



HPE6-A15^{Q&As}

Aruba Certified Clearpass Professional 6.5

Pass HP HPE6-A15 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/hpe6-a15.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

A customer wants all guests who access a company's guest network to have their accounts approved by the receptionist, before they are given access to the network. How should the network administrator set this up in ClearPass? (Select two.)

- A. Enable sponsor approval confirmation in Receipt actions.
- B. Configure SMTP messaging in the Policy Manager.
- C. Configure a MAC caching service in the Policy Manager.
- D. Configure a MAC auth service in the Policy Manager.
- E. Enable sponsor approval in the captive portal authentication profile on the NAD.

Correct Answer: AD

A: Sponsored self-registration is a means to allow guests to self-register, but not give them full access until a sponsor (could even be a central help desk) has approved the request. When the registration form is completed by the guest/user, an on screen message is displayed for the guest stating the account requires approval.

Guests are disabled upon registration and need to wait on the receipt page for the confirmation until the login button gets enabled.

D. Device Mac Authentication is designed for authenticating guest devices based on their MAC address.

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 94 <https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf>

QUESTION 2

A client's authentication is failing and there are no entries in the ClearPass Access tracker. What is a possible reason for the authentication failure?

- A. The user account has expired.
- B. The client used a wrong password.
- C. The shared secret between the NAD and ClearPass does not match.
- D. The user's certificate is invalid.
- E. The user is not found in the database.

Correct Answer: C

QUESTION 3

Which component of a ClearPass Service is mandatory?



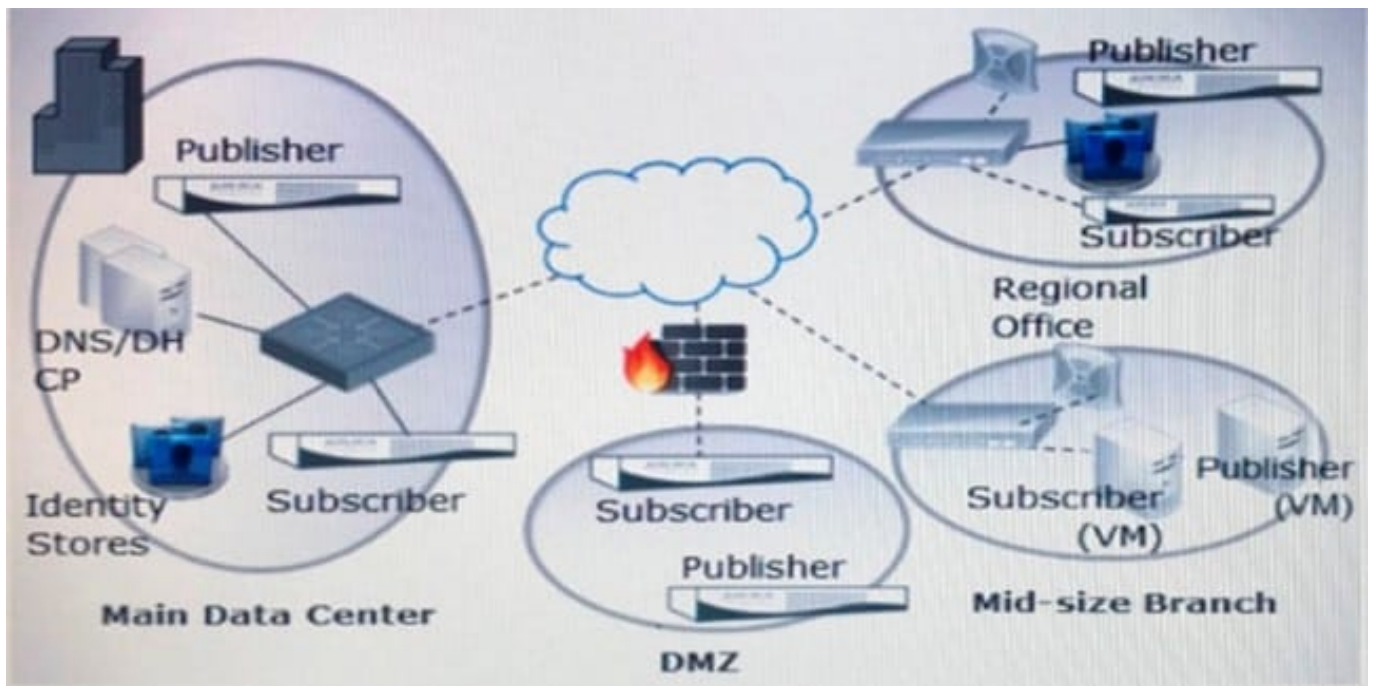
- A. Authorization Source
- B. Profiler
- C. Role Mapping Policy
- D. Enforcement
- E. Posture

Correct Answer: D

An enforcement policy is a way to organize enforcement profiles and apply them to users or Policy Manager roles. Based on the enforcement policy assigned to the role, enforcement profiles are applied to the service request.

QUESTION 4

Refer to the exhibit.



A customer wants to enable Publisher redundancy.

Based on the network topology diagram shown, which node should the network administrator configure as the standby Publisher for the Publisher in the main data center?

- A. Subscriber in the main data center
- B. Publisher in the regional office
- C. any of the other three Publishers
- D. Publisher in the mid-size branch



E. Publisher in the DMZ

Correct Answer: A

ClearPass Policy Manager allows you to designate one of the subscriber nodes in a cluster to be the Standby Publisher, thereby providing for that subscriber node to be automatically promoted to active Publisher status in the event that the Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum.

References: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster%20Deployment/Standby_publisher.htm

QUESTION 5

Refer to the exhibit.

View Endpoint			
MAC Address	98b8e362fddf	IP Address	192.168.1.252
Description		Static IP	FALSE
Status	Unknown	Hostname	
Added by	Policy Manager	MAC Vendor	Apple
		Category	SmartDevice
		OS Family	Apple
		Device Name	Apple iPad
		Updated At	Apr 10, 2013 19:47:28 UTC
		Show Fingerprint	<input checked="" type="checkbox"/>

Endpoint Fingerprint Details	
Host User Agent	Mozilla/5.0 (iPad; CPU OS 6_0_2 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A8500 Safari/8536.25
DHCP Option55	["1,3,6,15,119,252"]
DHCP Options	["53,55,57,61,50,51,12"]

Based on the Endpoint information shown, which collectors were used to profile the device as Apple iPad? (Select two.)

- A. HTTP User-Agent
- B. SNMP
- C. DHCP fingerprinting
- D. SmartDevice
- E. OnGuard Agent

Correct Answer: AC

HTTP User-Agent

In some cases, DHCP fingerprints alone cannot fully classify a device. A common example is the Apple family of smart devices; DHCP fingerprints cannot distinguish between an Apple iPad and an iPhone. In these scenarios, User-Agent strings sent by browsers in the HTTP protocol are useful to further refine classification results.



User-Agent strings are collected from:

*

ClearPass Guest

*

ClearPass Onboard

*

Aruba controller through IF-MAP interface

Note: Collectors are network elements that provide data to profile endpoints. The following collectors send endpoint attributes to Profile:

*

DHCP DHCP snooping Span ports

*

ClearPass Onboard

*

HTTP User-Agent

*MAC OUI ?Acquired via various auth mechanisms such as 802.1X, MAC auth, etc.

*

ActiveSync plugin

*

CPPM OnGuard

*SNMP

*

Subnet Scanner

*

IF-MAP

*

Cisco Device Sensor (Radius Accounting)

*

MDM



References: Tech Note: ClearPass Profiling (2014), page 11 <https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf>

[Latest HPE6-A15 Dumps](#)

[HPE6-A15 Practice Test](#)

[HPE6-A15 Braindumps](#)