



HPE6-A81^{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.pass4itsure.com/hpe6-a81.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

Refer to the exhibit:

Administration > Server Manager > Server Configuration - p50-t12-cp4

Server Configuration - p50-t12-cp4 (10.1.129.4)

Set Time Zone
Synchronize Cluster Password
Promote to Publisher

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	p50-t12-cp4				
FQDN:					
Policy Manager Zone:	default				
Enable Performance Monitoring Display:	<input type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input checked="" type="checkbox"/> Enable Insight <input type="checkbox"/> Enable as Insight Master Current Master: p50-t12-cp2(10.1.129.2)				
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server				
Master Server in Zone:	-- None --				
Span Port:	-- None --				

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 2

When is it recommended to use a certificate with multiple entries on the Subject Alternative Name?

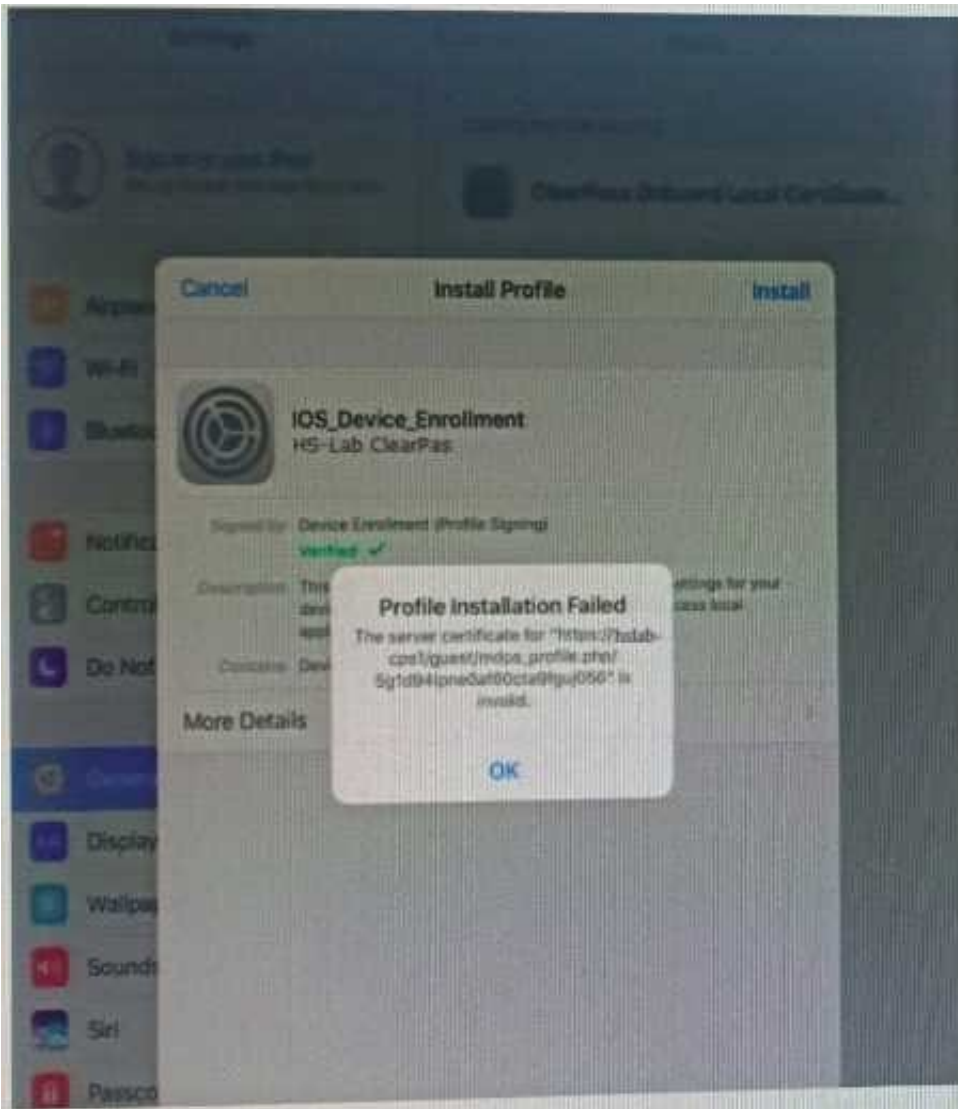
- A. The ClearPass servers are placed in different OnGuard zones to allow the client agent to send SHV updates.
- B. Using the same certificate to onboard clients and the Guest Captive Portal on a single ClearPass server.
- C. The primary authentication server is not available to authenticate the users.
- D. The ClearPass server will be hosting captive portal pages for multiple FQDN entries

Correct Answer: A

QUESTION 3



Refer to the exhibit:



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 PKI 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 PKI HTTPS certificate for other devices.
- E. Check if the customer has installed the same internal PKI signed RADIUS server certificate as the HTTPS server certificate.

Correct Answer: AC



QUESTION 4

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 READONLY [Aruba TACACS read-only Admin])	[TACACS Read-only Admin]
2. (Tips:Role ADMIN [Aruba TACACS root Admin])	[TACACS Network Admin]

#	Server	Source	Username	Service	Login Status
1.	10.1.129.1	TACACS	read-only	ACCX Aruba Device Access Service	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
1	10.2.129.1	TACACS	read-only	AGC/ Aruba Device Access Service	REJECT

TACACS+ Session Details

Summary Request Policies Alerts

Authentication Request Messages

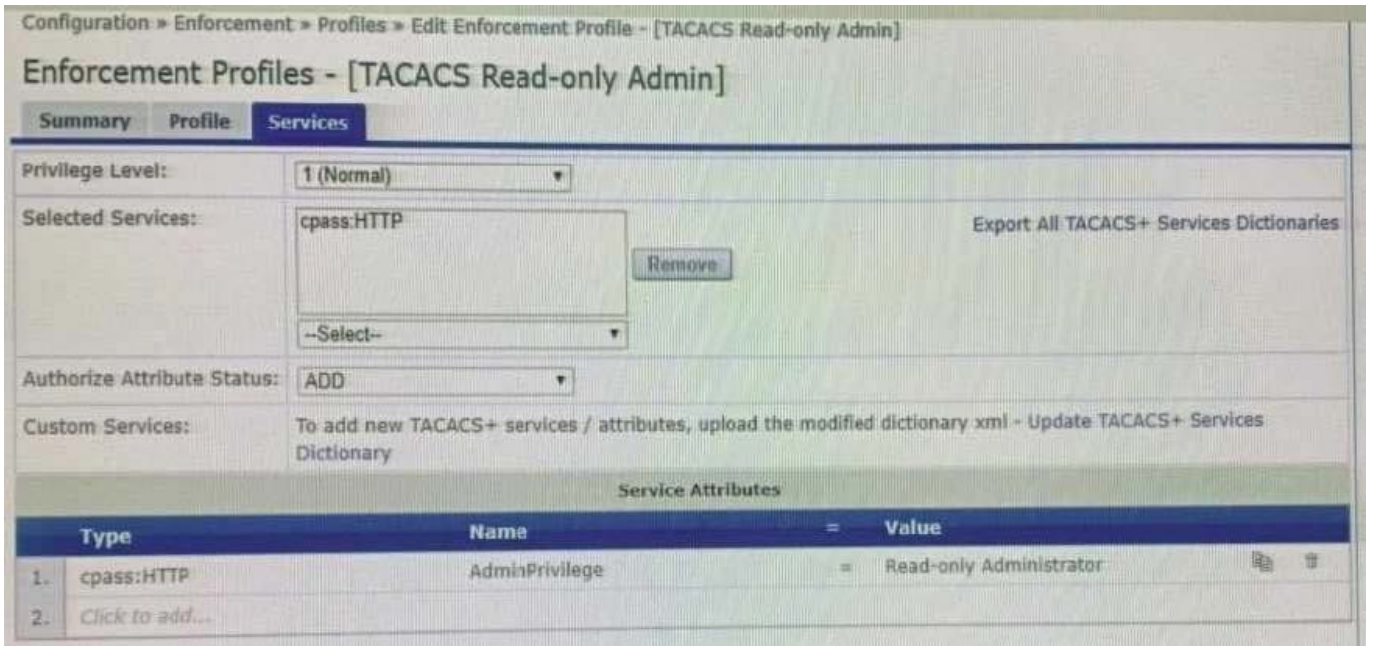
Error Category:	Tacacs authentication
Error Code:	Authentication privilege level mismatch

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.

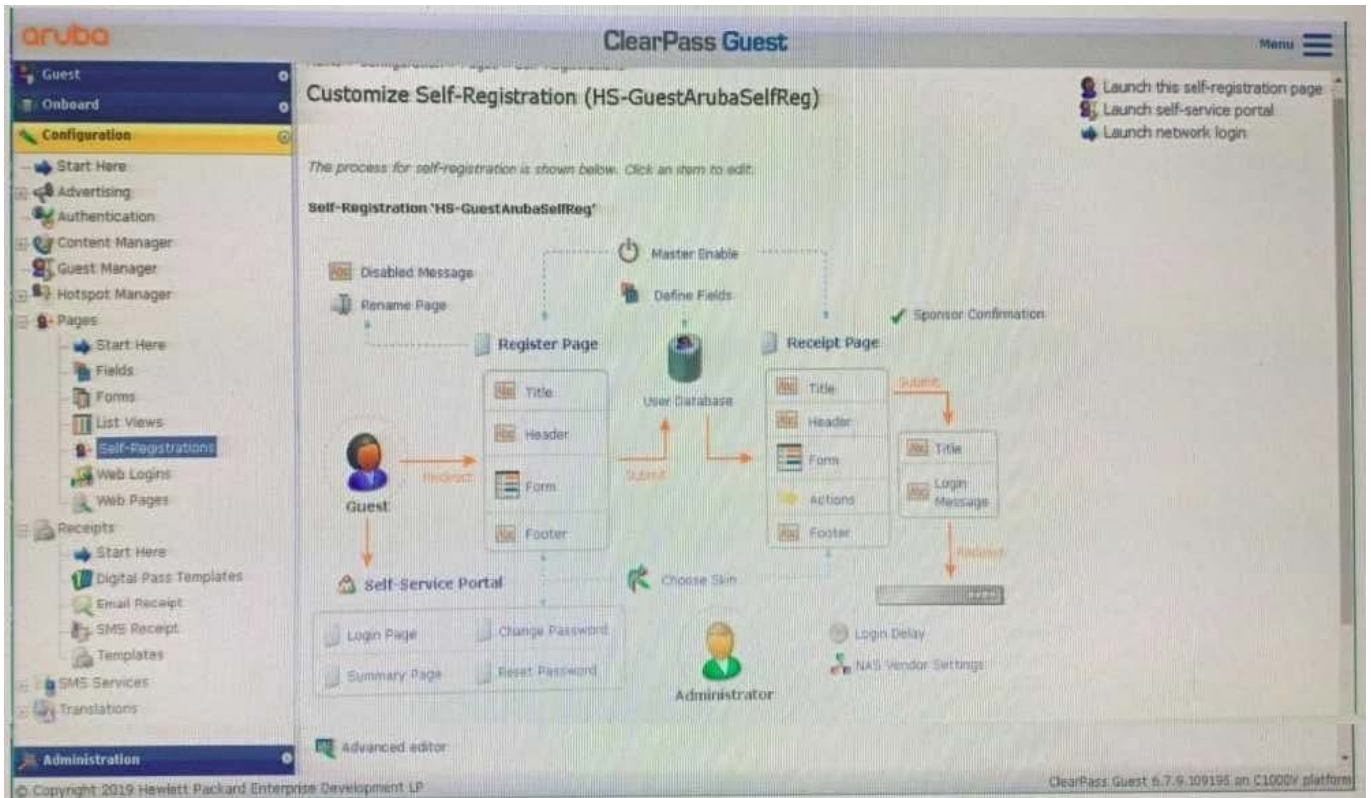
Given the screen shot what could be the reason for the Login status REJECT?

- 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

QUESTION 5

Refer to the exhibit:



A customer is deploying Guest Self-Registration with Sponsor Approval but does not like the format of the sponsor email. Where can you change the sponsor email?

- A. in the Receipt Page - Actions
- B. in the Sponsor Confirmation section
- C. in me Configuration - Receipts - Email Receipts
- D. in the Configuration - Receipts - Templates

Correct Answer: B

[HPE6-A81 PDF Dumps](#)

[HPE6-A81 Practice Test](#)

[HPE6-A81 Study Guide](#)