HPE6-A81$^{\text{Q\&As}}$

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

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

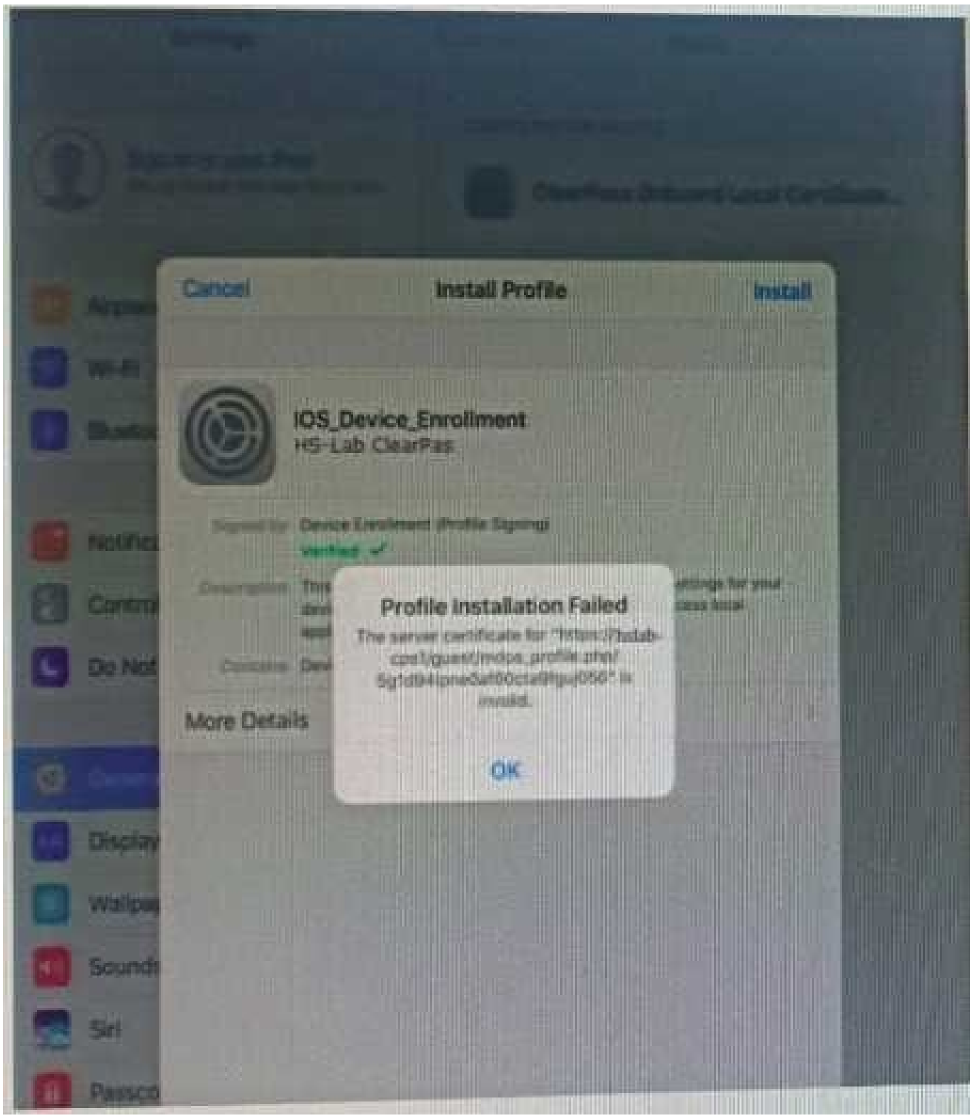
https://www.passapply.com/hpe6-a81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Refer to the exhibit:



Profile Installation Failed

The server certificate for "https://hslab-cps1/guest/mdps_profile.php/5g1d94lpne0af00cta9lgu0i56" is invalid.

A customer has configured Onboard and Windows devices work as expected but cannot get the Apple iOS devices to Onboard successfully. Where would you look to troubleshoot the Issued (Select two)

A. Check if the ClearPass HTTPS server certificate installed in the server is issued by a trusted commercial certificate authority.

B. Check if the customer installed the internal PKl Root certificate presented by the ClearPass during the provisioning process.

C. Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client.

D. Check if the customer has Instated a custom HTTPS certificate for IDS and another internal PKl HTTPS certificate for other devices.

E. Check if the customer has installed the same internal PKl signed RADIUS server certificate as the HTTPS server certificate.

Correct Answer: AC

QUESTION 2

A customer has a ClearPass cluster deployment with four servers, two servers at the data center and two servers at a large remote site connected over an SD-WAN solution The customer would like to implement OnGuard, Guest Self-Registration, and 802.1x authentication across their entire environment. During testing the customer is complaining that users connecting to an Instant Cluster Employee SSID at the remote site, with the OnGuard Persistent Agent installed are randomly getting their health check missed. What could be a possible cause of this behavior?

A. The OnGuard Clients are automatically mapped to the Policy Manager Zone based on their IP range but an ACL on the switch could be blocking access.

B. The traffic on the TCP port 6658 is congested due to the fact that this port is also used by the IPsec keep-alive packets of the SD-WAN solution.

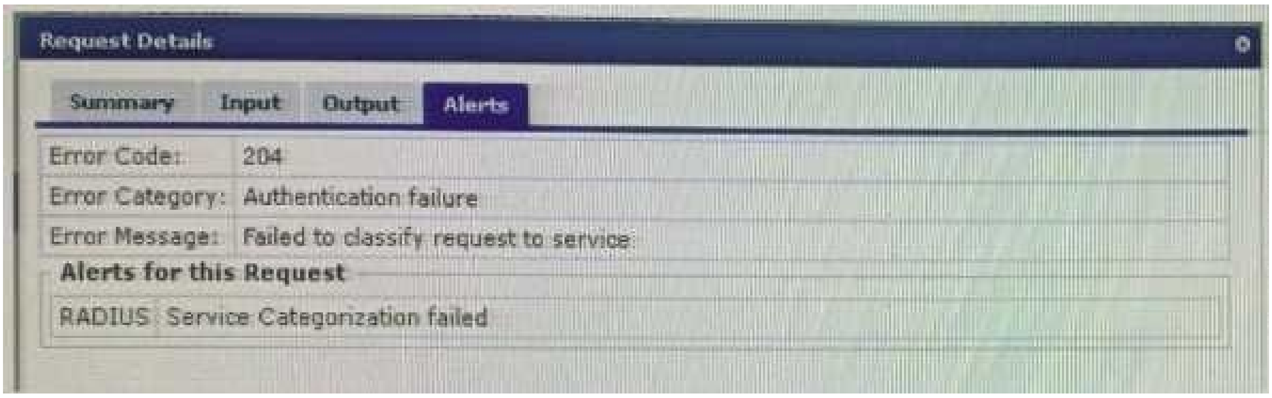
C. The ClearPass Policy Manager zones have been defined but the local IP sub-nets have not been property mapped to the zones and the OnGuard Agent might connect to any of the servers in the cluster.

D. The Aruba-user-role received by the IAP is filtering the TCP port 6658 to the ClearPass servers and after 10 seconds the SSL fallback gets activated and randomly generates the issue.

Correct Answer: D

QUESTION 3

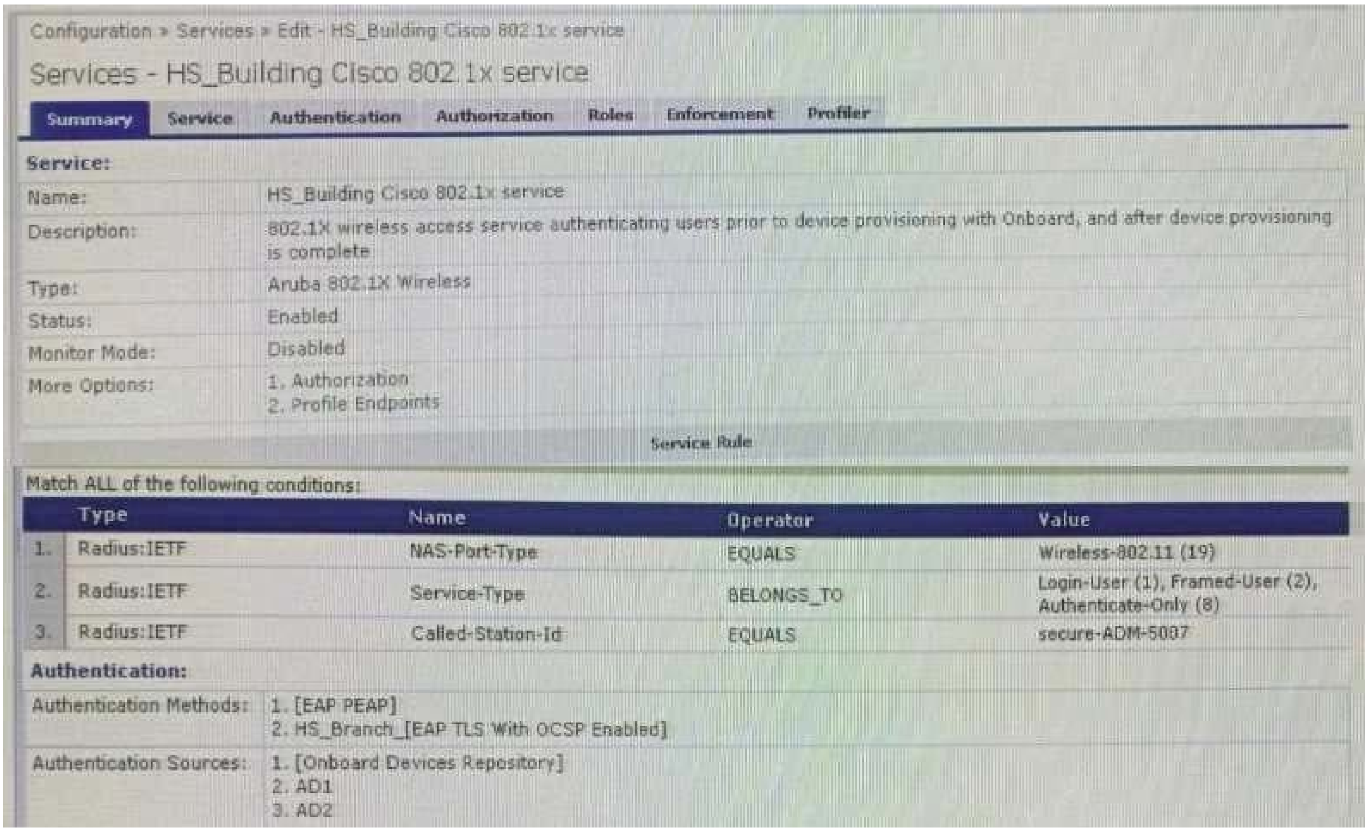
Refer to the exhibit: You configured a new Wireless 802.1X service for a Cisco WLC broadcasting the Secure-ADM-5007 SSID. The client falls to connect to the SSID. Using the screenshots as a reference, how would you fix this issue? (Select two.)



Error Code: 204
Error Category: Authentication failure
Error Message: Failed to classify request to service

Alerts for this Request

RADIUS Service Categorization failed



Configuration » Services » Edit - HS_Building Cisco 802.1x service

Services - HS_Building Cisco 802.1x service

Service:

Name:	HS_Building Cisco 802.1x service
Description:	802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	1. Authorization 2. Profile Endpoints

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:IETF	Called-Station-Id	EQUALS	secure-ADM-5007

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. HS_Branch_[EAP TLS With OCSP Enabled]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2

A. Update the service condition Radius:IETF Called-Station-ld CONTAINS secure-adm-5007

B. Make sure that the Network Devices entry for the Cisco WLC has a vendor setting of "Airspace"

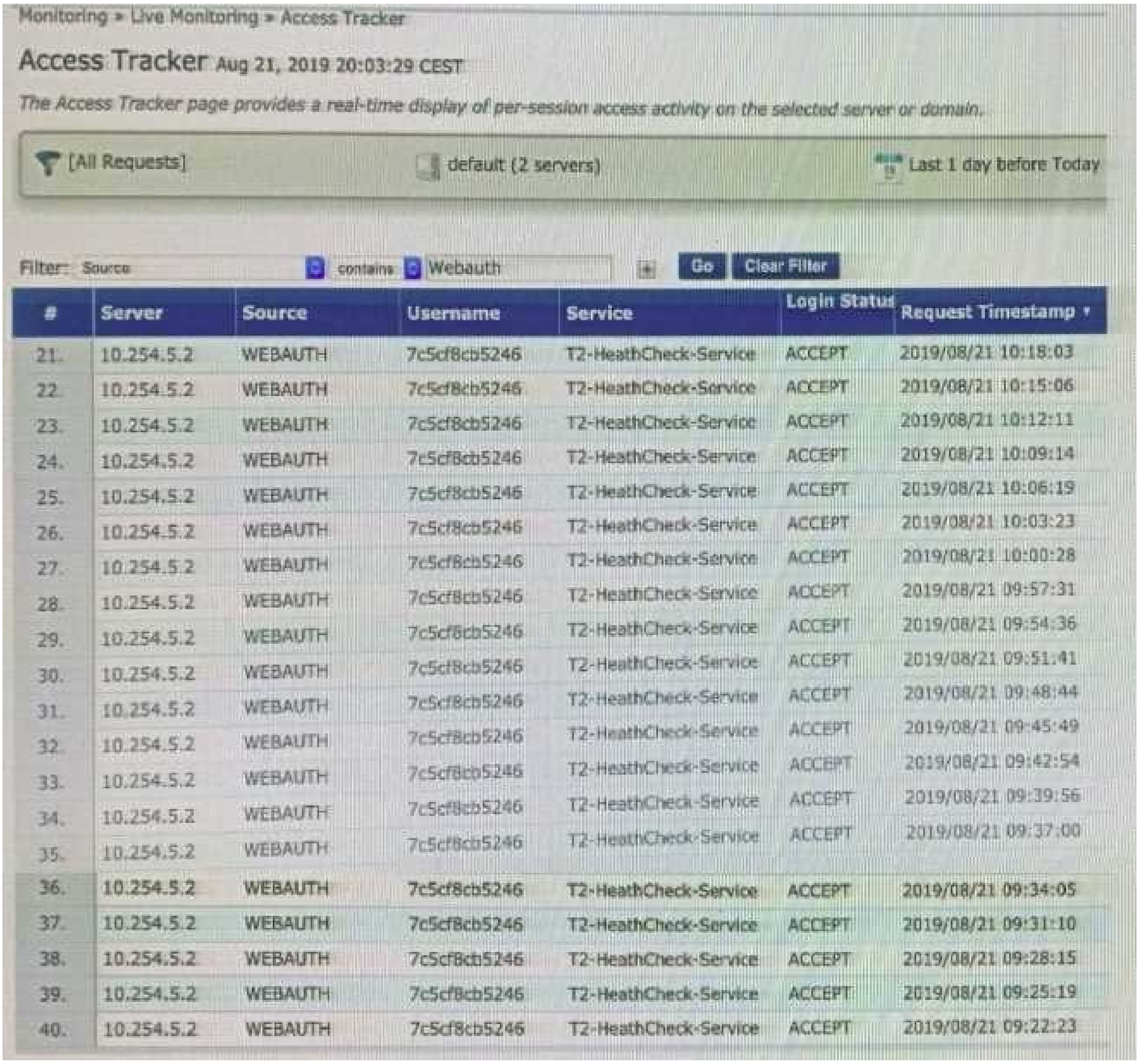
C. Remove the service condition Radius:lETF Service-Type BELONGSJTO Login-User (1). 2. 8

D. Change the service condition to Radius:lETF Calling-Station-ld EQUALS Secure-ADM-5007

Correct Answer: AC

QUESTION 4

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.

Filter: Source contains Webauth

#	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

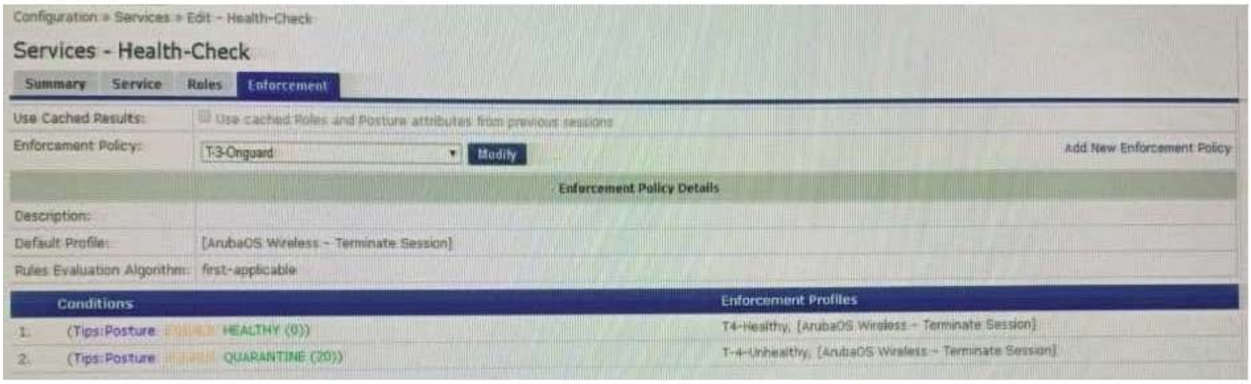
C. TCP port 6658 is not allowed between the client and the ClearPass server

D. The OnGuard Agent is connecting to the Data Port interface on ClearPass

Correct Answer: A

QUESTION 5

Refer to the exhibit:



Configuration » Services » Edit - Health-Check
Summary
Service
Roles
Enforcement
Modify
Add New Enforcement Policy

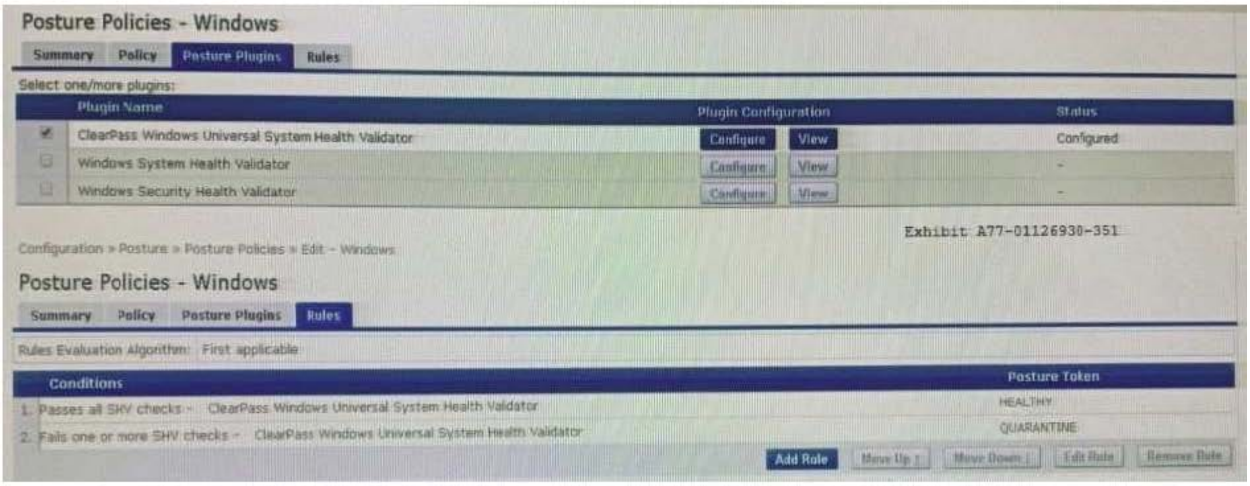
Services - Health-Check

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	T-3-Onguard

Enforcement Policy Details

Description:	
Default Profile:	[ArubaOS Wireless - Terminate Session]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Posture EQUALS HEALTHY (0))	T4-Healthy, [ArubaOS Wireless - Terminate Session]
2.	(Tips:Posture EQUALS QUARANTINE (20))	T-4-Unhealthy, [ArubaOS Wireless - Terminate Session]



Posture Policies - Windows

Select one/more plugins:

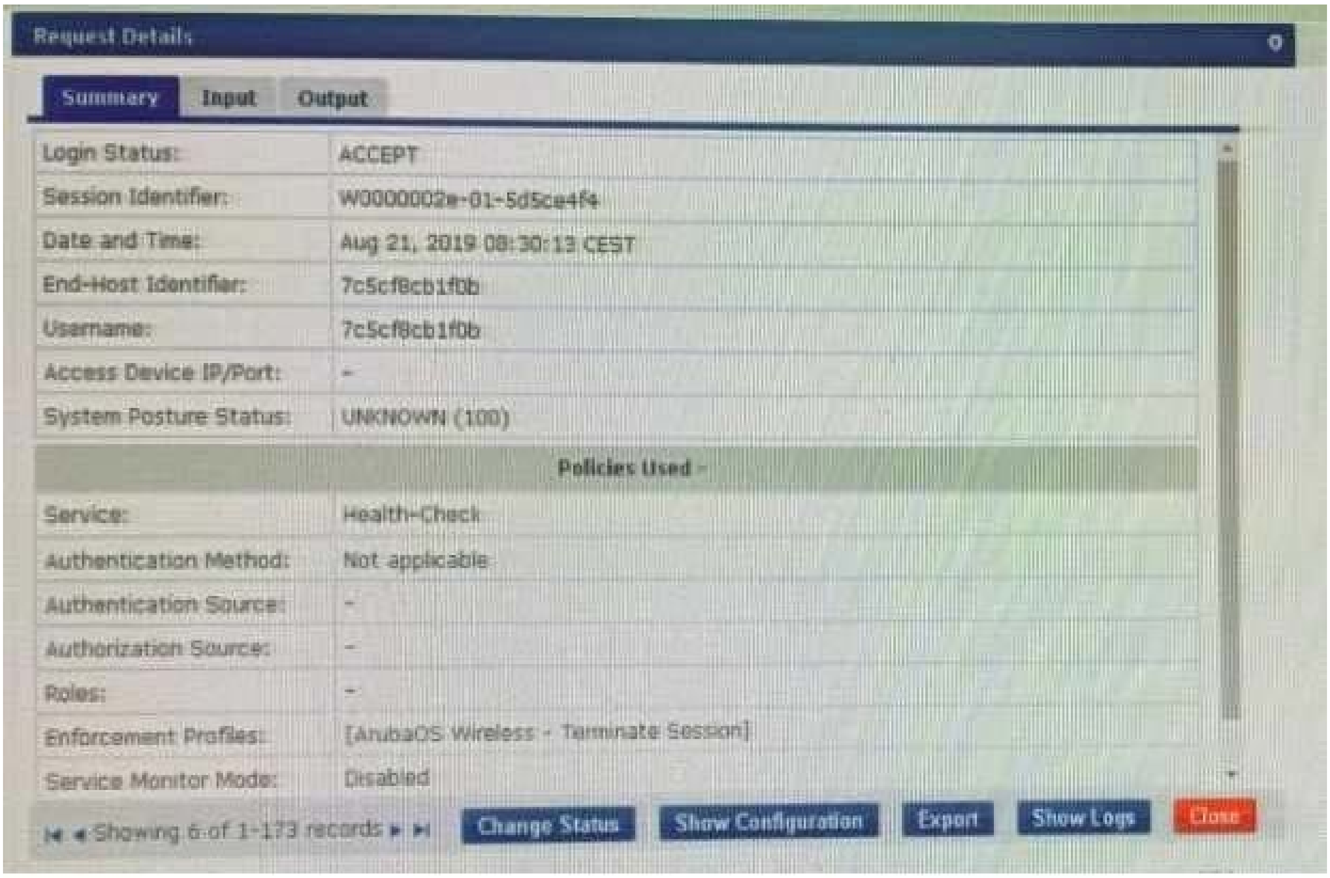
	Plugin Name	Plugin Configuration	Status
☑	ClearPass Windows Universal System Health Validator	Configure View	Configured
□	Windows System Health Validator	Configure View	-
□	Windows Security Health Validator	Configure View	-

Exhibit A77-01126930-351

Posture Policies - Windows

Rules Evaluation Algorithm: First applicable

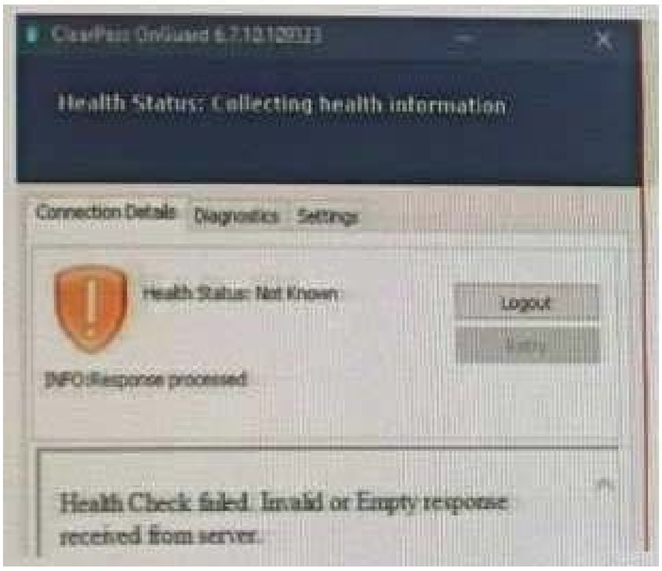
Conditions	Posture Token
1. Passes all SHV checks - ClearPass Windows Universal System Health Validator	HEALTHY
2. Fails one or more SHV checks - ClearPass Windows Universal System Health Validator	QUARANTINE



Request Details

Login Status:	ACCEPT
Session Identifier:	W0000002e-01-5d5ce4f4
Date and Time:	Aug 21, 2019 08:30:13 CEST
End-Host Identifier:	7c5cf8cb1f0b
Username:	7c5cf8cb1f0b
Access Device IP/Port:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Health-Check
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	-
Enforcement Profiles:	[ArubaOS Wireless - Terminate Session]
Service Monitor Mode:	Disabled

Showing 6 of 1-173 records



ClearPass OnGuard 6.7.12.120323

Health Status: Collecting health information

Health Status: Not Known

INFO:Response processed

Health Check failed. Invalid or Empty response received from server.

What could be causing the error message received on the OnGuard client?

A. The Service Selection Rules for the service are not configured correctly

B. The Web-Based Health Check service needs to be configured to use the Posture Policy

C. There is a firewall policy not allowing the OnGuard Agent to connect to ClearPass

D. The client\\'s OnGuard Agent has not been configured with the correct Policy Manager Zone

Correct Answer: D