

HPE6-A77^{Q&As}

Aruba Certified ClearPass Expert Written

Pass HP HPE6-A77 Exam with 100% Guarantee

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

<https://www.leads4pass.com/hpe6-a77.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

There is an Aruba Controller configured to send 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?

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

Correct Answer: D

QUESTION 2

Refer to the exhibit:

Monitoring » Live Monitoring » Access Tracker

Access Tracker Aug 21, 2019 20:03:29 CEST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] default (2 servers) Last 1 day before Today

Filter: Source contains Webauth Go Clear Filter

#	Server	Source	Username	Service	Login Status	Request Timestamp
21.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:18:03
22.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:15:06
23.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:12:11
24.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:09:14
25.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:06:19
26.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:03:23
27.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 10:00:28
28.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:57:31
29.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:54:36
30.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:51:41
31.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:48:44
32.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:45:49
33.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:42:54
34.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:39:56
35.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:37:00
36.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:34:05
37.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:31:10
38.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:28:15
39.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:25:19
40.	10.254.5.2	WEBAUTH	7c5cf8cb5246	T2-HeathCheck-Service	ACCEPT	2019/08/21 09:22:23

A customer has just configured a Posture Policy and the T2-Healthcheck Service. Next they installed the OnGuard Agent on Secure_Employee SSID. When they check Access Tracker they see many WEBAUTH requests are being triggered.

What could be the reason?

- A. OnGuard Web-Based Health Check interval has been wrongly configured to three minutes.
- B. The OnGuard Agent trigger the events based on changing the Health Status
- C. TCP port 6658 is not allowed between the client and the ClearPass server
- D. The OnGuard Agent is connecting to the Data Port interface on ClearPass

Correct Answer: A

QUESTION 3

You have integrated ClearPass Onboard with Active Directory Certificate Services (ADCS) web enrollment to sign the final device TLS certificates. The customer would also like to use ADCS for centralized management of TLS certificates including expiration, revocation, and deletion through ADCS.

What steps will you follow to complete the requirement?

- A. Remove the EAP-TLS authentication method and add "EAP-TLS with OCSP Enabled\\" authentication method in the OnBoard Provisioning service. No other configuration changes are required.
- B. Copy the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL, remove EAP-TLS and map the custom created method to the Onboard Provisioning Service.
- C. Copy the default [EAP-TLS with OSCP Enabled] authentication method and update the correct ADCS server OCSP URL. remove EAP-TLS and map the custom created method to the OnBoard Authorization Service.
- D. Edit the [EAP-TLS with OSCP Enabled) authentication method and set the correct ADCS server OCSP URL. remove EAP-TLS and map the [EAP-TLS with OSCP Enabled) method to the Onboard Provisioning Service.

Correct Answer: A

QUESTION 4

A customer is complaining that some of the devices, in their manufacturing network, are not getting profiled while other IoT devices from the same subnet have been correctly profiled. The network switches have been configured for DHCP IP helpers and IF-MAP has been configured on the Aruba Controllers. What can the customer do to discover those devices as well? (Select two.)

- A. Update the Fingerprints Dictionary to the latest in case new devices have been added.
- B. Open a TAC case to help you troubleshoot the DHCP device profile functionality.
- C. Add the ClearPass Server IP as an IP helper address on the default gateway as well.
- D. Allow time for IF-MAP service on the controller to discover the new devices as well.
- E. Manually create a new device fingerprint for the devices that are not being profiled.

Correct Answer: DE

QUESTION 5

You have configured a Guest SSID with Captive-portal Web Authentication and MAC authentication. The MAC caching expiry time is set to 12 hours and the Guest Account expiration time is set to 8 hours. What will happen if the guest were to disconnect from the SSID and re-connect 9 hours later?

- A. The client will fail the MAC authentication and be denied access to the Guest SSID.
- B. The client will successfully pass the mac authentication until the mac caching time expires.
- C. The client will successfully pass the MAC authentication but still be redirected to captive portal page.
- D. The client will fail the MAC authentication and will be redirected to the Captive-portal login page.

Correct Answer: C

[HPE6-A77 PDF Dumps](#)

[HPE6-A77 Study Guide](#)

[HPE6-A77 Braindumps](#)