

Aruba Certified ClearPass Expert Written Exam

Questions & Answers Demo

Version: 4.0

Question: 1

Refer to the exhibit:

aruba	ClearPass Guest	Menu 🚍
Guest Onboard Configuration	Customize Self-Registration (HS-GuestArubaSelfReg)	Launch this self-registration page Launch self-service portal Launch network login
Start Here Start Here Start Here Substration Guest Manager Guest Manager Substrat Here Fields Fields Fields Guest Manager Start Here Fields Guest Manager Guest Manager Fields Guest Manager Guest M	The process for self-registration is shown bable. Cick an item to esit. Self-Registration 'HS-CuestAnubaSelfReg' Disabled Message Paname Page Paname Page Pa	ato
Templatas	Summary Page Reset Password Administrator	
Administration	Advanced editor	ClearPass Guest 6.7.9 109195 on C1000V platfic

A customer is deploying Guest Self-Registration with Sponsor Approval but does not like the format of the sponsor email. Where can you change the sponsor email?

- A. in the Receipt Page Actions
- B. in the Sponsor Confirmation section
- C. in me Configuration Receipts Email Receipts
- D. in the Configuration Receipts Templates

Answer: B

Question: 2

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

Answer: A

Question: 3

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]

of guration.						
WLANS:	- Admin Authenticat	tion Options				
Roles & Policies	Default role:	1000				
Access Points	Erutie:					
AP Groups	MSCHAPV2	a l				
Authentication	Server group:	Oes	Pess Tecara			
Services	Management techn	ti access				
troarfaces	Login activities per	nistence period: 0	days			
System						
Tasks	Lögin benner text					
gnostics	Banner has bit be	eccepted:				
ntenance	WEBUT AUTHENT	ICATION .				
	Uternamelpasses					
	Webui HTTPS port					
	Client certificate:					
	Server certificate	det	10 M			
	lide sension times	n#: 15	minutes	200		
ith Servers AAA Profi	Ide session Cines Re-extractication Rs L2 Authentication L3 A	treise	mouter			
Server Group - OnacPass	Te authentication L3 A leases Servers Options	terretuit:	Rules Ad		O Drag rom	a ta re o
Server Group - DearPass	Re-authentication L3 A Inceas Servers Options Inc. If Address	server Balles	Thules Ad	wanced		a ta re s
Server Group - DearPass	Te authentication L3 A leases Servers Options	server Balles	Thules Ad	arced	O Drag row	a la ce se
Server Group - DearPass	Re-authentication L3 A Inceas Servers Options Inc. If Address	server Balles	Thules Ad	wanced		ateres
Server Group - DearPass	Re-authentication L3 A Inceas Servers Options Inc. If Address	server Balles	Thules Ad	wanced		ateres
Server Group - DearPass	Te extraction L3 A locaes Servers Options ITE in Access MADE DECEMBER 1	terreitut: Authentication User Server Bulles Terre repos	The Ad	anced		Abres
Server Group - DearPass	Te extraction L3 A locaes Servers Options ITE in Access MADE DECEMBER 1	server Balles	The Ad	anced		
Server Group - DearPass	Teresterication L3 A Technic Servers Options Tru Procession Technic Completes T Server Options	terreitut: Authentication User Server Bulles Tana regos	The Ad	anced		
Server Group - ClearPean Countres 1 1	Te extraction L3 A locaes Servers Options ITE in Access MADE DECEMBER 1	terreitut: Authentication User Server Bulles Tana regos	The Ad	anced		
Server Group - ClearPass	Terestruction L3 A	terreitut: Authentication User Server Bulles Tana regos	The Ad	anced		
Server Group - ClearPean Countres 1 1	Teresterication L3 A Technic Servers Options Tru Procession Technic Completes T Server Options	terreitut: Authentication User Server Bulles Tana regos	The Ad	anced		
Server Group - ClearPass	Terestruction L3 A	terreitut: Authentication User Server Bulles Tana regos	The Ad	anced		
Server Group - CheerPeen Comments Server Group - ClearPeen Hunt: Hunt: Hunt: Hunt: Retype Hay:	Teresteriors L3 A	terreitut: Authentication User Server Bulles Tana regos	The Ad	anced		
Server Group - CherrPeen Name r Comments 1 1 Server Group - CherrPeen Hunt: Ray: Ratype Say: TCP port: Retromotic:	Terest + OcearPass T Server Op	terreitut: Authentication User Server Bulles Tana regos	The Ad	anced		
Server Group - CherrPean Name 7 Comments 1 1 Comments 1 Server Group - ClearPean Hunt: Hunt: Hunt: Retype Key: TCP port:	Es L2 Authentication L3 A	terreitut: Authentication User Server Bulles Tana regos	The Ad	anced		

P 10.1.120.100 - P	UTTY		- 0	×
				Í

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

Answer: CE

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.

Answer: A

Question: 5

Refer to the exhibit:

arubo		
Nease login (to the network using your usernam	e and password.
	new account clickCreate Account.	
-	Login	
Username:	accx@exam.com	
	Invalid username or password	
Password:		
Terms:	I accept the terms of use	
	Log in	

Request Details					
	Input Outpu	t Alerta			
The second se	1				
Login Status: Session Identif	REI	the state of the s			
Date and Time		00000c+01-5d68+82b			
End-Host Ident		23, 2019 11:43:40 EDT			
Usemame:		@exam.com			
Access Device	The second s	Cerexen cons			
System Postur					
379000070000	C DURINE	net door			
Servicet		Policies Us	net - unit in the second s		
Authentication	Mathadi Nat	appiicable			
Authentication		abbiecable			
Authorization 1					
Rolesz	Porta Car				
Enforcement P					
Service Monito					
Online Status:		Available			
1					
He + Showing 3	of 1-16 record	S # #4	antigoration Export	ihow Logs	
			and the second second second second	Constant of the local division of the	
Request Det	ails				
and the second division of the second divisio	n sandan ka	Alerts			
Summary	Input (Dutput Alerts			
Error Messa	ge: Failed to	ication failure classify request to ser	vice		
Error Messa Alerts for WebAuthSe	ge: Failed to this Reques	classify request to ser it eClassification failed {N			
Error Messa Alerts for WebAuthSe	ge: Failed to this Reques rvice Service > Edit- ACCX Gues	classify request to ser it eClassification failed {N			
Error Messa Alerts for WebAuthSe	ge: Failed to this Reques rvice Service > Edit- ACCX Gues	classify request to ser it eClassification failed {N			
Error Messa Alerts for WebAuthSe	ge: Failed to this Reques rvice Service > Edit - ACCX Gues Guest Access	classify request to ser it eClassification failed {N			
Error Messa Alerts for WebAuthSe figuration > Services VICes - ACCX Commany Service	ge: Failed to this Reques rivice Service > Edit - ACCX Gues Guest Access Authentication	classify request to ser it eClassification failed {N t Access Roles Enforcement			
Error Messa Alerts for WebAuthSe figuration > Services VICes - ACCX Commany Service Plices e:	ge: Failed to this Request invice Service > Edit - ACCX Guest Guest Access Authentication ACCX Guest Access	classify request to ser it eClassification failed {N t Access: Roles Enforcement	io service matched)		
Error Messa Alerts for WebAuthSe figuration > Services vices - ACCX C mmary Service rice: e: pription:	ge: Failed to this Request rvice Service > Edit - ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu	o classify request to ser at a Classification failed {N t Access: Roles Enforcement is est users logging in via captive po		ter their session ends.	
Error Messa Alerts for WebAuthSe figuration > Services VICes - ACCX Commany Service Plices e:	ge: Failed to this Request invice Service > Edit - ACCX Guest Guest Access Authentication ACCX Guest Access	o classify request to ser at a Classification failed {N t Access: Roles Enforcement is est users logging in via captive po	io service matched)	ter their session ends.	
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX Commany service rice: e: cription: :: us: tor Mode:	ge: Failed to this Request rvice Service Edit - ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled Disabled	o classify request to ser at a Classification failed {N t Access: Roles Enforcement is est users logging in via captive po	io service matched)	ter their session ends.	
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX Commany service rice: e: pription: e: us:	ge: Failed to this Request rvice Service Edit - ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled	o classify request to ser at a Classification failed {N t Access: Roles Enforcement is est users logging in via captive po	o service matched) rtal. Guests must re-authenticate at	ter their session ends.	
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX Commany Service rice: e: aription: :: us: tor Mode: e Options:	ge: Failed to this Request rvice Service Edit - ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled Disabled	o classify request to ser at a Classification failed {N t Access: Roles Enforcement is est users logging in via captive po	io service matched)	ter their session ends.	
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX Commany service rice: e: cription: :: us: tor Mode:	ge: Failed to this Request rvice Service Edit - ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled Disabled	o classify request to ser at a Classification failed {N t Access: Roles Enforcement is est users logging in via captive po	o service matched) rtal. Guests must re-authenticate at	ter their session ends.	Yalue
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX (Commany service rice: e: pription: e: us: tor Mode: e Options:	ge: Failed to this Request rvice Service Edit - ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled Disabled	Caling-Station-Id	o service matched) Intal. Guests must re-authenticate at Service Rule Operator EXISTS		
Error Messa Alerts for WebAuthSe figuration > Services wices - ACCX Commany Service rice: e: rription: :: us: tor Mode: toptions: h ALL of the following Type Radius:IETF Connection	ge: Failed to this Request rvice Service Edit - ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled Disabled	Caling-Station-Id Client-Mac-Address	o service matched) rtal. Guests must re-authenticate at Service Rule Operator EXISTS NOT_EQUAL:		%{Radius:IETF:User-Nat
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX (Commany service e: rription: e: sus: tor Mode: e Options: h ALL of the following Type Radius: IETF Connection Radius: Aruba	ge: Failed to this Request rvice Service Edit - ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled Disabled	Caling-Station-Id	o service matched) Intal. Guests must re-authenticate at Service Rule Operator EXISTS		
Error Messa Alerts for WebAuthSe figuration > Services wices - ACCX Commany Service rice: e: rription: :: us: tor Mode: toptions: h ALL of the following Type Radius:IETF Connection	ge: Failed to this Request rvice Service Edit - ACCX Gues Guest Access Authentication ACCX Guest Access To authenticate gu RADIUS Enforcem Enabled Disabled - conditions:	Caling-Station-Id Client-Mac-Address	o service matched) rtal. Guests must re-authenticate at Service Rule Operator EXISTS NOT_EQUAL:		%{Radius:IETF:User-Nat
Error Messa Alerts for WebAuthSe figuration > Services wices - ACCX Commany service e: cription: :: us: tor Mode: tor Mode: tor Mode: coptions: h ALL of the following Type Radius:IETF Connection Radius:Aruba hentication:	ge: Failed to this Request rvice Service > Edit - ACCX Gues Guest Access Authentication ACCX Guest Access To authenticate gu RADIUS Enforcem Enabled Disabled - conditions:	Calassify request to ser at aclassification failed (N t Access Roles Enforcement s est users logging in via captive po ent (Generic) Name Calling-Station-1d Client-Mac-Address Aruba-Essid-Name	o service matched) rtal. Guests must re-authenticate at Service Rule Operator EXISTS NOT_EQUAL:		%{Radius:IETF:User-Nat
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX (Commany Service e: e: pription: e: sus: tor Mode: e Options: h ALL of the following Type Radius:IETF Connection Radius:Aruba hentication: entication Methods:	ge: Failed to this Request rvice Service Edit- ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled Disabled - conditions:	Calassify request to ser at aclassification failed (N t Access Roles Enforcement s est users logging in via captive po ent (Generic) Name Calling-Station-1d Client-Mac-Address Aruba-Essid-Name	o service matched) rtal. Guests must re-authenticate at Service Rule Operator EXISTS NOT_EQUAL:		%{Radius:IETF:User-Nat
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX (Commany service e: ristice: e: rription: e: soptions: h ALL of the following Type Radius: IETF Connection Radius:Aruba hentication: ientication Methods:	ge: Failed to this Request rvice Service Edit- ACCX Gues Guest Access Authentication ACCX Guest Acces To authenticate gu RADIUS Enforcem Enabled Disabled - conditions:	Calassify request to ser at aclassification failed (N t Access Roles Enforcement s est users logging in via captive po ent (Generic) Name Calling-Station-1d Client-Mac-Address Aruba-Essid-Name	o service matched) rtal. Guests must re-authenticate at Service Rule Operator EXISTS NOT_EQUAL:		%{Radius:IETF:User-Nat
Error Messa Alerts for WebAuthSc figuration > Services rvices - ACCX C mmary Service rice: e: cription: :: us: tor Mode: e Options: h ALL of the following Type Radius:IETF Connection Radius:Aruba hentication: entication Methods: username Rules: rice Certificate: us:	ge: Failed to this Request rvice Service > Edit - ACCX Gues Guest Access Authentication ACCX Guest Access To authenticate gu RADIUS Enforcem Enabled Disabled - conditions: 1. [PAP] 2. [MSCHAP] 3. [CHAP] [Guest User Report -	Calassify request to ser at aclassification failed (N t Access Roles Enforcement s est users logging in via captive po ent (Generic) Name Calling-Station-1d Client-Mac-Address Aruba-Essid-Name	o service matched) rtal. Guests must re-authenticate at Service Rule Operator EXISTS NOT_EQUAL:		%{Radius:IETF:User-Nat
Error Messa Alerts for WebAuthSe figuration > Services rvices - ACCX (Commany Service e: rice: e: rription: e: source: e Options: h ALL of the following Type Radius:IETF Connection Radius:Aruba hentication: entication Methods: outper Rules: rice Certificate:	ge: Failed to this Request rvice Service Edit- ACCX Gues Guest Access Authentication ACCX Guest Access To authenticate gu RADIUS Enforcem Enabled Disabled - conditions: 1. [PAP] 2. [MSCHAP] 3. [CHAP] [Guest User Report	Calassify request to ser at aclassification failed (N t Access Roles Enforcement s est users logging in via captive po ent (Generic) Name Calling-Station-1d Client-Mac-Address Aruba-Essid-Name	o service matched) rtal. Guests must re-authenticate at Service Rule Operator EXISTS NOT_EQUAL:		%{Radius:IETF:User-Nat

Veb Login (ACC	* Pages > Web Logins: (X_1 ahTast)
e this form to make	changes to the Web Login ACCK_LabTest
والمعادية فتع	Web Login Editor
* Name:	ACCX_LubJest Exter a name for this web login page.
Page Namer	ACCX_TextPage Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Descriptions	
* Vendor Settings:	Comments or descriptive text about the web login. Arube Networks
Login Methods	Controller-Indiated Guest browser performs HTTP form subrid
* Address:	securelogn andbanet works com Enter the IP address or bestname of the wendur's product here.
Secure Login:	Ealerst a security uption to apply to the web logic process.
Dynamic Address	The controller will send the IP to submit condentials In multi-controller deployments, it is often required to post credentials to different addresses made evaluate as part of the original redirection The address above will be used whenever the parameter to not evaluable or fails the requirements helice.
age Redirect	arameters pasced in the initial redirect.
Security Hashr	Do not check - login will always be permitted. Select the laws of checking to easily to LFL parameters partied to the web lagin hape. Use this option to detect when UPL parameters have been modified by the specific as ample they SGAC address.
agin Form	e has average and constant of the lippin form.
Authentications	Credentials - Require a supername and password Salest the authentication requirement. Access Code requirement a regils code (summation) to be entered. Access Code requirement a regils code (summation) to be entered. Access code requirement for the same to entered block to be an entered. Access code to administration but the same it entered administrat.
Security Hashi	Do not check - login will always be permitted * Salect the level of checking to apply to URL parameters parsed to the web legin page. Use this option to detact when URL parameters have been modified by the user, for example their MAC address.
gin Form	
cons for specifying the	behaviour and content of the login form.
Authentications	Credentials - Require a unername and password Select the authentication requirement: Access Code requires a single code (username) to be entend. Ananymous allows a blank form requiring just the terms or a Log in buttom. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field inst.
Present CRAs	Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pag-up browser shown when juining a network that has a captive portal. Note that this option may not work with all wendors, depending on how the captive portal is implemented.
Custom Forme	Provide a custom login form If relected, you must supply your own HTML login form in the Header or Feoter HTML areas
Custom Labels:	Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login firm.
* Pre-Auth Checks	App Authentication — check using Aruba Application Authentication * Salect how the username and passened should be checked before proceeding to the NAS authentication.
Terms	III Require a Taims and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

A year ago, your customer deployed an Aruba ClearPass Policy Manager Server for a Guest SSIC hosted in an IAP Cluster. The customer just created a new Web Login Page for the Guest SSID. Even though the previous Web Login page worked test with the new Web Login Page are falling and the customer has forwarded you the above screenshots What recommendation would you give the customer to tix the issue? A. The service type configured is not correct. The Guest authentication should De an Application authentication type of service.

B. The customer should reset the password tor the username accx@exam com using Guest Manage Accounts

C. The Address filed under the WebLogin Vendor settings is not configured correctly, it should be set to instant arubanetworks.com

D. The WebLogin Pre-Auth Check is set to Aruba Application Authentication which requires a separate application service on the policy manager

Answer: A

Thank You For Trying HPE6-A77 PDF Demo

To try our HPE6-A77 Premium Files visit link below:

https://examsland.com/latest-exam-questions/HPE6-A77/

Start Your HPE6-A77 Preparation

Use Coupon EL25 for extra 25% discount on the purchase of Practice Test Software.