



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.passapply.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 corporate ClearPass Cluster with two servers located at a single site, has both Management and Data port IP addresses configured. The Management port IPs are in the DataCenter networks subnet, while the Data port IPs are in the DMZ. What is the difference between using one Virtual IP for the AAA traffic versus sending AAA requests to the physical IPs for each server? (Select two.)

A. The failover can be accomplished only by using Virtual IP.

- B. The Individual IPs can provide failover and load balancing.
- C. One Virtual IP can be used together with the individual server IPs for load balancing.
- D. By using the Virtual IP, the failover convergence is faster than using individual server IPs.

E. Using the one Virtual IP can provide failover and load balancing.

Correct Answer: BE

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

Refer to the exhibit:



Configuration = Services :	= Edit - Health-Check			
Services - Health	h-Check			
Summary Service	Roles Enforcement			
Use Cached Results:	Use cached Roles and Po	store attributes from previous reasions		
Enforcement Policy:	T-3-Onguard	Madily	Add New Enforcem	nt Policy
		Enforcement	Policy Details	
Description:				
Default Profile:	(ArubaOS Wireless - Termin	ate Session)		
Pules Evaluation Algorithm	m: first-applicable			
Conditions			Enforcement Profiles	
1. (Tips:Posture	HIM HEALTHY (0))		T4-Healthy, [ArubaOS Wireless - Terminate Session]	
2. (Tips:Posture	QUARANTINE (20))		T-4-Unhealthy, (AnuliaOS-Wreless - Terminate Session)	

elect	one/wore plugins:			
	Plugin Name	Plugin Config	uration	Status
×	ClearPass Windows Universal System Health Validator	Configure	View	Configured
B	Windows System Health Validator	Cauligure	View	
	Windows Security Health Validator	Cardigson	Miene	
	ration » Posture » Posture Policies » Edit - Windows ure Policies - Windows		Exh	1b11 A77-01126930-351
	ure Policies - Windows		Exh	1bit A77-01126930-351
osta	ure Policies - Windows		Exh	1bit A77-01126930-351
Summ Summ	ure Policies - Windows nary Policy Posture Plugins Rules		Exh	ibit A77-01126930-351 Posture Token
Summ Summ Ules E	ure Policies - Windows nary Policy Pasture Plugins Rules valuation Algorithm: First applicable		Exh	



Summary Input O	utput
Login Status:	ACCEPT
Session Identifier:	W0000002e-01-5d5ce4f4
Date and Time:	Aug 21, 2019 08:30:13 CEST
End-Host Identifier:	7c5cf8cb1fbb
Usemame:	7cScf8cb1f0b
Access Device IP/Port:	
System Posture Status:	UNKNOWN (100)
	Policies Used -
Service:	Health-Check
Authentication Method:	Not applicable
Authentication Source:	
Authorization Source:	
Roles:	
Enforcement Profiles:	[ArubaOS Wireless - Terminate Session]
Service Monitor Mode:	Disabled



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 4

Refer to the exhibit:

	Customize Self-Registration	
Login Options controlling loggin	g in for self-registered guests.	
Enabled:	Enable guest login to a Network Access Server ~	
* Vender Settings:	Aruba Networks	
Login Method:	Controller-initiated — Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's NAC address to be available, usually from the captive portal redirection process.	
* IP Address:	securelogin.erubanetworks.com Enter the IP address or hostname of the vendor's product here.	
Secure Login:	Secure login using HTTPS V Select a security option to apply to the web login process.	
Dynamic Address:	The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original res The address above will be used whenever the parameter is not available or fails the requirements below.	firection
Security Hash:	Do not check - login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the uses for example their MAC address.	
Default Destination Options for controlling th	e destination clients will redirect to after login.	
* Default URL:	Enter the default URL to redirect clients. Please ensure you prepend 'http://" for any external domain.	
Override Destination:	Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.	
	Save Changes 📫 Save and Continue	

A customer with multiple Aruba Controllers has just installed a new certificate for "*.customerdomain com" on all Aruba Controllers. While testing the existing guest Self-Registration page the customer noticed that the logins are failing. While troubleshooting they are finding no entries in the Event Viewer or Access Tracker for the tests. Suspecting that the Aruba Controllers may not be properly posting the credentials from the guest browser, they open the NAS Vendor Settings for the Guest Self-Registration Page. From the screen shown, how can you fix the errors?

A. Change the "IP Address: field to" securelogin.customerdomain.com.

B. Change the "Secure Login:" field to "Use Vendor Default".

- C. Change the "IP Address field to "captiveportal-login.customerdomain.com".
- D. Add PTR records on the DNS server for "securelogin.arubanetworks.com".

Correct Answer: B



QUESTION 5

Refer to the exhibit:



Summary Input	Output Alerts
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:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	HEALTHY (0)
	Policies Used -
Services	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

lequest Details		
Summary Input	Output	Alierta
Enforcement Profiles: System Posture Status: Audit Posture Status:		
RADIUS Response		0
Radius:Aruba:Aruba-U	Jser-Role	BYOD-Provision
Posture Evaluation Re	sults	
* * Showing 1 of 1-20		Change Status Show Configuration Export Show Logs Close



ACADOMICS CONTRACTOR	Authentication Authorization	Roles	Enforcement	Profiler	
se Cached Results:	B Use cached Roles and Posture	attributes	from previous se	ssions	
nforcement Policy:	HS_Building 802.1x Enforcement Policy	<u>1</u>	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	and the second second	Enforcement Profiles	
. (Endpoint:MDM En	abled Studies true)			Aruba Full Access Profile	
(Tips:Role Stude	Corp SQL Tablet)			Aruba Full Access Profile	
. (Tips:Role BRUAL	VIP User)			Aruba VIP Full Access Profile	
Wester Designation of the local line in the	terMethod EQUALS EAP-TLS.)			Aruba Full Access Profile	
Tips:Role	sterMethod (SOCIALS EAP-PEAP) (September [User Authenticated])			Redirect to Aruba OnBoard Portal	
Machine Authentica (Authentica (Tips:Posta	stion: Source HEALTHY (0))			Aruba Full Access Profile	
(Tips:Role [Machine Authentics (Authentics (Tips:Post)	et mai [User Authenticated] sted]) ston:Source Follow AD1) are condition (INKNOWN (100))			Redirect to Aruba Dissolvable_pag	e Profile
(Tips:Role	[]_ML [User Authenticated]			Redirect to Aruba Quarantine Profi	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

HPE6-A77 PDF Dumps	HPE6-A77 VCE Dumps	HPE6-A77 Braindumps