



Free Questions for HPE6-A81 by certsdeals

Shared by Riddle on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The customer would like to add a default common self-registration sponsor email under the initial value on all the ten self-registration pages created for different locations except for the guest registration page created for Sunnyvale location to use a different sponsor email in initial value. Under self-registration form fields, you have "Edit" and "Edit Base Field"

Which edit options will you choose to make minimal configuration changes to implement the customer's requirement? (Select two)

Options:

- A-** Update the common sponsor email by clicking the 'Edit' option of the sponsor email form field on the one of the self-registration register form page
- B-** Update the sponsor email by clicking on both 'Edit' and 'Edit Base Field' options of the sponsor_email filed on the Sunnyvale register page
- C-** Update the specific sponsor email by clicking on 'Edit Base Field' option of the sponsor_email form filed on the Sunnyvale location register form page
- D-** Update the common sponsor email by clicking the 'Edit Base Field' option of the sponsor_email form field on the one of the self-registration form page
- E-** Update the specific sponsor email by clicking on the 'Edit' option of the sponsor_email form filed on the Sunnyvale self-registration register form page

Answer:

A, B

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

Create New Report

Sample Report

What would you like to see in your new Report?

Report Name <input type="text" value="Name"/>	Category Authentication ▾	Notifications <input checked="" type="checkbox"/> Notify by Email <input type="text" value="it@ad1.com"/>	Options <input checked="" type="checkbox"/> Include raw data in output This is an executive report which includes pre-defined CSV columns
Description <input type="text" value="Description"/>	<input type="radio"/> Accounting - Bandwidth and Session <input type="radio"/> Auth Overview <input type="radio"/> Auth Trend <input type="radio"/> Auth by AuthSrc <input type="radio"/> Auth by ClearPass	<input type="checkbox"/> Notify by SMS <input type="text"/>	<input type="checkbox"/> Enable remote copy Configure the Remote Directory in the Administration section to specify the remote copy destination.

When creating a new report, there is in option to send report Notifications by Email Where is the email server configured?

Options:

A- In the ClearPass Policy Manager Messaging Setup under Administration.

- B-** In the Insight report on the next screen of the report definition
- C-** In the Insight Reports Interface under Administration on the sidebar menu
- D-** In the ClearPass Policy Manager Endpoint Context Servers under Administration.

Answer:

D

Question 3

Question Type: MultipleChoice

Which statement is true about Radius IETF attributes Called-Station-Id and Calling-Station-Id?

Options:

- A-** Called-Station-Id contains the mac address of the supplicant while Calling-Station-Id contains the mac address of the authenticator.
- B-** Called-Station-Id contains the mac address of the supplicant and SSID name while Calling-Station-Id contains the mac address of the authenticator.
- C-** Called-Station-Id contains the mac address of the authenticator while Calling-Station-Id contains the mac address of the supplicant.
- D-** Called-Station-Id contains the mac address of the authenticator while Calling-Station-Id contains the mac address of the supplicant

and SSID name.

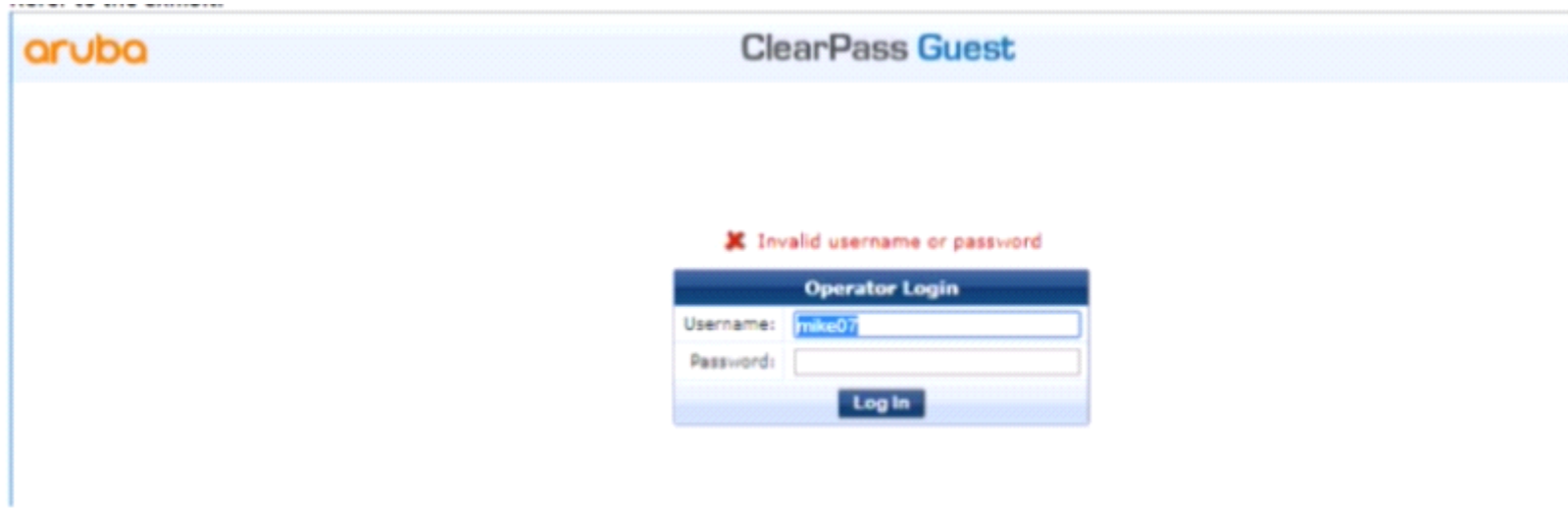
Answer:

D

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



The screenshot displays the Aruba ClearPass Guest Operator Login interface. At the top left is the Aruba logo, and at the top right is the text "ClearPass Guest". In the center, a red error message reads "X Invalid username or password". Below this is a login form titled "Operator Login" with a blue header. The form contains two input fields: "Username:" with the value "jrnike07" and "Password:" which is empty. A "Log In" button is positioned at the bottom of the form.

Request Details

Summary Input Output

Login Status:	ACCEPT
Session Identifier:	W0000000e-01-5ddfe2e3
Date and Time:	Nov 28, 2019 10:08:19 EST
End-Host Identifier:	-
Username:	mike07
Access Device IP/Port:	- -
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Guest Operator Logins - AD
Authentication Method:	Not applicable
Authentication Source:	AD1
Authorization Source:	AD1
Roles:	[User Authenticated]

Request Details

Summary Input Output

Login Status:	ACCEPT
Session Identifier:	W0000000e-01-5ddfe2e3
Date and Time:	Nov 28, 2019 10:08:19 EST
End-Host Identifier:	-
Username:	mike07
Access Device IP/Port:	- -
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Guest Operator Logins - AD
Authentication Method:	Not applicable
Authentication Source:	AD1
Authorization Source:	AD1
Roles:	[User Authenticated]
Enforcement Profiles:	Operator Login - AD Users
Service Monitor Mode:	Disabled
Callin Status:	Not Available

Showing 1 of 1-255 records

Change Status

Show Configuration

Export

Show Logs

Close

Request Details

Summary Input Output

Enforcement Profiles:	Operator Login - AD Users
System Posture Status:	UNKNOWN (100)

The customer configured a guest operator access by creating a custom operator profile and the built-in universal ClearPass profile mapping translation rule. When he tests the setup, he gets authentication failed. Using the screenshots sent by the customer as a reference, what would suggest to the customer to fix the issue?

Options:

- A-** To map the operator profile name HS_Receptionist in the translation rule value field
- B-** To re-enter the correct username and password for the Active Directory user Mike07.
- C-** To correct the case sensitive attribute name in the enforcement profile to admin_privileges
- D-** To verify if the username Mike07 has the Active Directory Title attribute set as Reception.

Answer:

A

Question 5

Question Type: MultipleChoice

The customer has configured the guest self-registration with sponsor approval. The guest users that the sponsor email and the other requested details while registering the account but the users were able to complete the authentication and access the internet without

the sponsor's approval.

What configuration settings will you check to make this setup work?

Options:

- A-** Check if sponsor name field is enabled in the register form page
- B-** Check if sponsor email field is enabled in the register form page
- C-** Check if authentication option n is enabled in the self-registration page enabled.
- D-** Check if sponsor confirmation is enabled in the self-registration page

Answer:

B

Question 6

Question Type: MultipleChoice

There is an Aruba Controller configured to stand 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?

Options:

- A- Aruba Controller will send stop messages only if EAP termination and Interim accounting are enabled.
- B- Configure EAP Termination on the Aruba Controller and the client will send a stop message.
- C- Aruba Controller will send stop messages if RADIUS Accounting Server Group is defined in the authentication profile.
- D- Aruba Controller will send stop messages only if both accounting and Interim accounting are enabled.

Answer:

C

Question 7

Question Type: MultipleChoice

A customer is troubleshooting a user that has complained about randomly having issues connecting the network with EAP PEAP using the Corporate Laptop. The initial checks are showing a number of authentication failures but no sign of issues with the ClearPass server or AD.

What can the Customer do to monitor this user Authentication trend closely over the next few days?

Options:

- A- configure a Report using Radius Failed Authentication template and schedule it to run every 5 mins
- B- configure an Alert using Failed Authentication template with Threshold 1. Interval 5 mins
- C- add the user name in the Insight/Alert/Watchlist and get the authentication failures notifications within 30 seconds
- D- add to ClearPass Insight Dashboard the Authentication Status widget for this specific user

Answer:

C

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

The screenshot shows a 'Request Details' window with four tabs: Summary, Input, Output, and Alerts. The Alerts tab is active, displaying the following information:

Error Code:	215
Error Category:	Authentication failure
Error Message:	TLS session error

Alerts for this Request

```
RADIUS Cannot connect to OCSP server p50-t07-cp1
EAP-TLS: fatal alert by server - internal_error
TLS Handshake failed in SSL_read with error:2006A066: BIO routines: BIO_get_host_ip: bad
hostname lookup
eap-tls: Error in establishing TLS session
```

At the bottom of the window, there is a navigation bar with the text 'Showing 1 of 1-20 records' and four buttons: 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

A customer has configured Onboard in a cluster. After the Primary server's failure, the BYOD devices fail to connect to the network. Which step below is the best starting point when troubleshooting'

Options:

A- Verify the CPPM hostname in OSCP URL under TLS authentication method is updated to localhost instead of primary server's hostname.

- B-** Reboot the active ClearPass server and reconnect the client to the SSID by selecting the correct certificate when prompted.
- C-** Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client.
- D-** Check EAP certificate on the secondary node is issued by the same common root Certificate Authority (CA).

Answer:

A

Question 9

Question Type: MultipleChoice

Refer to the exhibit.

Services - HPE-Aruba Wired Mac auth

Summary Service Authentication Authorization Roles Enforcement Profiler

Service:

Name:	HPE-Aruba Wired Mac auth
Description:	MAC-based Authentication Service
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	1. Authorization 2. Profile Endpoints

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Radius:IETF	NAS-IP-Address	BELONGS_TO_GROUP	HPE-Aruba Switches

Authentication:

Authentication Methods:	[Allow All MAC AUTH]
Authentication Sources:	[Local User Repository]
Strip Username Rules:	-

Authorization:

Authorization Details:	[Endpoints Repository]
------------------------	------------------------

Roles:

Role Mapping Policy:	HS_Building Role Mapping Policy
----------------------	---------------------------------

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	HPE-ArubaOS Mac auth policy

Profiler:

Endpoint Classification:	ANY
RADIUS CoA Action:	[ArubaOS Switching - Bounce Switch Port]

[← Back to Services](#)

Disable

Copy

Save

Cancel

Services - HS_Building Aruba 802.1x service

Summary Service Authentication Authorization Roles Enforcement Profiler

Role Mapping Policy:	HS_Building Role Mapping Policy	Modify	Add New Role Mapping Policy
----------------------	---------------------------------	--------	-----------------------------

Role Mapping Policy Details

You configured the Wired MAC - Auth service enforcement conditions with the Endpoint profiling data. When mac-auth based clients connect to the network, ClearPass assigns Deny access profile. The customer has sent you the above screenshots. How would you resolve the issue?

Options:

- A-** Change the Rules evaluation algorithm in the Enforcement policy of HPE ArubaOS Mac auth policy as 'select all matches' and add the CoA action as HPE Bounce switch port in the profiler tab.
- B-** Create a new condition in last position with Type and operator as Tips:Role EQUALS [User Authenticated] with action as Allow access profile permitting any services and any ports to do profiling.
- C-** Create a new condition in first position with Type and operator as Authorization (Endpoint Repository):Category NOT_EXISTS with action as Limited access profile allowing only DHCP service.
- D-** Create a new condition in the first position with Type and operator as Authorization [Endpoint Repository] Category NOT_EXISTS with action as Limited access profile and ArubaOS wireless terminate session

Answer:

A

Question 10

Question Type: MultipleChoice

Refer to the exhibit.

TACACS+ Session Details

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]

Select a capture mode

Showing 2 of 1-2 records

Export Show Logs Close

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Diagnostics

Maintenance

Admin Authentication OptionsDefault role: Enable: MSCHAPv2: Server group: Management telnet access: Login activities persistence period: daysLogin banner text: Banner has to be accepted: **WEBUI AUTHENTICATION**Username/password: Webui HTTPS port (443) access: Client certificate: Server certificate: Idle session timeout: minutesRe-authentication timeout: minutes**Server Group > ClearPass Tacacs** **Servers** Options Server Rules Drag rows to re-order

NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
ClearPass T	TACACS	10.1.129.111	--	+

**Server Group > ClearPass Tacacs > ClearPass T** **Server Options** Server Group Trim FQDN Server Group Match Rules

Host:

```
10.1.120.100 - PuTTY
(P50-T12-MC) [mynode] #show loginsessions

Session Table
-----
ID  User Name  User Role  Connection From  Idle Time  Session Time  Path
--  -
1   admin      root       10.1.29.90       00:00:10   00:00:42     /
2   read-only  root       10.1.29.90       00:00:39   00:01:45     /
3   admin      root       10.1.29.90       00:00:25   00:18:45     /
```

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.)

Options:

- A- The read-only enforcement profile is mapped to the root role
- B- The ClearPass user role associated to the read-only user is wrong.
- C- On the Controller, the TACACS authentication server is not configured for Session authorization
- D- The Controller's Admin Authentication Options Default role is mapped to root
- E- The Controller Server Group Match Rules are changing the user role.

Answer:

B, D

To Get Premium Files for HPE6-A81 Visit

<https://www.p2pexams.com/products/hpe6-a81>

For More Free Questions Visit

<https://www.p2pexams.com/hp/pdf/hpe6-a81>

