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

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.

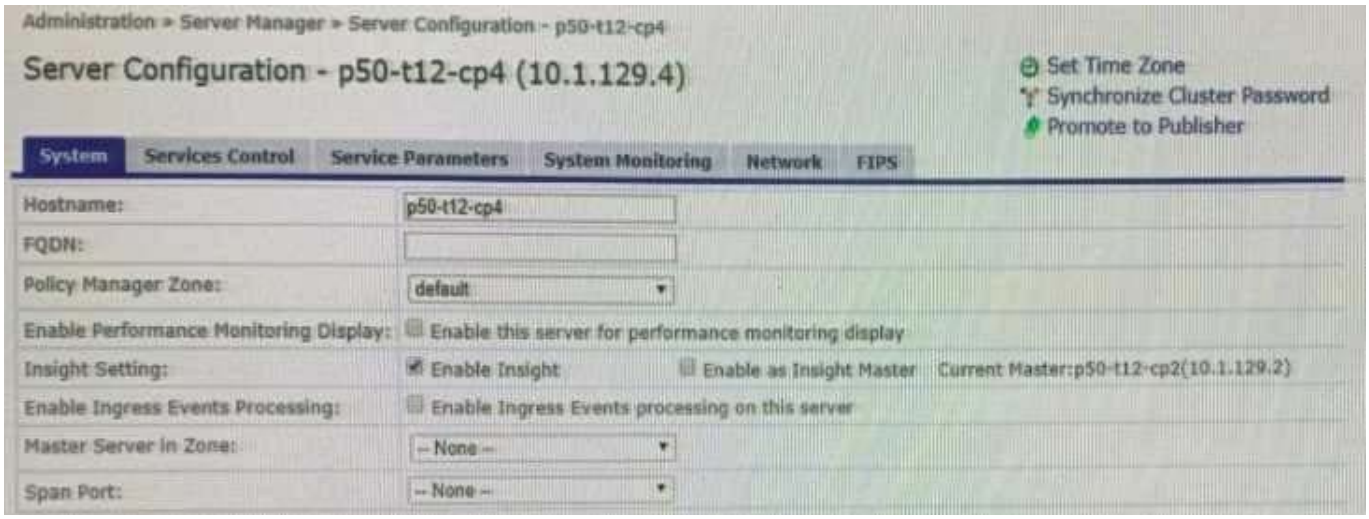
C. The ClearPass Policy Manager zones have been defined but the local IP sub-nets have not been property mapped to the zones and the OnGuard Agent might connect to any of the servers in the cluster.

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 2

Refer to the exhibit:



What is true about the Insight Master Server? {Select two)

A. It Is recommended to have an insight server for every zone to limit the traffic between sites.

B. The Publisher is selected by default as Insight Master Server but It can be changed.

C. There is no need to configure an insight Master Server when using default reports and alerts.

D. An insight Master Server should be selected in order to configure reports and alerts.

E. When enabling a server to be the insight Master any existing insight Master is overwritten.

Correct Answer: BD

QUESTION 3

You have configured a Guest SSID with Captive-portal Web Authentication and MAC authentication The MAC caching expiry time 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 tail 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.

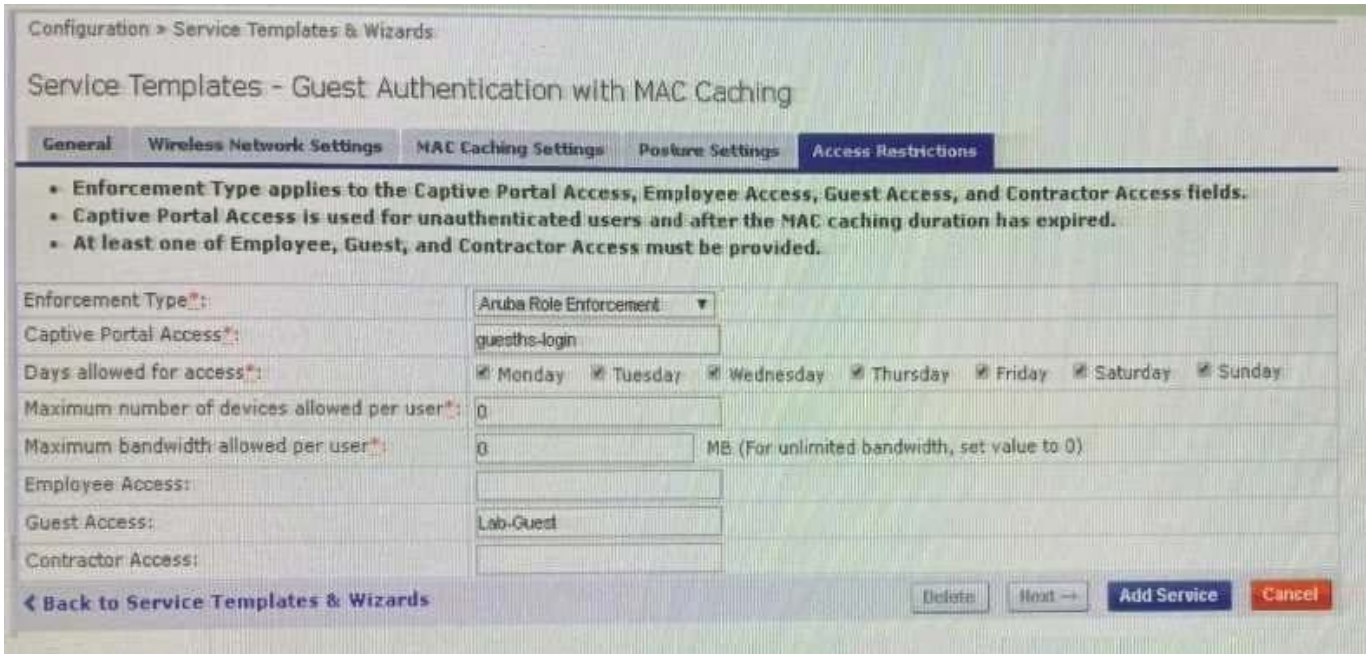
C. The client will successfully pass the MAC authentication but still be redirected to captive portal page.

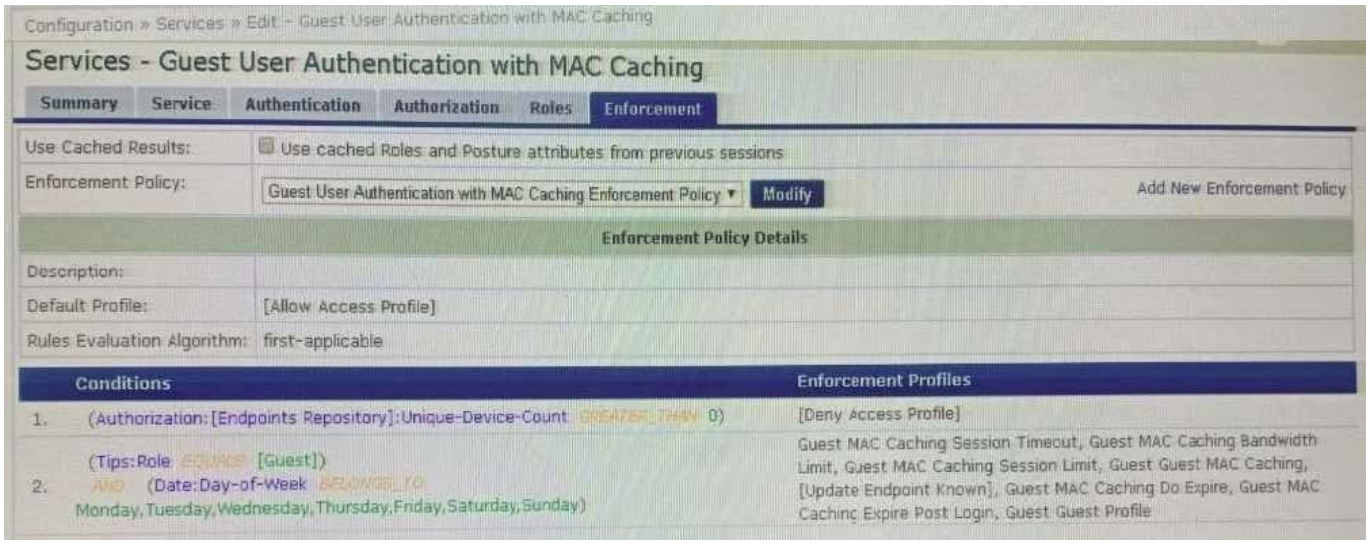
D. The client will fail the MAC authentication and will be redirected to the Captive-portal login page.

Correct Answer: C

QUESTION 4

Refer to the exhibit: You are doing a ClearPass PoC at a customer site with a single Aruba Mobility Controller. The customer asked for a demonstration of a simple Web Login functionality. You used a service template to create the guest services. During testing, the user gets redirected back to the weblogin page with an Authentication failed message. The guest configurations on the Aruba Mobility Controller are configured correctly. Why would the guest fail to authenticate successfully?





A. The authentication source mapped in the service is incorrect, it should be mapped as (Guest Device Repository] [Local SQL DB].

B. The username and/or password used for authentication is incorrect Re-enter the correct password on the weblogin page.

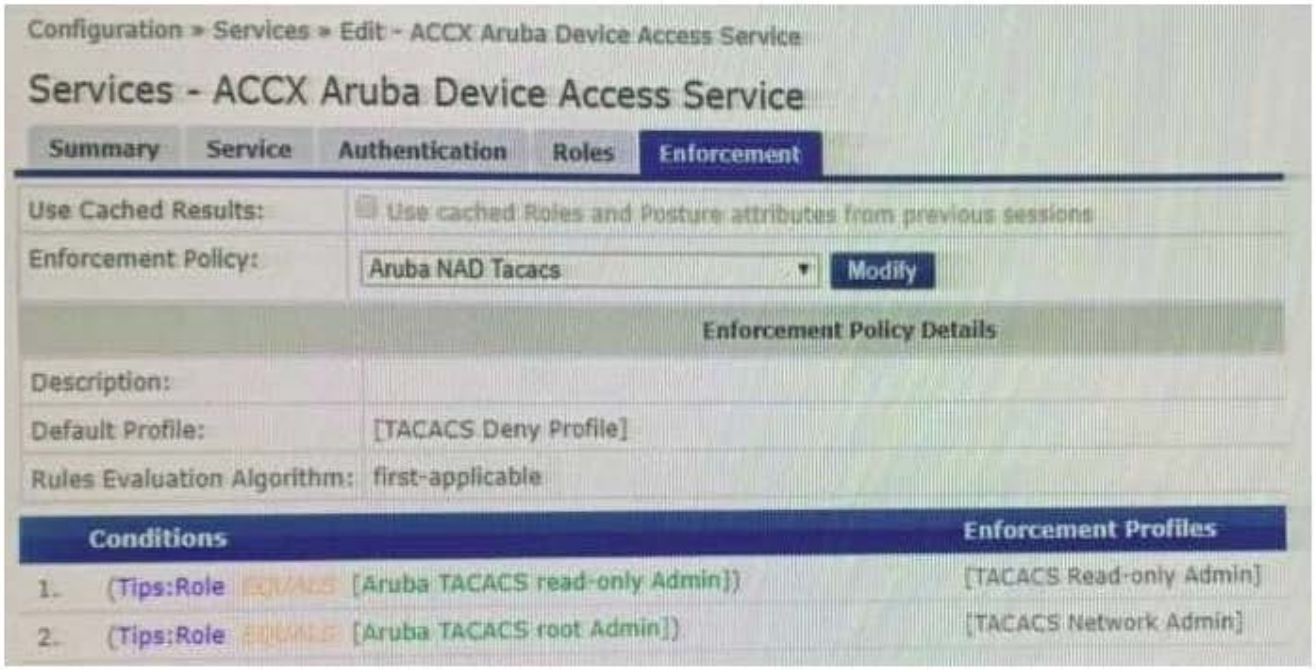
C. The username used for authentication does not exist in the Guest User Database Create a new user and authenticate again.

D. The Unique-Device-Count does not allow any Client devices. Update the Enforcement policy condition: Unique-Device-Count.

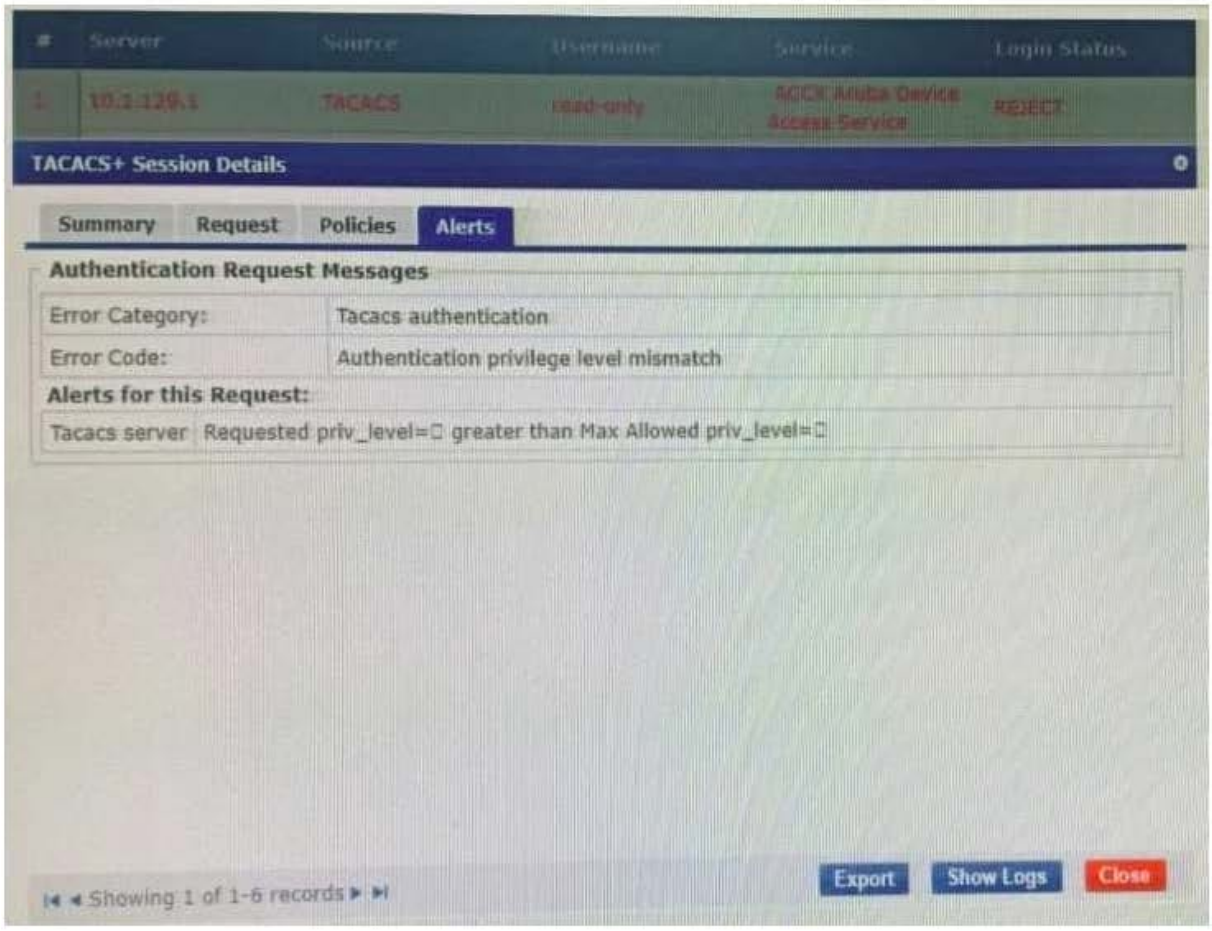
Correct Answer: A

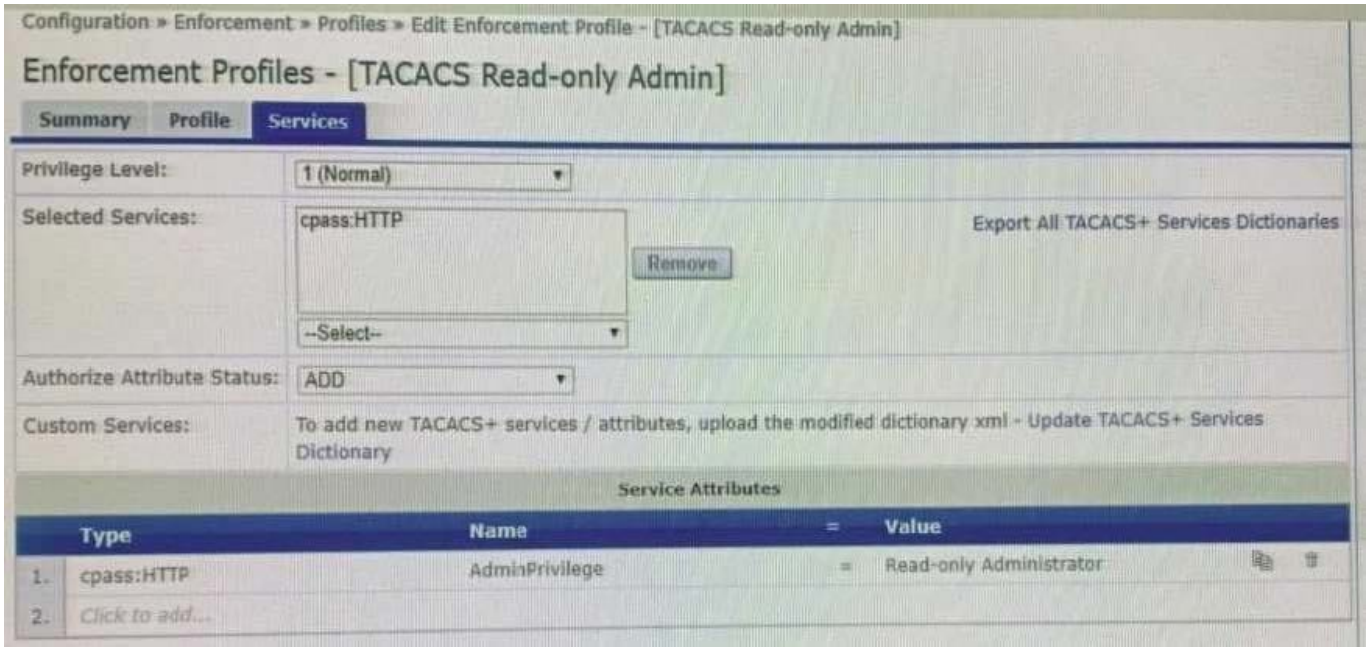
QUESTION 5

Refer to the exhibit:


Configuration » Services » Edit - ACCX Aruba Device Access Service
Services - ACCX Aruba Device Access Service
Summary
Service
Authentication
Roles
Enforcement
Use Cached Results:
Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:
Aruba NAD Tacacs
Modify
Enforcement Policy Details
Description:
Default Profile:
[TACACS Deny Profile]
Rules Evaluation Algorithm:
first-applicable
Conditions
Enforcement Profiles
1. (Tips:Role [Aruba TACACS read-only Admin])
[TACACS Read-only Admin]
2. (Tips:Role [Aruba TACACS root Admin])
[TACACS Network Admin]


Server
Source
Username
Service
Login Status
TACACS
read-only
REJECT
TACACS+ Session Details
Summary
Request
Policies
Alerts
Session ID:
T00000006-01-5d55aba6
Username:
read-only
Time:
Aug 15, 2019 14:59:50 EDT
Status:
AUTHEN_STATUS_FAIL
Authorizations:
0
Showing 1 of 1-6 records
Export
Show Logs
Close


Server
Source
Username
Service
Login Status
TACACS
read-only
REJECT
TACACS+ Session Details
Summary
Request
Policies
Alerts
Authentication Request Messages
Error Category:
Tacacs authentication
Error Code:
Authentication privilege level mismatch
Alerts for this Request:
Tacacs server
Requested priv_level=□ greater than Max Allowed priv_level=□
Showing 1 of 1-6 records
Export
Show Logs
Close



A customer is trying to configure a TACACS Authentication Service for administrative access to the Aruba Controller, During testing the authentication is not successful.

Given the screen shot what could be the reason for the Login status REJECT?

A. The password used by the administrative user, user is wrong.

B. The Enforcement profile is not designed to be used on Aruba Controller.

C. The Read-only Administrator role does not exist on the Controller.

D. The Enforcement profile used is not a TACACS profile.

Correct Answer: A