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.passapply.com/hpe6-a77.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Where is the following information stored in ClearPass?

1.

Roles and Posture for Connected Clients

2.

System Health for OnGuard

3.

Machine authentication State

4.

CoA session info

5.

Mapping of connected clients to NAS/NAD

A. Multi-Master cache

B. Endpoint database

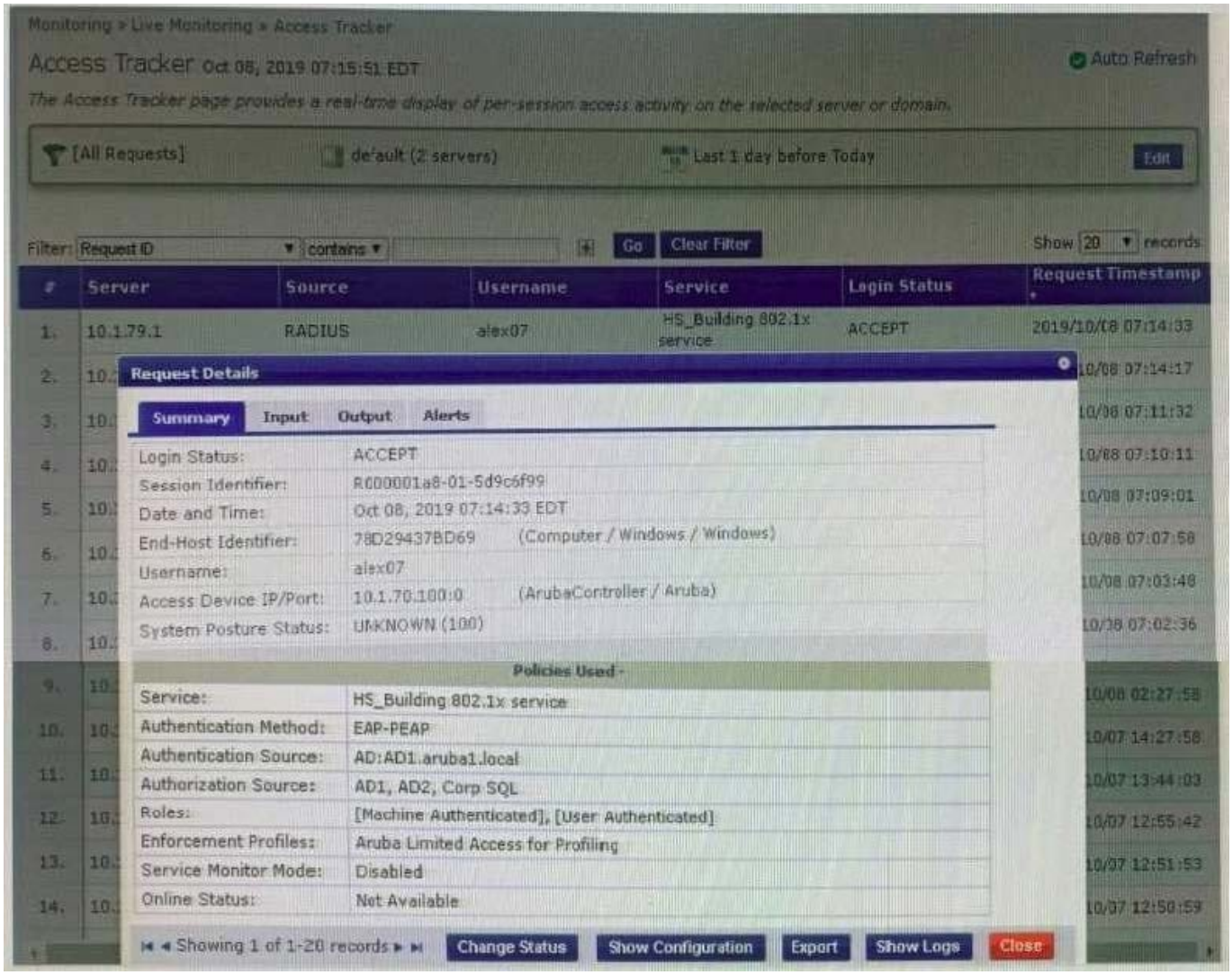
C. insight database

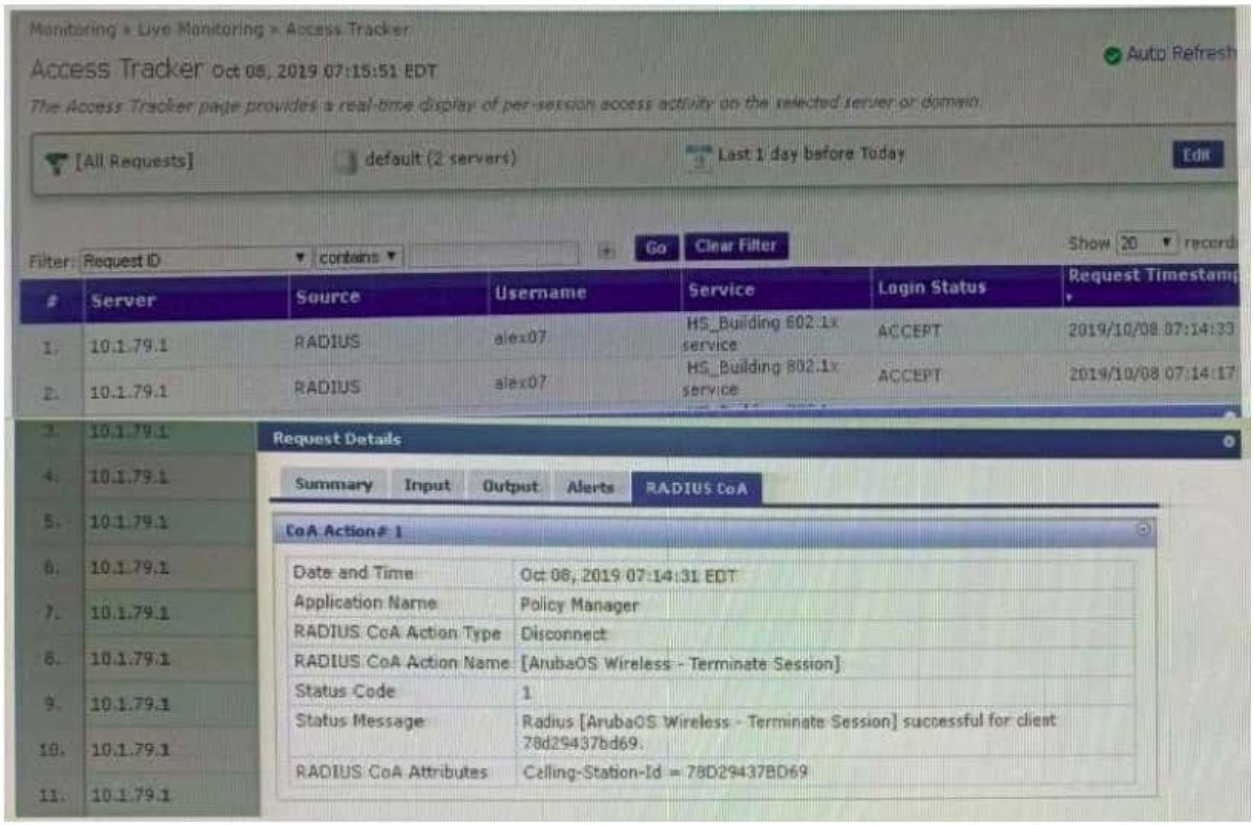
D. ClearPass system cache

Correct Answer: D

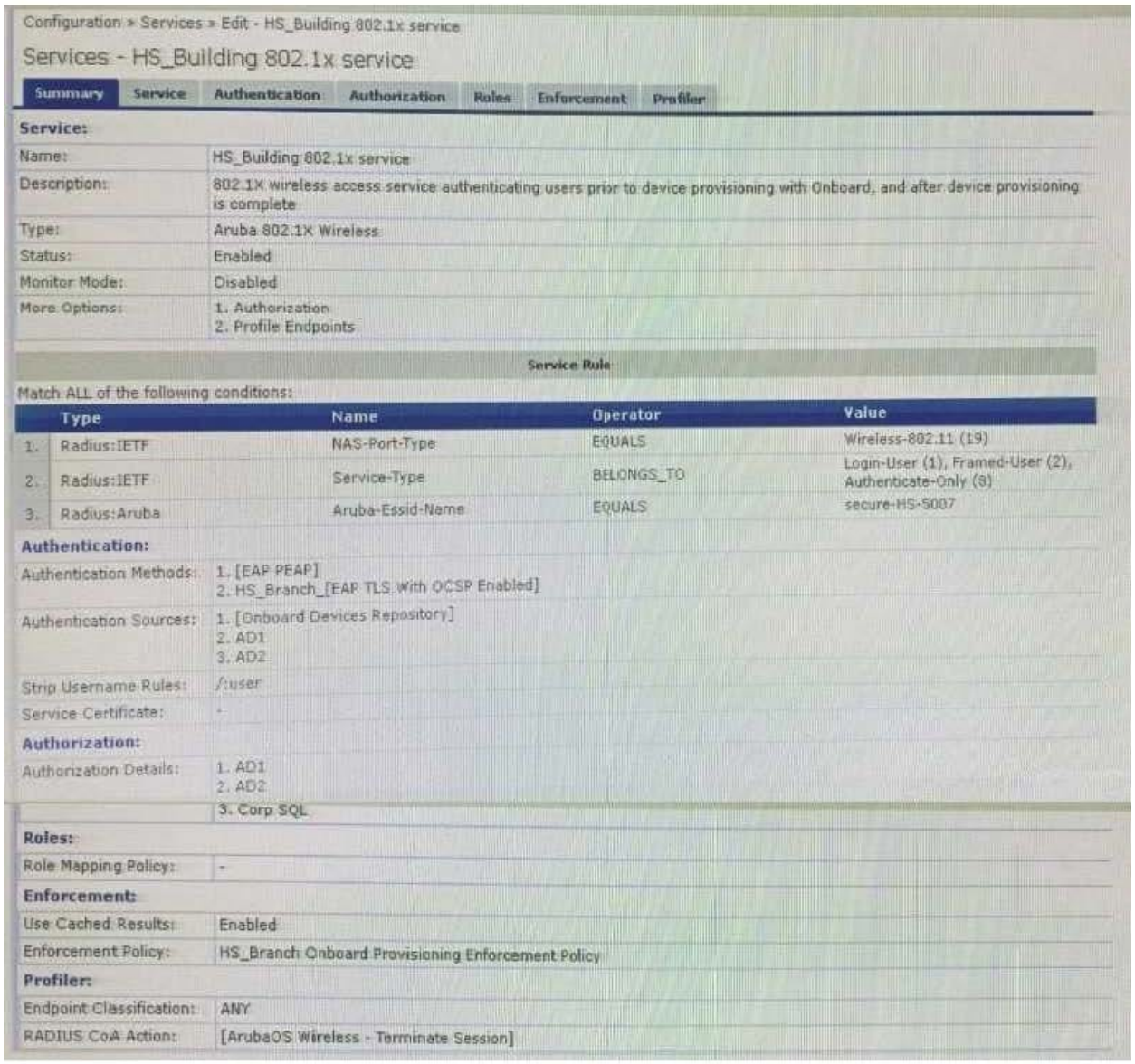
QUESTION 2

Refer to the exhibit:


Monitoring » Live Monitoring » Access Tracker
Access Tracker Oct 08, 2019 07:15:51 EDT
Auto Refresh
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
Edit
Filter: Request ID contains Go Clear Filter
Show 20 records
Server Source Username Service Login Status Request Timestamp
1. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:14:33
2. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:14:17
3. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:11:32
4. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:10:11
5. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:09:01
6. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:07:58
7. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:03:48
8. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:02:36
9. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 02:27:58
10. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/07 14:27:58
11. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/07 13:44:03
12. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/07 12:55:42
13. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/07 12:51:53
14. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/07 12:50:59
Request Details
Summary Input Output Alerts
Login Status: ACCEPT
Session Identifier: R000001a8-01-5d9c6f99
Date and Time: Oct 08, 2019 07:14:33 EDT
End-Host Identifier: 78D29437BD69 (Computer / Windows / Windows)
Username: alex07
Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: HS_Building 802.1x service
Authentication Method: EAP-PEAP
Authentication Source: AD:AD1.aruba1.local
Authorization Source: AD1, AD2, Corp SQL
Roles: [Machine Authenticated], [User Authenticated]
Enforcement Profiles: Aruba Limited Access for Profiling
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Monitoring » Live Monitoring » Access Tracker
Access Tracker Oct 08, 2019 07:15:51 EDT
Auto Refresh
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
Edit
Filter: Request ID contains Go Clear Filter
Show 20 records
Server Source Username Service Login Status Request Timestamp
1. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:14:33
2. 10.1.79.1 RADIUS alex07 HS_Building 802.1x service ACCEPT 2019/10/08 07:14:17
Request Details
Summary Input Output Alerts RADIUS CoA
CoA Action# 1
Date and Time Oct 08, 2019 07:14:31 EDT
Application Name Policy Manager
RADIUS CoA Action Type Disconnect
RADIUS CoA Action Name [ArubaOS Wireless - Terminate Session]
Status Code 1
Status Message Radius [ArubaOS Wireless - Terminate Session] successful for client 78d29437bd69.
RADIUS CoA Attributes Calling-Station-Id = 78D29437BD69


Configuration » Identity » Endpoints
Endpoints
Add
Import
Export All
This page automatically lists all authenticated endpoints. An endpoint device is an Internet-capable hardware device on a TCP/IP network (e.g. laptops, smart phones, tablets, etc.).
Filter: MAC Address contains 78D29437BD69 Go Clear Filter
Show 20 records
MAC Address Hostname Device Category Device OS Family Status Profiled
1. 78d29437bd69 p50-t07-vlt4 Computer Windows Unknown Yes
Showing 1-1 of 1
Authentication Records Bulk Update Bulk Delete Trigger Server Action Update Fingerprint Export Delete



Configuration » Services » Edit - HS_Building 802.1x service

Services - HS_Building 802.1x service

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Service:

Name:	HS_Building 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:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-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
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	1. AD1 2. AD2 3. Corp SQL

Roles:

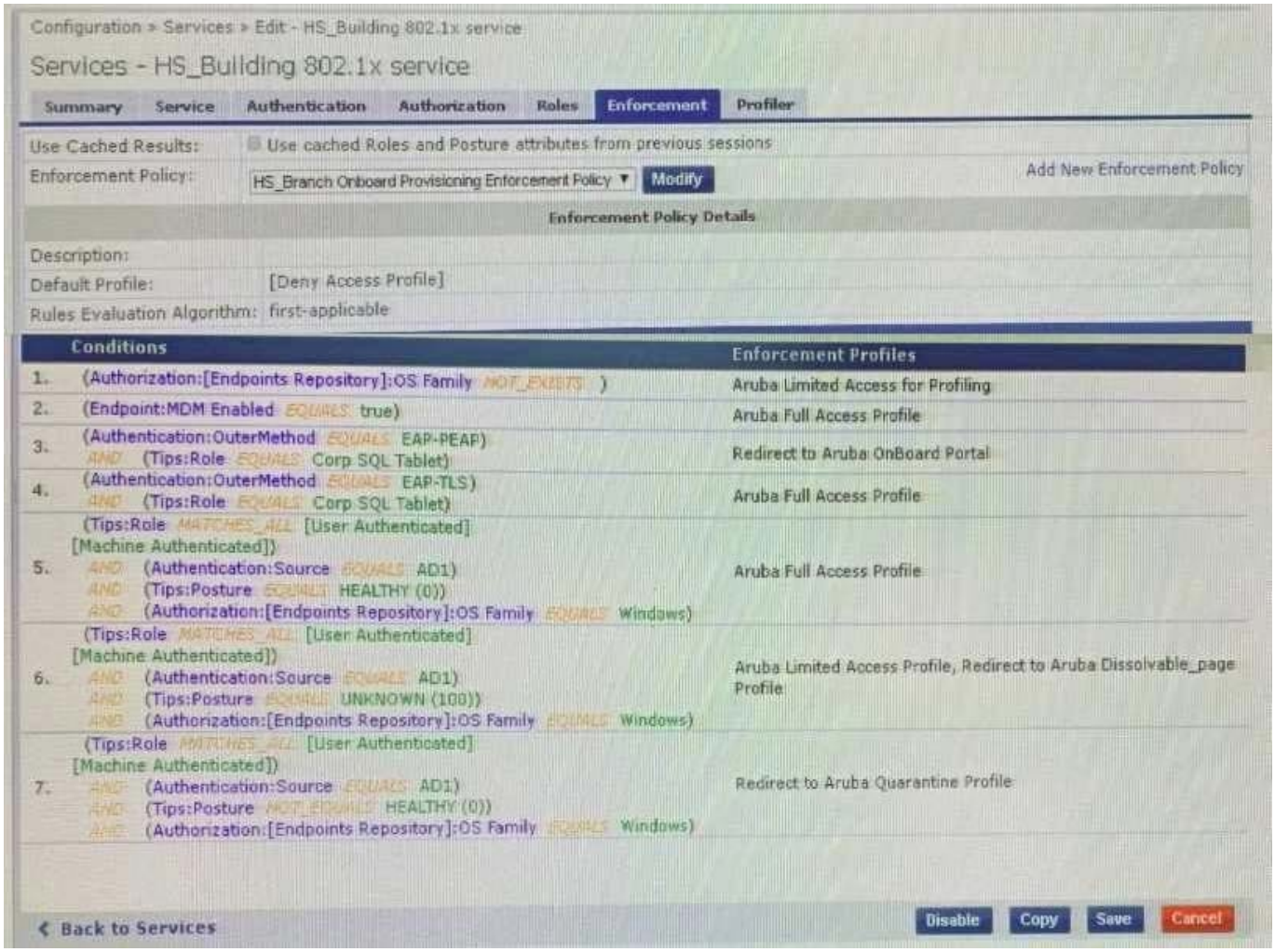
Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Enabled
Enforcement Policy:	HS_Branch Onboard Provisioning Enforcement Policy

Profiler:

Endpoint Classification:	ANY
RADIUS CoA Action:	[ArubaOS Wireless - Terminate Session]



You configured the 802 1 x service enforcement conditions with the Endpoint profiling data. When the client connects to the network. ClearPass successfully profiles the client but the client always receives an incorrect enforcement profile The configurations in the Aruba controller are completed correctly. What is the cause of the issue?

A. An additional authorization source should be configured for profiling to work.

B. The enforcement policy conditions configured with profiling data are not correct.

C. The enforcement policy rules evaluation algorithm Is not configured correctly.

D. The option, use cached roles and posture from previous sessions should be enabled.

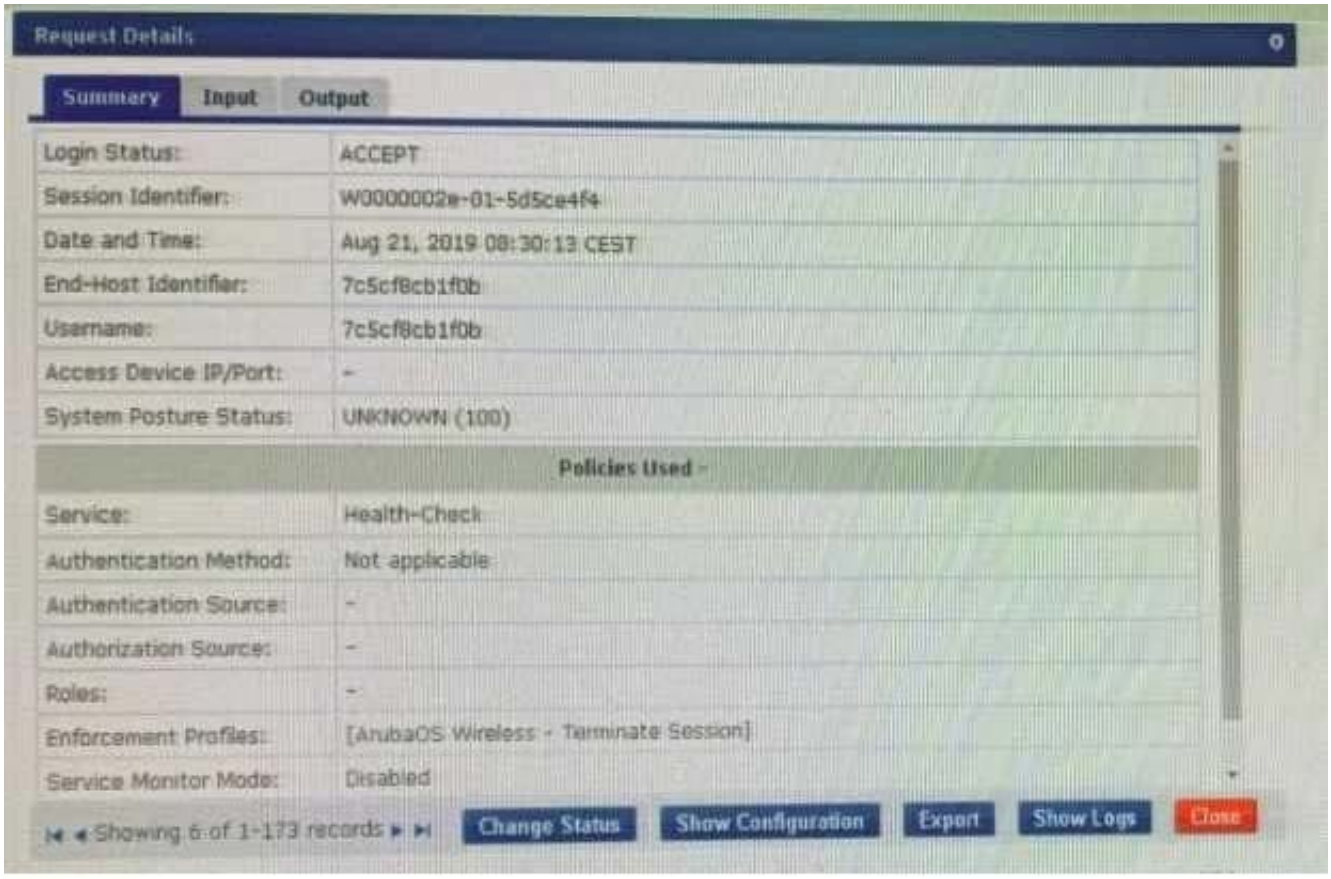
Correct Answer: B

QUESTION 3

Refer to the exhibit:


Configuration » Services » Edit - Health-Check
Services - Health-Check
Summary
Service
Roles
Enforcement
Use Cached Results:
Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:
T-3-Onguard
Modify
Add New Enforcement Policy
Enforcement Policy Details
Description:
Default Profile:
[ArubaOS Wireless - Terminate Session]
Rules Evaluation Algorithm:
first-applicable
Conditions
Enforcement Profiles
1. (Tips:Posture HEALTHY (0))
T4-Healthy, [ArubaOS Wireless - Terminate Session]
2. (Tips:Posture QUARANTINE (20))
T-4-Unhealthy, [ArubaOS Wireless - Terminate Session]


Posture Policies - Windows
Summary
Policy
Posture Plugins
Rules
Select one/more plugins:
Plugin Name
Plugin Configuration
Status
ClearPass Windows Universal System Health Validator
Configure
View
Configured
Windows System Health Validator
Windows Security Health Validator
Exhibit A77-01126930-351
Configuration » Posture » Posture Policies » Edit - Windows
Posture Policies - Windows
Summary
Policy
Posture Plugins
Rules
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
Add Rule
Move Up ↑
Move Down ↓
Edit Rule
Remove Rule



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

QUESTION 4

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 5

What is used to validate the EAP Certificate? (Select three.)

A. Common Name

B. Date

C. Key usage

D. Server Identity

E. SAN entries

F. Trust chain

Correct Answer: ACF