Money Back Guarantee

Vendor:HP

Exam Code: HPE6-A77

Exam Name: Aruba Certified ClearPass Expert Written

Version:Demo

QUESTION 1

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

QUESTION 2

Refer to the exhibit: A customer has configured Onboard in a cluster. After the Primary server\\'s failure, the BYOD devices fail to connect to the network. What would you do to troubleshoot?

Error Cod	e:	215
Error Cate	egory:	Authentication failure
Error Mes	sage:	TLS session error
Alerts fo	or this Req	quest
	hostname I	fatal alert by server - internal_error hake failed in SSL_read with error:2006A066:BIO routines:BIO_get_host_ip:bad lookup ror in establishing TLS session
	hostname I	hake failed in SSL_read with error:2006A066;BIO routines:BIO_get_host_ip:bad lookup
	hostname I	hake failed in SSL_read with error:2006A066;BIO routines:BIO_get_host_ip:bad lookup
	hostname I	hake failed in SSL_read with error:2006A066;BIO routines:BIO_get_host_ip:bad lookup
	hostname I	hake failed in SSL_read with error:2006A066:BIO routines:BIO_get_host_ip:bad lookup
	hostname I	hake failed in SSL_read with error:2006A066:BIO routines:BIO_get_host_ip:bad lookup

A. Verify the OSCP URL under TLS authentication method is mapped to http://localhost/ guestmdps_ocsp.php/2

B. Reboot the active ClearPass server and reconnect the client to the SSID by selecting the correct certificate when

prompted

C. Check EAP certificate on the secondary node is issued by the same common root Certificate Authority (CA)

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

Correct Answer: B

QUESTION 3

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?



Configuration > Service Templates & Wizards Service Templates - Guest Authentication with MAC Caching General Wireless Network Settings NAC Caching Settings Posture Settings Access Restrictions Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields. Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired. At least one of Employee, Guest, and Contractor Access must be provided. Enforcement Type": Aruba Role Enforcement . Captive Portal Access*: guesths-login Days allowed for access*1 🕷 Monday 🕷 Tuesday 🕷 Wednesday 📽 Thursday 🕷 Friday 🕷 Saturday Sunday. Maximum number of devices allowed per user*: n Maximum bandwidth allowed per user*: n MB (For unlimited bandwidth, set value to 0) Employee Access: Guest Access: Lab-Guest Contractor Access: Add Service Delete Hoat -> < Back to Service Templates & Wizards

Configuration » Services »	Edit - Guest User Authentication with MAC Caching	
Services - Guest	User Authentication with MAC Caching	
Summary Service	Authentication Authorization Roles Enforcement	
Use Cached Results:	Use cached Roles and Posture attributes from previous ses	sions
Enforcement Policy:	Guest User Authentication with MAC Caching Enforcement Policy •	Modify Add New Enforcement Policy
	Enforcement Policy	Details
Description:		
Default Profile:	[Allow Access Profile]	
Rules Evaluation Algorithm	first-applicable	
Conditions		Enforcement Profiles
1. (Authorization: [End	paints Repository]:Unique-Device-Count (CREATER, THEW 0)	[Deny Access Profile]
2. AND (Date: Day-	[Guest]) of-Week <mark>SSLOWER (O</mark> dnesday, Thursday, Friday, Saturday, Sunday)	Guest MAC Caching Session Timeout, Guest MAC Caching Bandwidth Limit, Guest MAC Caching Session Limit, Guest Guest MAC Caching, [Update Endpoint Known], Guest MAC Caching Do Expire, Guest MAC Caching Expire Post Login, 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 4

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 5

Refer to the exhibit:

Monitoring > Live Monitoring > Access Tracker

Access Tracker Aug 21, 2019 20:03:29 CEST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

er	Source	Cont	ains 🖸 Webauth	Go Cis	ar Filter	
	Server	Source	Username	Service	Login Statu	Request Timestamp
212	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:18:03
22	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:15:06
23.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:12:11
24.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:09:14
25.	10.254.5.2	WEBAUTH	7c5cf8cb5246	TZ-HeathCheck-Service	ACCEPT	2019/08/21 10:06:19
26.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:03:23
27.	10.254.5.2	WEBAUTH	7c5cf6cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:00:28
28.	10.254.5.2	WEBAUTH	7cScf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:57:31
29.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:54:36
30.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:51:41
31.	10.254.5.2	WEBAUTH	7cScf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:48:44
32	10.254.5.2	WEBAUTH	7c5cf8cb5246	72-HeathCheck-Service	ACCEPT	2019/08/21 09:45:49
33.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:42:54
34.	10.254.5.2	WEBAUTH	7cScf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:39:56
35.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:37:00
36.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:34:05
37.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:31:10
38.	10.254.5.2	WEBAUTH	7cScf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:28:15
39.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:25:19
40.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:22:23

A customer has just configured a Posture Policy and the T2-Healthcheck Service. Next they installed the OnGuard Agent on Secure_Employee SSID. When they check Access Tracker they see many WEBAUTH requests are being triggered.

- What could be the reason?
- A. OnGuard Web-Based Health Check interval has been wrongly configured to three minutes.
- B. The OnGuard Agent trigger the events based on changing the Health Status
- C. TCP port 6658 is not allowed between the client and the ClearPass server
- D. The OnGuard Agent is connecting to the Data Port interface on ClearPass

QUESTION 6

Refer to the exhibit:

Request Details	
Summary Input	Output Alerts
Login Status:	REJECT
Session Identifier:	R00000218-01-5d9db68b
Date and Time:	Oct 09, 2019 06:29:34 EDT
End-Host Identifier:	78D29437BD68 (Computer / Windows / Windows 10)
Usemame:	andy07
Access Device IP/Port:	18.1.78.108:0 (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
A Showing 1 of 1-20 r	ecords Show Configuration Export Show Logs Close
Request Details	
Summary Input	Output: Alerts
Error Code: 206	
Error Category: Authent	tication failure
Error Message: Access	denied by policy
Alerts for this Reque	st
RADIUS Applied 'Rejec	ť profile

Services - HS_Bui	rung Aruba	502.1X	Service		
Summary Service	Authentication	Roles	Enforcement	Profiler	
Service:					
Name:	HS_Building Arub				and the second se
Description:	602.1X wireless is complete	access se	rvice authenticat	ing users prior to device provisi	oning with Onboard, and after device provisionin
Туре:	Aruba 802.1X Wi	reless			
Status:	Enabled				
Monitor Mode:	Disabled				
More Options:	Profile Endpoints				
				Service Rale	
Match ALL of the following	conditions:				
Туре	N	ame		Operator	Yalue
1. Radius:IETF	N	AS-Port-	Туре	EQUALS	Wireless-802.11 (19)
2. Radius:IETF	s	ervice-T)	(pe	BELONGS_TO	Login-User (1), Framed-User (2) Authenticate-Only (8)
3. Radius:Aruba		ruba-Ess	id-Name	EQUALS	secure-HS-5007
Authentication:					
Authentication Mathods:	1. [EAP PEAP] 2. HS_Branch_[E	AP TLS)	Vith OCSP Enable	ed]	
Authentication Sources:	1. [Onboard Dev 2. AD1 3. AD2	ices Rep	ository]		
Strip Username Rules:	liuser				
Service Certificate:	-				
Roles:					
Role Mapping Policy:	HS_Building Role	e Mapping	2 Policy		
Enforcement:					
Use Cached Results:	Enabled				
Enforcement Policy:	HS_Building 802	1: Enfor	cement Policy		
Profiler:					
Profiler: Endpoint Classification:	ANY				
	ANY [ArubaOS Wirele	ess - Terr	ninate Session]		

			» Edit - HS_Buildi Iding Aruba					
Si	unumary Ser	vice	Authentication	Roles	Enforcement	Profiler		
Role	e Mapping Polic	:y:	HS_Building Role N	Aapping Polic	7 •	Modify		Add New Role Mapping Policy
				Contraction of the	Role	Mapping Policy D	etals	
Des	scription:							
Def	fault Role:		[Other]					
Rul	es Evaluation A	Igorithr	n: first-applicabl	8:				
	Conditions	0					Rale	
1.0	(Connection:	Client-I	lac-Address <i>(BEI</i>	XINGS_70	GROOM VIP I	Iser MAC)	VIP User	
2.	(Authorizatio)	n:Corp	SQLIMAC EXTEN	-)			Corp SQL Tablet	
310	(Authorization	n:[End;	oints Repository]:Category	E EQUARE VOI	P Phone)	IP Phone.	
4.	(Authorizatio	n [End;	oints Repository]:Category	EQUALS Sm	artDevice)	Personal SmartDevice	
5.	(Authorization	n:[End;	points Repository]:Categor	ERMANN POI	nt of Sale devices)	Vending Machine	
6.	(Authorization doil: (Authority) INC.)	n:[Endp orizatio	n:[Endpoints Repository]:Category ository]:M	Prir AC Vendor	ter) CANON	Printer	
7.	(Authorizatio	ionizatio	points Repository n:[Endpoints Rep]:Categor ository]:M		work Camera)	IP Camera	

Configuration > Se	rvices = Edit - HS_Building Aruba 802.1x service	
Services - HS	Building Aruba 802.1x service	
Summary Ser		Profiler
Lise Cached Result	s: Kuse cached Roles and Posture attributer	s from previous sessions Add. New Enforcement Policy
Enforcement Policy	HS_Building 602.1x Enforcement Policy	Modefy Modefy
	Enfos	rcement Policy Details
Description:		
Default Profile:	[Deny Access Profile]	
Rules Evaluation A	Igorithm: first-applicable	
Conditions		Enforcement Profiles
1. (Endpoint:M	DM Enabled ECHALS true)	Aruba Full Access Profile
A PMO (Tips	ion:OuterMethod EQUALS EAP-PEAP) :Role Equals Corp SQL Tablet)	Redirect to Arube OnBoard Portal
	ion:OuterMethod POWNER EAP-TLS) ::Role Powner Corp SQL Tablet)	Aruba Full Access Profile
4. (Tips:Role	EQUALS VIP User)	Aruba VIP Full Access Profile
5. [Machine Aut	henticated]) henticated]) hentication:Source (AD1) s:Posture (D))	Aruba Full Access Profile
6. [Machine Aut AND (Aut	hentication:Source Status AD1) s:Posture Source UNKNOWN (180))	Aruba Limited Access Profile, Redirect to Aruba Discolvable_page Profile
7. [Machine Aut	High Res Acc [User Authenticated] henticated]) hentication:Source (19745 ADI) s:Posture (1977 English HEALTHY (0))	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 7

While configuring a guest solution, the customer is requesting that guest user receive access for four hours from their first login. Which Guest Account Expiration would you select?

A. expire_after

B. do_expire

C. expire_time

D. expire_ postlogin

Correct Answer: A

QUESTION 8

Refer to the exhibit:

Summary Service At	thentication Roles Enforce	ement
Use Cached Results:	Use cached Roles and Posture	attributes from previous sessions
Enforcement Policy:	Aruba NAD Tacacs	Modify
	En	forcement Policy Details
Description:		
Default Profile:	[TACACS Deny Profile]	
Rules Evaluation Algorithm:	first-applicable	
Conditions		Enforcement Profiles
1. (Tips:Role CONALS [Aruba TACACS read-only Admin)) [TACACS Read-only Admin]
2. (Tips:Role anticities [Aruba TACACS root Admin])	[TACACS Network Admin]

				Login Status
8. 20(1)229(3			ACCE Aruba Devi Access Service	OF ASSIST
TACACS+ Session Deta	ils			
Summary Reques	t Policies Alerts			
Session ID:	T0000006-01-5d	55aba6		
Username:	read-only			
Time:	Aug 15, 2019 14:	59:50 EDT		
Status:	AUTHEN_STATUS	FAIL		
Authorizations:	0			
H + Showing 1 of 1-6	records 🕨 🖬		Export	Show Logs Close

 Server 						
10.2 129.1	TAC			ACCH MILLS	IE)EEX	
ACACS+ Session	Details					0
Summary Re	quest Polic	ies Alerts				
Authentication	Request Mes	sages				
Error Category:	Ta	cacs authentica	tion			
Error Code:	Au	thentication pr	vilege level mismatch			
Alerts for this F	Request:					

Summary Profile S	rvices	
Privilege Level:	1 (Normal)	
Selected Services:	cpass:HTTP	Export All TACACS+ Services Dictionaries
	Select	· ////////////////////////////////////
Authorize Attribute Status:	ADD •	
Custom Services:	To add new TACACS+ services / Dictionary	attributes, upload the modified dictionary xml - Update TACACS+ Services
		Service Attributes
Туре	Name	= Value
1. cpass:HTTP	AdminPrivileg	je = Read-only Administrator 🐴 🕸
2. Click to add		

A customer is trying to configure a TACACS Authentication Service for administrative access to the Aruba

Controller, During testing the authentication is not successful.

Given the screen shot what could be the reason for the Login status REJECT?

- A. The password used by the administrative user, user is wrong.
- B. The Enforcement profile is not designed to be used on Aruba Controller.
- C. The Read-only Administrator role does not exist on the Controller.
- D. The Enforcement profile used is not a TACACS profile.

Correct Answer: A

QUESTION 9

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 10

Refer to the exhibit:

Error Cod	e:	215						
Fror Cate		territor and the second	tion failure					
Error Mes		TLS sessio						
Alerts f	or this Req	uest						
	unknown ca	1	n SSL_read		094418:SSL	routines:ssl3	s_read_bytes:tisv	1 alert
		1	n SSL_read	with error:14	094418:SSL	routines:ssl3	š_read_bytesitisv	1 alert
	unknown ca	1	n SSL_read	with error:14	094418:SSL	routines:ssl3	s_read_bytes:tisv	1 alert
	unknown ca	1	n SSL_read	with error:14	094418:SSL	routines:ssl3	s_read_bytes:tisv	1 alert
	unknown ca	1	n SSL_read	with error:14	094418:SSL	routines:ssl3	s_read_bytes:tisv	1 alert
	unknown ca	1	n SSL_read	with error:14	094418:SSL	routines:ssl3	s_read_bytes:tisv	1 alert

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 11

You are deploying ClearPass Policy Manager with Guest functionality for a customer with multiple Aruba Networks Mobility Controllers The customer wants to avoid SSL errors during guest access but due to company security policy cannot use a wildcard certificate on ClearPass or the Controllers. What is the most efficient way to configure the customers guest solution? (Select two.)

- A. Build multiple Web Login pages with vendor settings configured for each controller
- B. Install the same public certificate on all Controllers with the common name "controller {company domain}"
- C. Build one Web Login page with vendor settings for controller (company domain)
- D. Install multiple public certificates with a different Common Name on each controller

Correct Answer: AB

QUESTION 12

When is it recommended to use a certificate with multiple entries on the Subject Alternative Name?

- A. The ClearPass servers are placed in different OnGuard zones to allow the client agent to send SHV updates.
- B. Using the same certificate to Onboard clients and the Guest Captive Portal on a single ClearPass server.
- C. The primary authentication server Is not available to authenticate the users.
- D. The ClearPass server will be hosting captive portal pages for multiple FQDN entries

Correct Answer: A