- now do t nx ans proble	MT				
e this list to manage certil	ficate authorities.				
	ame	Mode	Status	Expiry	OESP UHL
H5_Branch		root	🖌 Valid	2029-09-25703:19:47-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/
Local Certificate Aution This is the default certifica		reat	🖌 Valid	2029-06-25T21:25:44-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/
C' Refresh				1	
	Vame	Mode	Status	Expiry	OCSP URL
KS_Beanch	The life of the local division of the	root	🖌 Valid	2029-09-25703:19:47-04:00	http://p50+t07-cp1/guest/mdps_ocsp.php/
O Hide Details Fidit	Duplicate . Show Use	ga 🛃 Thust d	Sain 🔄 Cer	tificates 🍐 Renew 🐊 Delete Client Ce	utificates
	Certificate Authority Sett				
	Ceruncate Automity set	and the second se			
	HS_Branch				
Namer Descriptions				I. C. Station and T	
Namer Descriptions	H5_Branch				
Namer Description: Mode: Certificate Issuing Authority Info Access	HS_Branch Root CA Specify an OCSP Respond	erURL			
Namer Description: Mode: Certificate Issuing Authority Info Access	H5_Branch	er URL mdp3_9csp.ph	p/2		
Namer Description: Mode: Certificate Issuing Authority Info Access	H5_Branch Root CA Specify an OCSP Respond http://p50-t07-cp1/guest/	er LIRL mdps_ocip.ph	9/2		
Namer Description: Mode: Certificate Issuing Authonity Info Access OCEP URL:	HS_Branch Root CA Specify an OCSP Respond http://p50-t07-cp1/guest/ 265	er LIRL mdps_ocsp.ox	s/2		



aruba	ClearPass Onboa	rd					
Guest	Home > Onboard > Deployment and Provisioning > Provisioning Sattings Dravic Loning Cothings	Home > Onboard > Deployment and Provisioning > Provisioning Settings Provisioning Settings					
Start Here Certificate Authorities Management and Control Start Here View by Device View by Username View by Certificate	There are errors with the server certificate configuration that will prevent devices from provision p30-t07-cp1: The ClearPass HTTPS server root certificate is not trusted by Apple. This will p50-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will be the PS0-t07-cp2: The PS0-t07-cp2 server root certificate is not trusted by Apple. This will be the PS0-t07-cp2 server root certificate is not trusted by Apple. This will be the PS0-t07-cp2 server root certificate is not trusted by Apple. This will be the PS0-t07-cp2 server root certificate is not trusted by Apple. This will be the PS0-t07-cp2 server root certificate is not trusted by Apple. This will be the PS0-t07-cp2 server root certificate is not trusted by Apple. This will be the PS0-t07-cp2 server root certificate is not trusted by Apple. This will be the PS0-t07-cp2 server root certificate is not trusted by Apple. This will be the PS0-t07-cp2 serv	cause enrollment over HTTPS to fail on 108 devices. cause enrollment over HTTPS to fail on 108 devices.					
Usaga	Name	CA.					
Configuration	& HS_Branch	HS_Branch					
T Network Settings	🚺 Hide Details 📑 Edit 🗳 Duplicate 🔞 Delete 🛸 Launch	CONTRACTOR OF THE OWNER O					
iOS Settings	Device Provisioning Settings						
Windows Applications	Name: H9_Branch						
Deployment and Provisioning	Description:						
- Start Here	Organization: Aruba						
- Configuration Profiles	Identity						
Provisioning Settings	Certificate Authority: HS_Brendt Signer: Onboard Certificate Authority						
Self-Service Portal	TLS Certificate Authority: HS_Branch	and the second					
	Key Type: 2048-bit RSA - created by device						
	Unique Device Credentials: Enabled						
	Authorization Authorization Methods: App Authentication – check using Aruba Application	authentication					
	Use SSO: Disabled						
	Configuration Profile: secure-H5-5007	and the second s					
	Maximum Devices: 0						
	Actions	and the second s					
	Certificate Expiry: Disabled						
Configuration	Revoke Inactive: Disabled						
Administration	O Delete Duplicates: Disabled						

You have configured Onboard and cannot get it working The customer has sent you the above

screenshots.

How would you resolve the issue?

- A. Re-provision the client by running the QuickConnect application as Administrator
- B. Install a public signed server authentication certificate on the ClearPass server for EAP
- C. Reconnect the client and select the correct certificate when prompted
- D. Copy the [EAP-TLS with OSCP Enabled] authentication method and set the correct OCSP URL

Correct Answer: A

QUESTION 4

A Customer has these requirements:

*

2.000 IoT endpoints that use MAC authentication

*



6,000 endpoints using a mix of username/password and certificate (Corporate/BYOD) based authentication

1,000 guest endpoints at peak usage that use guest self-registration

*

1500 BYOD devices estimated as 3 devices per User (500 users)

*

2,500 endpoints that have OnGuard installed and connect on a daily basis

What licenses should be installed to meet customer requirements?

A. 11,500 Access, 500 Onboard, 2,500 Onguard

B. 13.000 Access, 1.500 Onboard, 2,500 Onguard

C. 11,500 Access, 1,500 Onboard, 2.500 Onguard

D. 9,000 Access, 500 Onboard. 2.500 Onguard

Correct Answer: C

QUESTION 5

There is an Aruba Controller configured to send Guest AAA requests to ClearPass. If the customer would like the most effective way to ensure the lowest license usage counts, how should the controller be configured?

A. Aruba Controller will send stop messages only if EAP termination and Interim accounting are enabled.

B. Aruba Controller will send stop messages if RADIUS Accounting Server Group is defined in the authentication profile.

C. Aruba Controller will send stop messages only if both accounting and interim accounting are enabled.

D. Configure EAP Termination on the Aruba Controller and the client will send a stop message.

Correct Answer: D

HPE6-A77 PDF Dumps

HPE6-A77 Exam Questions

HPE6-A77 Braindumps