

[Q17-Q31 Tested Material Used To HPE6-A82 Test Engine Exam Questions in here [Jul-2022]



Tested Material Used To HPE6-A82 Test Engine Exam Questions in here [Jul-2022]

Penetration testers simulate HPE6-A82 exam PDF NO.17 What is the benefit to installing a wild card certificate for captive portal authentication?

- * Guests no longer are required to validate certificates during captive portal.
- * Allows different certificates for each controller for increased security
- * Wild card certificates are provide greater security than normal certificates
- * Allows the single wild card certificate to be installed on all controllers in the environment

NO.18 What needs to be configured for ClearPass use an enforcement rule base on client Data Cap?

- * Interim Accounting on the Network Access Device (NAD).
- * Enable Active Sessions in ClearPass Guest
- * Enable Logging of Accounting Start-Stop packets.
- * Make sure the Endpoint Profiling is configured

NO.19 Sponsorship has been enabled on the guest network. A guest user connects and completes the self- registration form indicating a valid sponsor. The guest then clicks submit.

What is the current state of the guest account?

- * The guest account is created in an enabled state with the '“Log In” button functional.
- * The guest account is created in disabled state, the '“Log In” button will appear only after the sponsor approval process is completed.

- * The guest account is created in a disabled state with the “Log In” button grayed out.
- * The guest account is not yet created and remains in a disabled state. There is not “Log In” button yet displayed.

NO.20 What services are recommended to be allowed by the pre-authenticated role assigned to the Client during the Captive Portal process? (Choose three.)

- * HTTPS to the internet
- * DHCP options 43 and 150
- * DHCP address assignment
- * RADIUS to ClearPass
- * HTTPS to ClearPass
- * DNS resolution

NO.21 Which option supports DHCP profiling for devices in a network?

- * Configuring DHCP relay on ClearPass in order to allow the client to receive DHCP after being profited
- * Enabling DHCP relay on Network Access Devices (NADs) to forward DHCP requests to ClearPass
- * DHCP profiling is enabled on ClearPass by default configuration of DHCP relay on the Network Access Device (NAD) is not required
- * Enabling the DHCP server to profile endpoints and forward the meta-data to Clearpass.

NO.22 Refer to the exhibit.

Web Login (Guest Network)

Use this form to make changes to the Web Login **Guest Network**.

Web Login Editor	
* Name:	<input type="text" value="Guest Network"/> Enter a name for this web login page.
Page Name:	<input type="text" value="arubalogin"/> Enter a page name for this web login. The web login will be accessible from <code>{youripaddress}/page-name.php</code> .
Description:	<input type="text"/> Comments or descriptive text about the web login.
* Vendor Settings:	<input type="text" value="Aruba Networks"/> Select a predefined group of settings suitable for standard network configurations.
Login Method:	<input type="text" value="Controller-initiated — Guest browser performs HTTP form submit"/> Select how the user's network login will be handled. <small>Controller-initiated: The user's browser is redirected to the controller's web login page, usually from the captive portal redirection process.</small>
* Address:	<input type="text" value="securelogin.arubanetworks.com"/> Enter the IP address or hostname of the vendor's product here.
Secure Login:	<input type="text" value="Use vendor default"/> Select a security option to apply to the web login process.
Dynamic Address:	<input checked="" type="checkbox"/> 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 redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

Where will the guests browser be redirected during a captive portal login attempt?

- * The captive portal page hosted on the Aruba controller
- * The redirect will time out and fan to resolve
- * The captive portal page hosted on ClearPass

* The captive portal page hosted on Aruba Central in the cloud

NO.23 Which option supports DHCP profiling for devices in a network?

- * configuring ClearPass as a DHCP relay for the client
- * DHCP profiling is enabled on ClearPass by default; configuration of the network access devices is not necessary
- * enabling the DHCP server to profile endpoints and forward meta-data to ClearPass
- * enabling DHCP relay on our network access devices so DHCP requests are forwarded to ClearPass

NO.24 ClearPass receives fingerprinting profile data for a client device that is based on MAC OUI, NMAP, DHCP, and OnGuard. Which fingerprint or fingerprints are used?

- * All fingerprints are applied
- * The last fingerprint gathered
- * NMAP because it is actively obtained
- * OnGuard because it is application based

NO.25 A customer with 677 employees would like to authenticate employees using a captive portal guest web login page. Employees should use their AD credentials to login on this page.

Which statement is true?

- * The customer needs to add second guest service in the policy manager for the guest network.
- * The customer needs to add the AD server as an authentication source in a guest service.
- * Employees must be taken to a separate web login page on the guest network.
- * The customer needs to add the AD servers RADIUS certificate to the guest network.

NO.26 Refer to the exhibit.

Enforcement Policies - Corp SSID Access

Summary | Enforcement | Rules

Enforcement:

Name: Corp SSID Access
Description:
Enforcement Type: RADIUS
Default Profile: Allow Internet Only Access

Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (User:Role EQUALS Employee)	Allow Full Access
2. (User:Role EQUALS [Contractor])	Corp Secure Contractor
3. (User:Role EQUALS Corp BYOD)	Secure Corp BYOD Access

Configuration > Identity > Local Users

Local Users

Filter: Role contains employee [Go] [Clear Filter]

#	User ID	Name	Role
1.	john	john	[Employee]
2.	mike	mike	[Employee]
3.	neil	neil	[Employee]

Showing 1-3 of 3

Exhibit: ACCA82-345

what will be the enforcement for the user “neil”?

- * Corp Secure Contractor

- * Allow Full Access
- * Secure Corp BYOD Access
- * Allow internet Only Access

NO.27 Refer to the exhibit.

Web Login (Guest Network)

Use this form to make changes to the Web Login **Guest Network**.

The screenshot shows the 'Web Login Editor' interface. The form is titled 'Web Login Editor' and contains the following fields and options:

- Name:** Guest Network (text input)
- Page Name:** arubalogin (text input)
- Description:** (text area)
- Vendor Settings:** Aruba Networks (dropdown menu)
- Login Method:** Controller-initiated — Guest browser performs HTTP form submit (dropdown menu)
- Address:** securelogin.arubanetworks.com (text input, highlighted with a red box)
- Secure Login:** Use vendor default (dropdown menu)
- Dynamic Address:** The controller will send the IP to submit credentials

Where will the guests browser be redirected during a captive portal login attempt?

- * The captive portal page hosted on the Aruba controller
- * The redirect will time out and fan to resolve
- * The captive portal page hosted on ClearPass
- * The captive portal page hosted on Aruba Central in the cloud

NO.28 Sponsorship has been enabled on the guest network A guest user connects and completes the self-registration form indicating a valid sponsor. The guest then clicks submit What is the current state of the guest account?

- * The guest account is created in a disabled state with the Log In button grayed out
- * The guest account is not yet created and remains in a disabled state There is not Log in button yet displayed
- * The guest account is created in disabled state, the Log In button will appear only after the sponsor approval process is completed
- * The guest account is created in an enabled state with the Log In button functional

NO.29 What is a function of the posture token in ClearPass OnGuard? (Select two)

- * Identifies clients that are not security compliant
- * Initiates the Auto-Remediation process
- * Controls access to network resources
- * Denies access to unhealthy clients

* indicates the Health Status of the Client

NO.30 Refer to the exhibit.

The screenshot shows the 'ClearPass Policy Manager' interface for configuring an authentication source. The breadcrumb trail is 'Configuration > Authentication > Sources > Add - Remote Lab AD'. The page title is 'Authentication Sources - Remote Lab AD'. There are tabs for 'Summary', 'General', 'Primary', 'Attributes', 'Backup 1', and 'Backup 2', with 'General' selected. The configuration fields are as follows:

- Name:** Remote Lab AD
- Description:** (Empty text area)
- Type:** Active Directory
- Use for Authorization:** Enable to use this Authentication Source to also fetch role mapping attributes
- Authorization Sources:** (Empty list with 'Remove' and 'View Details' buttons, and a '-- Select --' dropdown)
- Server Timeout:** 10 seconds
- Cache Timeout:** 36000 seconds
- Backup Servers Priority:** Backup 1, Backup 2 (with 'Move Up', 'Move Down', 'Add Backup', and 'Remove' buttons)

A client is attempting to authenticate using their Windows account with a bad password if the Remote Lab AD server is down for maintenance, what will be the expected result?

- * ClearPass receives a timeout attempt when trying the Remote Lab AD server first. It will then try the server Backup 1 and receive a result of Active Directory Authentication failed. No further processing will occur.
- * ClearPass try either server Backup 1 or Backup 2 depending on which has responded the fastest in prior attempts to authenticate ClearPass will then receive a result of Active Directory Authentication failed.

No further processing will occur.

- * ClearPass receives a timeout attempt when trying the Remote Lab AD server first. It will then try the server Backup 1 and Backup 2; both will send a result authentication failed.
- * ClearPass receive a timeout attempt when trying the Remote Lab AD server first. No further processing will occur until the Remote Lab AD server is marked as Down; by the Administrator.

NO.31 What is RADIUS Change of Authorization (CoA)?

- * It allows ClearPass to transmit messages to the Network Attached Device/Network Attached Server (NAD/NAS) to modify a user's session status
- * It allows clients to issue a privilege escalation request to ClearPass using RADIUS to switch to TACACS+
- * It is a mechanism that enables ClearPass to assigned a User-Based Tunnel (UBT) between a switch and controller for Dynamic

Segmentation

* It forces the client to re-authenticate upon roaming to an access point controlled by a foreign mobility controller.

Reference:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPM_UserGuide/Enforce/EPRADIUS_CoA.htm

Authentic Best resources for HPE6-A82 Online Practice Exam:

<https://www.actualtests4sure.com/HPE6-A82-test-questions.html>