

HPE6-A81^{Q&As}

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.pass2lead.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 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.)

Summary	Input	Output	Alerts		
Error Code:	204				
Error Categor	y: Authe	entication fa	silure		
Error Message	et Failed	to classify	request to service		
Alerts for t	his Requ	iest			
RADIUS Ser	vice Cat	econization	failed		

Su	ımmary	Service	Authentication	Authorization	Roles	Enforcement	Profiler	
sen	vice:	rinital.						
Nam	ne:		HS_Building Cisc	o 802.1x service				
Des	cription:		802.1X wireless - is complete	access service au	thenticati	ng users prior to	device provisioning	with Onboard, and after device provisioni
Туре	et		Aruba 802.1X Wi	reless				
Stat	us:		Enabled					
Mon	itor Mode:		Disabled					
Mori	e Options:		1, Authorization 2. Profile Endpoin	ıts				
						Service Rule		
Mato	Section and the second	following	conditions			علاياته والإستاعية ألا		
	Туре		15	ame	-	Operat	ar	Value
1.	RadiustIET	IF	N	AS-Port-Type		EQUALS		Wireless-802.11 (19)
2.	Radius:IET	71	S	ervice-Type		BELONG	ss_to	Login-User (1), Framed-User (2) Authenticate-Only (8)
3.	Radius: IET	TF	(alled-Station-Id		EQUALS		secure-ADM-5087
Aut	hentication	n:						
Auti	hentication I	Methods:	1. [EAP PEAP] 2. HS_Branch_[E	AP TLS With OCS	P Enable	d]		
Aut	hentication :	Sources:	1. [Onboard Dev 2. AD1 3. AD2	ices 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 2

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 3

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 4

Refer to the exhibit:



Summary Input	Output Aierts
Login Status:	ACCEPT
Session Identifier:	R00800238-01-5d9dd0b2
Date and Time:	Oct 09, 2019 08:21:07 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows 10)
Username:	alex07
Access Device IP/Port	: 10.1.70.198:0 (ArubaController / Aruba)
System Posture Statu	E 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:	
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 System Posti Audit Posture	ure Status:		
RADIUS Res	ponse	I Per concercione	
Radius:Arul	ba:Aruba-L	Iser-Role	BYOD-Provision
Posture Eva	aluation Re	sults	



AND COMPANY OF THE OWNER OF THE OWNER	Authentication	Authorization	Roles	Enforcement	Profiler	
Jse Cached Results:	B Use cached Rol	ies and Posture a	attributes	from previous se	Issions	
Inforcement Policy:	HS_Building 802.1x	Enforcement Policy		Modify		Add New Enforcement Polic
			Enfor	cement Policy De	tails	
Description:						
Default Profile:	[Deny Access	Profile]				
Rules Evaluation Algorithm	n: evaluate-all					
Conditions			and the second		Enforcement Profiles	
1. (Endpoint:MDM End	bled stands tru	(6)			Aruba Full Access Profile	
2. (Tips:Role Equation	Corp SQL Table	t) on the second se			Aruba Full Access Profile	
3. (Tips:Role EQUALS	VIP User)				Aruba VIP Full Access Profile	
4. (Authentication:Ou					Aruba Full Access Profile	
5. (Authentication:Ou die (Tips:Role	ECRIMAN [User Au	thenticated])			Redirect to Aruba OnBoard Portal	
(Tips:Postu	ted]) tion:Source re HEAC	AD1) THY (0))			Aruba Full Access Profile	
(Tips:Role [Machine Authentica 7. (Authentica (Tips:Postu	ted)) tion Source	AD1) HOWN (100))			Redirect to Aruba Dissolvable_pag	e Profile
(Tips:Role [Machine Authentica 8. (Authentica	ted])	AD1) HEAUTHY (0))			Redirect to Aruba Quarantine Prof	le

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 5

Which statements are true about Aruba downloadable user roles? (Select three.)



- A. Can be applied only on ports or WLAN users authenticated by ClearPass.
- B. Aruba downloadable user role are universally available across the environment
- C. Aruba downloadable user role is a built in enforcement template in ClearPass
- D. Downloadable role names must be defined in Aruba switch or controller
- E. Can use these roles for other authentication methods not involving ClearPass
- F. Administering downloadable user roles can be difficult for a large enterprise

Correct Answer: ADE

QUESTION 6

Refer to the exhibit:

rror Cod	e:	215
irror Cat	egory:	Authentication failure
irror Mes		TLS session error
Alerts f	or this Req	uest
	unknown ca	
	unknown ca	
	unknown ca	

A customer has configured onboard in a cluster with two nodes All devices were onboarded in the network through node1 but those clients tail to authenticate through node2 with the error shown. What steps would you suggest to make provisioning and authentication work across the entire cluster? (Select three.)

- A. Have all of the BYOD clients re-run the Onboard process
- B. Configure the Onboard Root CA to trust the Policy Manager EAP certificate root.



- C. Have all of the BYOD clients disconnect and reconnect to me network
- D. Make sure that the EAP certificates on both nodes are issued by one common root Certificate Authority (CA).
- E. Make sure that the HTTPS certificate on both nodes is issued as a Code Signing certificate
- F. Configure the Network Settings in Onboard to trust the Policy Manager EAP certificate

Correct Answer: BDF

QUESTION 7

How does the RadSec improve the RADIUS message exchange? (Select two.)

A. It can be used on an unsecured network or the Internet.

- B. It builds a TTLS tunnel between the NAD and ClearPass.
- C. Only the NAD needs to trust the ClearPass Certificate.
- D. It encrypts the entire RADIUS message.
- E. It uses UDP to exchange the radius packets.

Correct Answer: DE

QUESTION 8

You have integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment

to sign the final device TLS certificates. The customer would also like to use ADCS for centralized

management of TLS certificates including expiration, revocation, and deletion through ADCS.

What steps will you follow to complete the requirement?

A. Remove the EAP-TLS authentication method and add "EAP-TLS with OCSP Enabled\\' authentication method in the OnBoard Provisioning service. No other configuration changes are required.

B. Copy the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL, remove EAP-TLS and map the custom created method to the Onboard Provisioning Service.

C. Copy the default [EAP-TLS with OSCP Enabled] authentication method and update the correct ADCS server OCSP URL. remove EAP-TLS and map the custom created method to the OnBoard Authorization Service.

D. Edit the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL. remove EAP-TLS and map the [EAP-TLS with OSCP Enabled) method to the Onboard Provisioning Service.

Correct Answer: A

QUESTION 9



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 10

A customer has a ClearPass cluster deployment with one Publisher and one Subscriber configured as a Standby Publisher at the Headquarters DataCenter They also have a large remote site that is connected with an Aruba SD Branch solution over a two Mbps Internet connection. The Remote Site has two ClearPass servers acting as Subscribers. The solution implemented for the customer includes OnGuard, Guest Self Registration, and Employee 802. ix authentication. The client is complaining that users connecting to an IAP Clusters Guest SSID located at the Remote Site are experiencing a significant delay in accessing the Guest Captive Portal page. What could be a possible cause of this behavior?

A. The configuration of the captive portal is pointing to a link located on one of the servers in the Headquarters

B. The ClearPass Cluster has no zones defined and the guest captive portal request is being redirected to the Publisher

C. The guest page is not optimized to work with the client browser and a proper theme should be applied

D. The captive portal page was only created on the Publisher and requests are getting redirected to a Subscriber

Correct Answer: A

HPE6-A81 PDF Dumps

HPE6-A81 VCE Dumps HPE6-A81 Exam Questions