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.pass4itsure.com/hpe6-a77.html

100% Passing Guarantee
100% Money Back Assurance

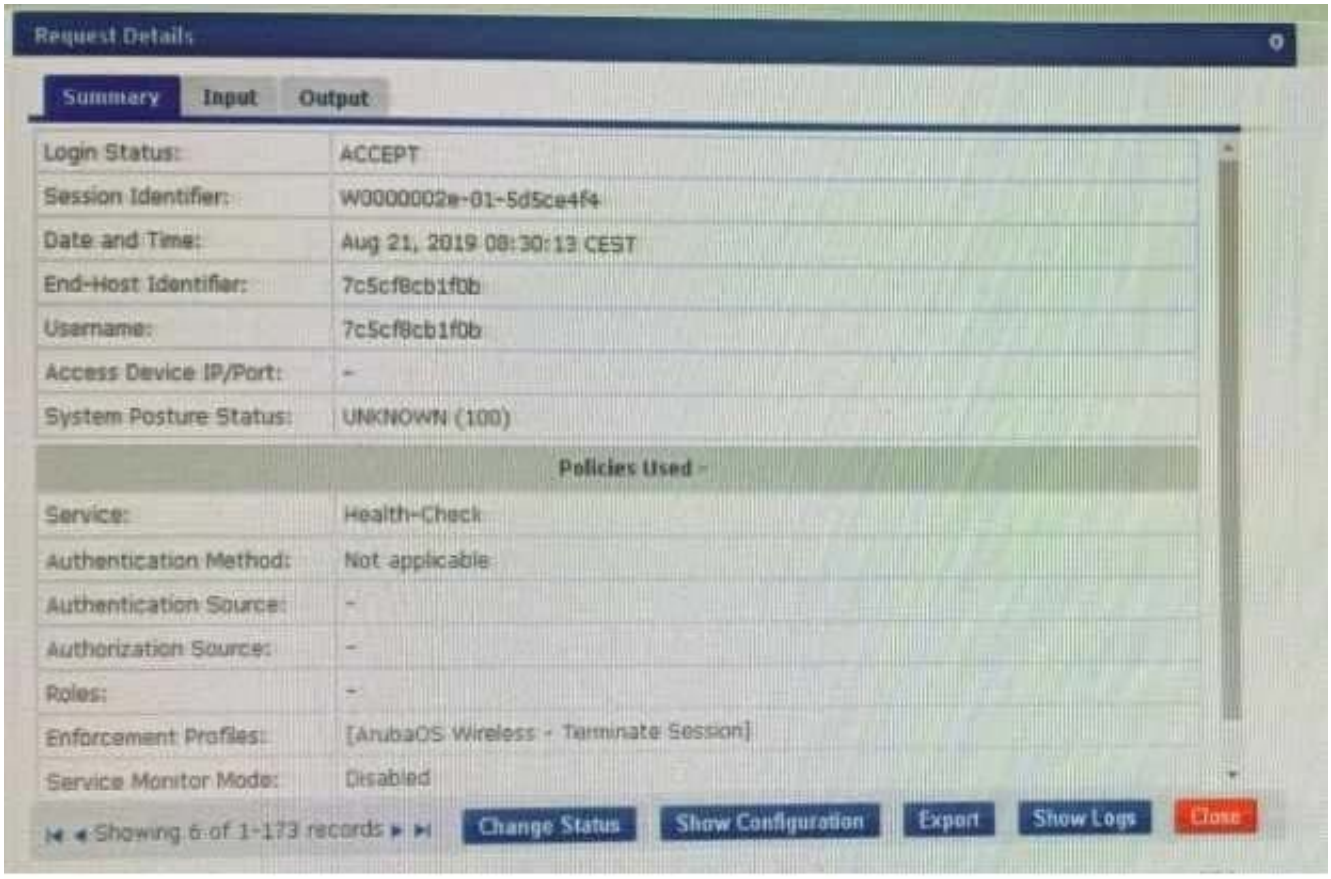
Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

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

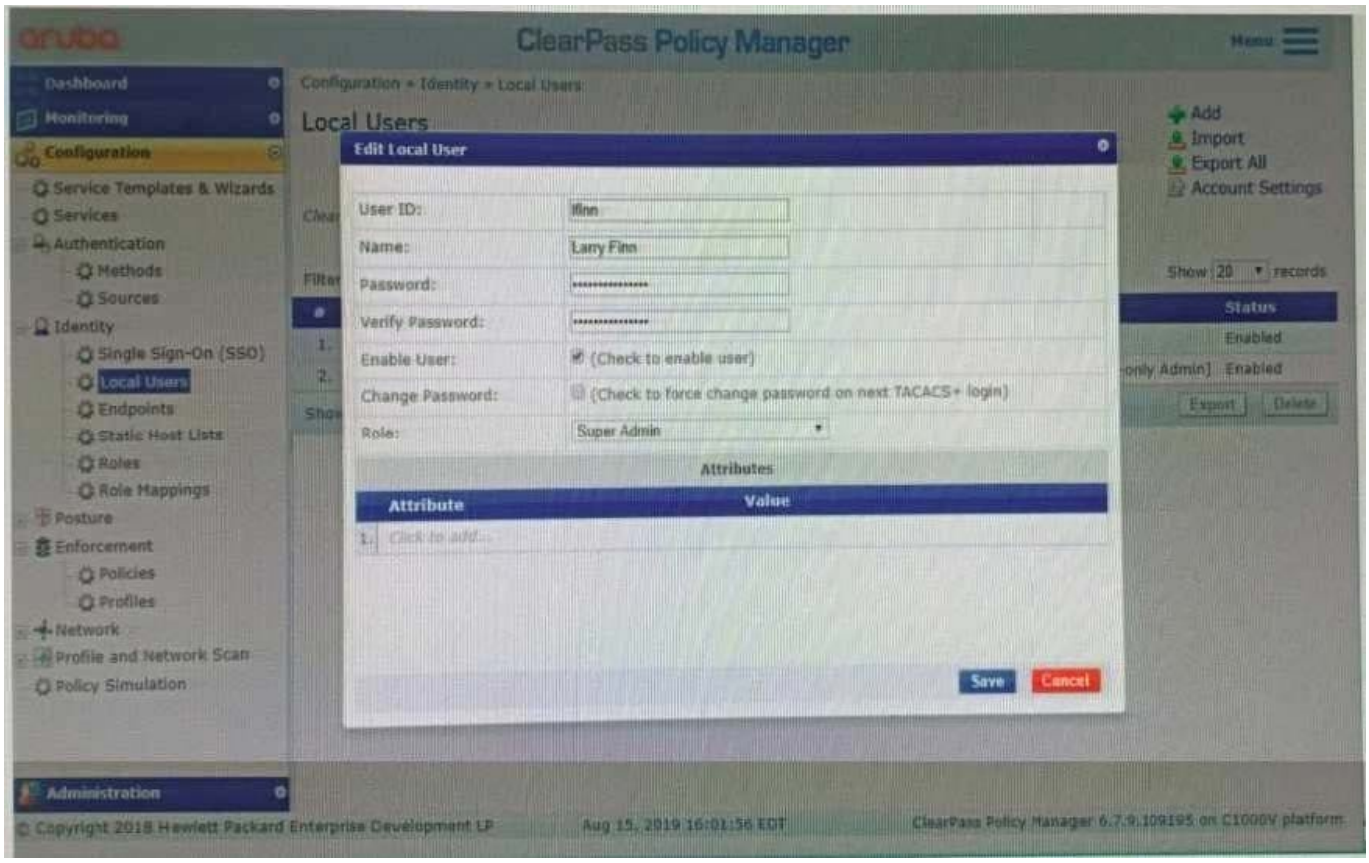
C. There is a firewall policy not allowing the OnGuard Agent to connect to ClearPass

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

Correct Answer: D

QUESTION 2

Refer to the exhibit:



The customer complains that the user shown cannot log into the ClearPass Server as an administrator using the [Policy Manager Admin Network Login Service]. What could be the reason for this?

A. The user might be used for a TACACS authentication

B. The account created does not fit this purpose.

C. The mapping on the role should be changed to [RADIUS Super Admin]

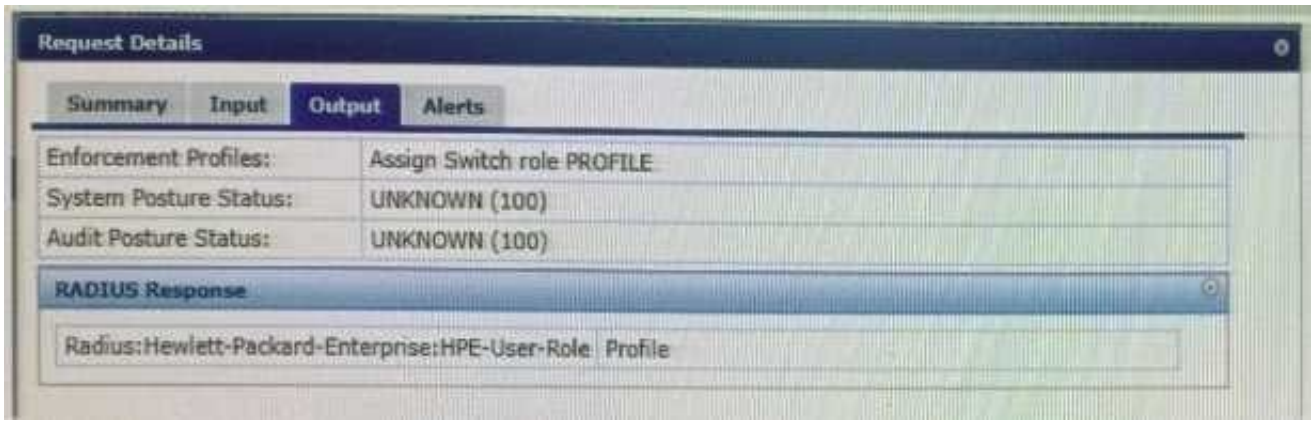
D. The local user authentication might be disabled

Correct Answer: B

QUESTION 3

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Login Status: ACCEPT
Session Identifier: R0000001e-01-5d9ef61c
Date and Time: Oct 10, 2019 05:13:00 EDT
End-Host Identifier: 20-4c-03-5b-4a-d2
Username: 204c035b4ad2
Access Device IP/Port: 10.1.70.5:3 (HPE Aruba switch / Hewlett-Packard-Enterprise)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: HPE-Aruba Wired Mac auth
Authentication Method: MAC-AUTH
Authentication Source: None
Authorization Source: [Endpoints Repository]
Roles: [User Authenticated]
Enforcement Profiles: Assign Switch role PROFILE
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
Alerts
Enforcement Profiles: Assign Switch role PROFILE
System Posture Status: UNKNOWN (100)
Audit Posture Status: UNKNOWN (100)
RADIUS Response
Radius:Hewlett-Packard-Enterprise:HPE-User-Role Profile

You have been asked to help a Customer troubleshoot an issue. They have configured an Aruba OS switch (Aruba 2930 with 16.09) to do MAC authentication with profiling using ClearPass as the authentication source. They cannot get it working.

Using the screenshots as a reference, how will you fix the issue?

A. Delete the initial role in the Aruba OS switch to force the device to get the server derived user roles

B. Use a CoA to bounce the switch port to force the port to change to the correct Aruba user role

C. Change the Vendor settings for the Aruba OS switch to "Aruba" so that the enforcement will use the correct VSAs

D. Modify the enforcement profile conditions with Aruba Vendor specific attributes and Aruba-user- roles

E. User-roles are case sensitive, update the correct role with correct case in the enforcement profile

Correct Answer: D

QUESTION 4

A customer has a ClearPass cluster deployment with one Publisher and one Subscriber configured as a Standby Publisher at the Headquarters DataCenter They also have a large remote site that is connected with an Aruba SD Branch solution over a two Mbps Internet connection. The Remote Site has two ClearPass servers acting as Subscribers. The solution implemented for the customer includes OnGuard, Guest Self Registration, and Employee 802. ix authentication. The client is complaining that users connecting to an IAP Clusters Guest SSID located at the Remote Site are experiencing a significant delay in accessing the Guest Captive Portal page. What could be a possible cause of this behavior?

A. The configuration of the captive portal is pointing to a link located on one of the servers in the Headquarters

B. The ClearPass Cluster has no zones defined and the guest captive portal request is being redirected to the Publisher

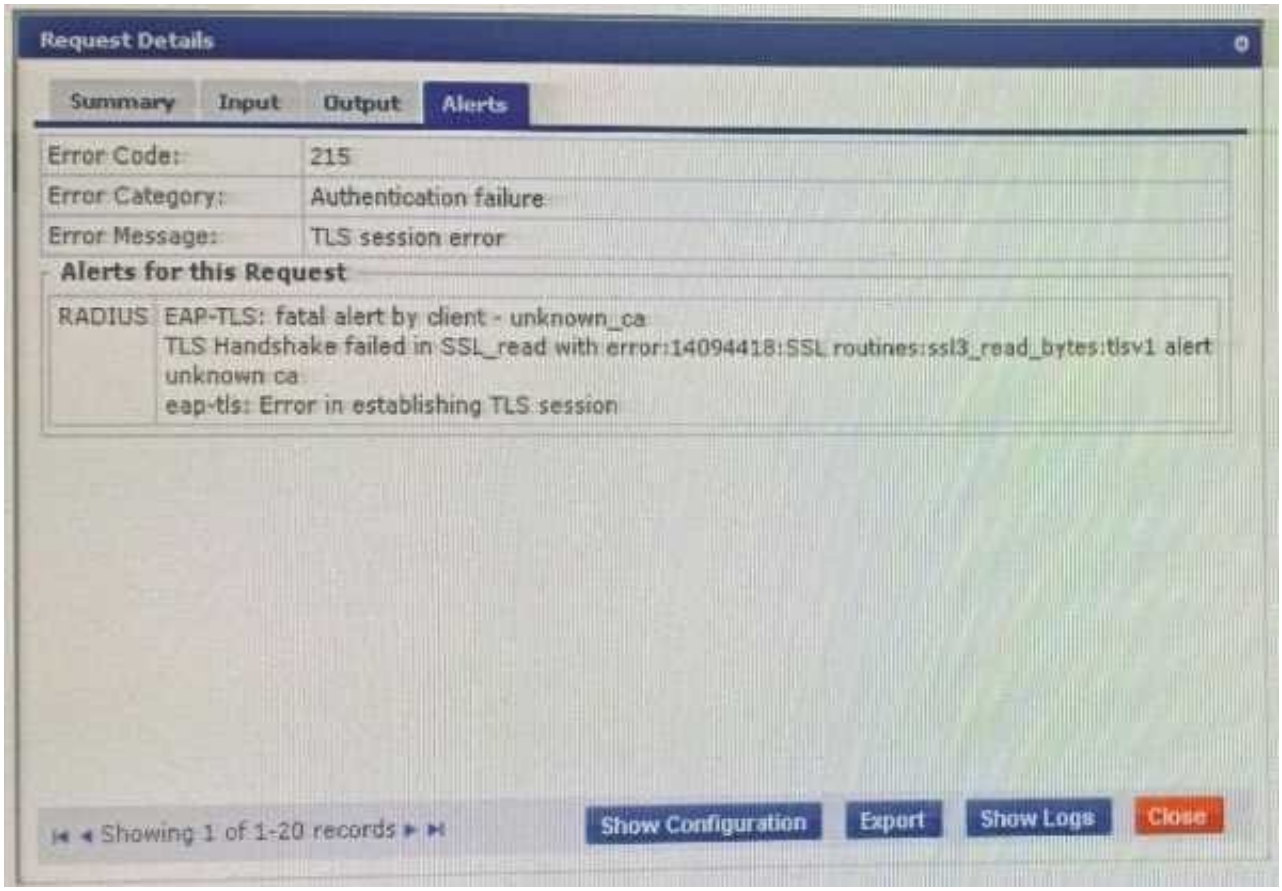
C. The guest page is not optimized to work with the client browser and a proper theme should be applied

D. The captive portal page was only created on the Publisher and requests are getting redirected to a Subscriber

Correct Answer: A

QUESTION 5

Refer to the exhibit:



A customer has configured onboard in a cluster with two nodes All devices were onboarded in the network through node1 but those clients tail to authenticate through node2 with the error shown. What steps would you suggest to make provisioning and authentication work across the entire cluster? (Select three.)

A. Have all of the BYOD clients re-run the Onboard process

B. Configure the Onboard Root CA to trust the Policy Manager EAP certificate root.

C. Have all of the BYOD clients disconnect and reconnect to me network

D. Make sure that the EAP certificates on both nodes are issued by one common root Certificate Authority (CA).

E. Make sure that the HTTPS certificate on both nodes is issued as a Code Signing certificate

F. Configure the Network Settings in Onboard to trust the Policy Manager EAP certificate

Correct Answer: BDF