

HPE6-A82^{Q&As}

HPE Sales Certified - Aruba Products and Solutions

Pass HP HPE6-A82 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/hpe6-a82.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

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. (Tips:Role EQUALS employee)	Allow Full Access
2. (Tips:Role EQUALS [Contractor])	Corp Secure Contractor
3. (Tips:Role EQUALS Corp BYOD)	Secure Corp BYOD Access

Configuration > Identity > Local Users

Local Users

Filter: contains

<input type="checkbox"/>	<input type="checkbox"/> User ID ▲	Name	Role
1.	<input type="checkbox"/> john	john	[Employee]
2.	<input type="checkbox"/> mike	mike	[Employee]
3.	<input type="checkbox"/> neil	neil	[Employee]

Showing 1-3 of 3

What will be the enforcement for the user "neil"?

- A. Allow Full Access
- B. Secure Corp BYOD Access
- C. Allow Internet Only Access
- D. Corp Secure Contractor

Correct Answer: A

QUESTION 2

Which must be taken into account if a customer wants to use the DHCP collector with 802.1X authentication?

- A. When a client sends an authentication request to ClearPass, the profiler will also gather DHCP information.
- B. Because DHCP fingerprinting is a Layer-3 function, it cannot be used with an 802.1X authentication service.
- C. The client needs to connect to an open network first to be profiled, then shifted to the secure 802.1x network.
- D. The client needs to be granted limited access before the enforcement policy can take into account the device type.

Correct Answer: A

QUESTION 3

Refer to the exhibit.

ClearPass Policy Manager
Configuration > Authentication > Sources > Add - Remote Lab AD

Authentication Sources - Remote Lab AD

Summary	General	Primary	Attributes	Backup 1	Backup 2
Name:	Remote Lab AD				
Description:					
Type:	Active Directory				
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes				
Authorization Sources:					Remove View Details
Server Timeout:	10 seconds				
Cache Timeout:	36000 seconds				
Backup Servers Priority:	Backup 1 Backup 2				Move Up Move Down
Add Backup Remove					

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?

- A. 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.
- B. 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.
- C. 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.

D. 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.

Correct Answer: A

QUESTION 4

What is an effect of the Cache Timeout setting on the authentication source settings for Active Directory?

- A. ClearPass will validate the user credentials, then, for the duration of the cache, ClearPass will just fetch account attributes.
- B. The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the A/D server by caching the attributes.
- C. ClearPass will validate the user credentials on the first attempt, then will always fetch the account attributes.
- D. The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the A/D server by caching the credentials.

Correct Answer: B

Reference: <https://community.arubanetworks.com/blogs/arunkumar1/2020/10/20/what-is-the-difference-between-authentication-cache-timeout-and-machine-authentication-cache-timeout>

QUESTION 5

Refer to the Endpoint in the screenshot.

Edit Endpoint			
Fingerprints	Endpoint	Attributes	
MAC Address	18ee6952ee34	IP Address	-
Description		Static IP	FALSE
Status	<input checked="" type="radio"/> Known client <input type="radio"/> Unknown client <input type="radio"/> Disabled client	Hostname	faculty:iOS 11.3:PDA 25
MAC Vendor	Apple, Inc.	Device Category	SmartDevice
Added by	clusteradmin	Device OS Family	Apple
Online Status	Not Available	Device Name	Apple iPad
Connection Type	Unknown	Added At	Feb 15, 2019 14:40:32 PST
		Last Profiled At	Feb 15, 2019 14:40:32 PST

Save Cancel

What are possible ways that it was profiled? (Choose two.)

- A. Exchange Plugging agent

B. NAD ARP listening handler

C. 3rd part MDM

D. DNS fingerprinting

E. Cisco Device Sensor

Correct Answer: BC

[HPE6-A82 VCE Dumps](#)

[HPE6-A82 Exam Questions](#)

[HPE6-A82 Braindumps](#)