



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.pass4itsure.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

What is true regarding Posturing and Profiling?

- A. Profiling describes categorizing the user based on their department while Posturing validates the user as authenticated.
- B. Profiling is the act of identifying the endpoint type while Posturing is assigning a status as to the health of the endpoint.
- C. Posturing and Profiling are role assignments in ClearPass used internally to map to enforcement policies.
- D. Both Posturing and Profiling describe the same thing; what is the health of the client endpoint?

Correct Answer: D

QUESTION 2

What is a function of the posture token in ClearPass OnGuard? (Choose two.)

- A. Identifies clients that are not security compliant.
- B. Initiates the Auto-Remediation process.
- C. Indicates the Health Status of the Client.
- D. Denies access to unhealthy clients.
- E. Controls access to network resources.

Correct Answer: CD

Reference: <https://docplayer.net/18755148-Clearpass-onguard-configuration-guide.html> (3)

QUESTION 3

Refer to the exhibit.



Summary	Service	Authentication	Authorization	Roles	Enforcement
Authorization Details:					
Authorization sources from which role mapping attributes are fetched					
Authentication Source					
1. [Endpoints Repository] [Local SQL DB]					
Additional authorization sources from which to fetch role-mapping attributes					
<div><div>[Time Source] [Local SQL DB]</div><div>[Guest User Repository] [Local SQL DB]</div></div>					
<div><div>Remove</div><div>View Details</div><div>Modify</div></div>					
<div>--Select to Add--</div>					

When creating a new ClearPass Service, the [Time Source] has been added as an authorization source. What time source is ClearPass referencing?

- A. the ClearPass server where Insight Master has been enabled
- B. the local clock of the ClearPass server doing the authentication
- C. the local time setting found on the authenticating client machine
- D. the NTP (Network Time Protocol) source indicated in the Cluster settings

Correct Answer: C

QUESTION 4

Which authentication method requires a client certificate?

- A. EAP-TLS
- B. Guest self-registration
- C. PEAP
- D. MAC Authentication

Correct Answer: A

QUESTION 5

Refer to the exhibit.



Configuration > Authentication > Sources > Add - AD1

Authentication Sources - AD1

Summary	General	Primary	Attributes	Backup 1	Backup 2
Name:	<input type="text" value="AD1"/>				
Description:	<input type="text"/>				
Type:	Active Directory				
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes				
Authorization Sources:	<div><input type="text" value="-- Select --"/></div> <div><input type="button" value="Remove"/> <input type="button" value="View Details"/></div>				
Server Timeout:	<input type="text" value="10"/> seconds				
Cache Timeout:	<input type="text" value="36000"/> seconds				
Backup Servers Priority:	<div><input type="text" value="Backup 1"/> <input type="text" value="Backup 2"/></div> <div><input type="button" value="Move Up"/> <input type="button" value="Move Down"/></div> <div><input type="button" value="Add Backup"/> <input type="button" value="Remove"/></div>				
< Back to Authentication Sources			<input type="button" value="Clear Cache"/>	<input type="button" value="Copy"/>	<input type="button" value="Save"/>

What are two consequences of the Cache Timeout being set to 36000 seconds? (Choose two.)

- A. ClearPass will cache all user and machine attributes from AD every 10 hours in anticipation of one of those users or machines attempting to authenticate.
- B. Less traffic is required between ClearPass and the AD server when re-authenticating within a 10 hour period.
- C. The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the AD server by caching user credentials for a 10 hour period.
- D. A user changing departments may not see their Department attribute change in AD reflected while authenticating until the Cache Timeout period has ended.
- E. On a failed authentication attempt, ClearPass will consider any subsequent attempts within 10 hours as total failed attempts before blacklisting the client.

Correct Answer: AC

[HPE6-A82 PDF Dumps](#)[HPE6-A82 Practice Test](#)[HPE6-A82 Study Guide](#)