Vendor:HP

Exam Code:HPE6-A77

Exam Name: Aruba Certified ClearPass Expert Written

Version: Demo

QUESTION 1

There is an Aruba Controller configured to send Guest AAA requests to ClearPass. If the customer would like the most effective way to ensure the lowest license usage counts, how should the controller be configured?

A. Aruba Controller will send stop messages only if EAP termination and Interim accounting are enabled.

B. Aruba Controller will send stop messages if RADIUS Accounting Server Group is defined in the authentication profile.

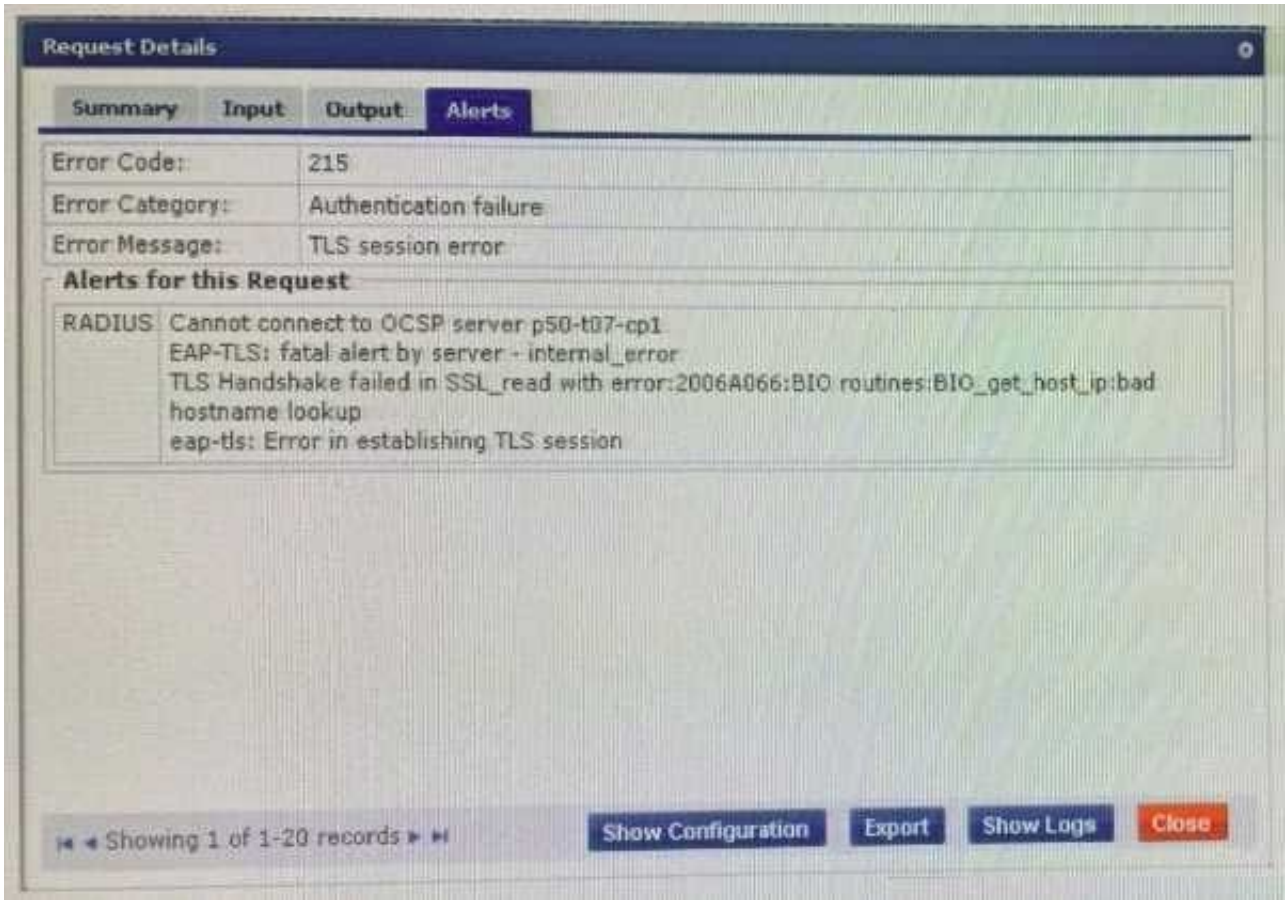
C. Aruba Controller will send stop messages only if both accounting and interim accounting are enabled.

D. Configure EAP Termination on the Aruba Controller and the client will send a stop message.

Correct Answer: D

QUESTION 2

Refer to the exhibit: A customer has configured Onboard in a cluster. After the Primary server\\'s failure, the BYOD devices fail to connect to the network. What would you do to troubleshoot?



A. Verify the OSCP URL under TLS authentication method is mapped to http://localhost/ guestmdps_ocsp.php/2

B. Reboot the active ClearPass server and reconnect the client to the SSID by selecting the correct certificate when

prompted

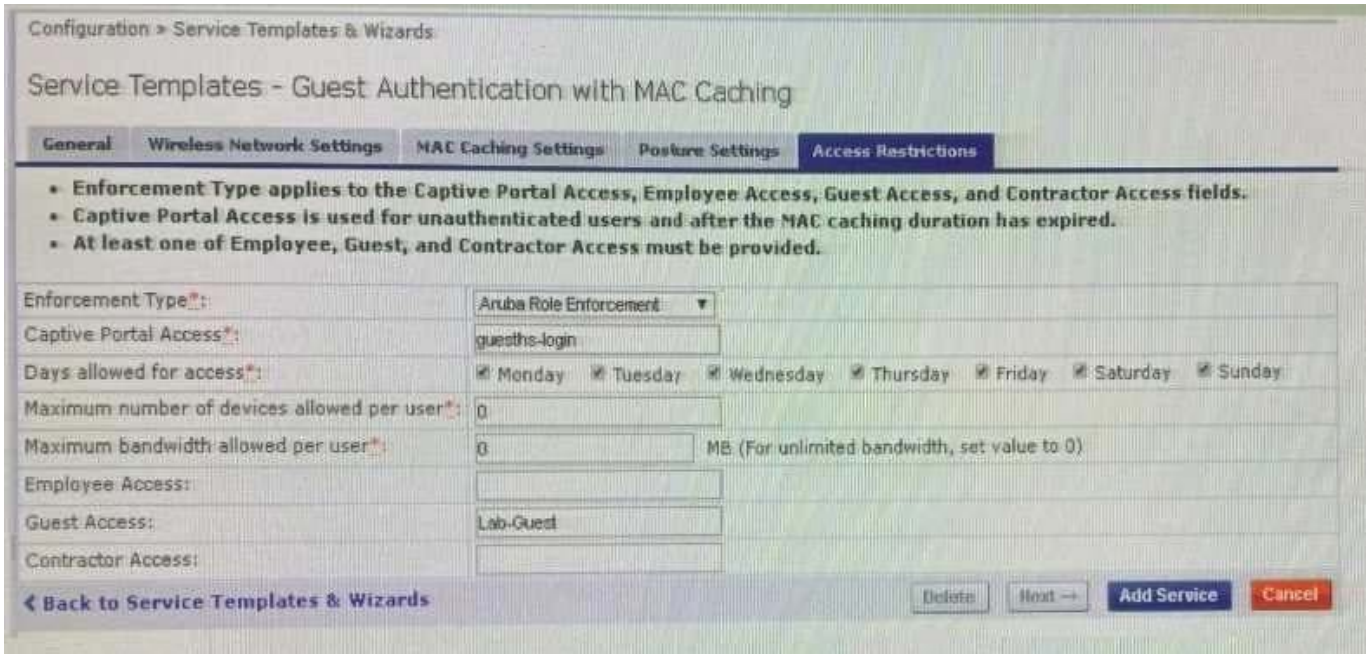
C. Check EAP certificate on the secondary node is issued by the same common root Certificate Authority (CA)

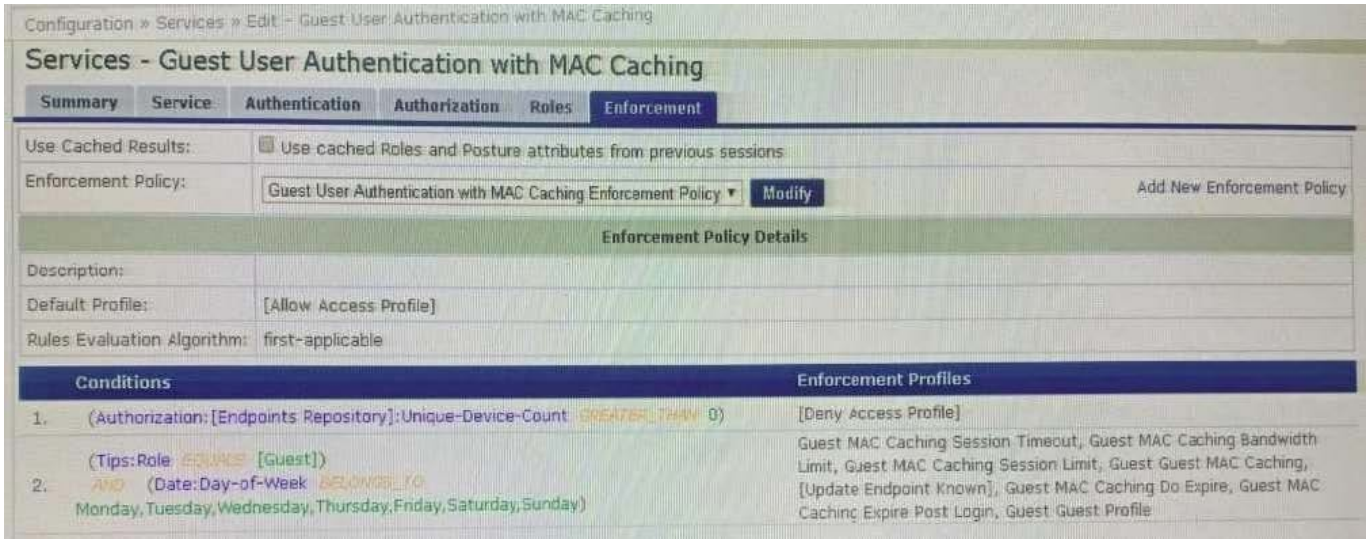
D. Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client

Correct Answer: B

QUESTION 3

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 4

You have recently implemented a serf-registration portal in ClearPass Guest to be used on a Guest SSID broadcast from an Aruba controller. Your customer has started complaining that the users are not able to reliably access the internet after clicking the login button on the receipt page. They tell you that the users will click the login button multiple times and alter about a minute they gain access. What could be causing this issue?

A. The self-registration page is configured with a 1 minute login delay.

B. The guest client is delayed getting an IP address from the DHCP server.

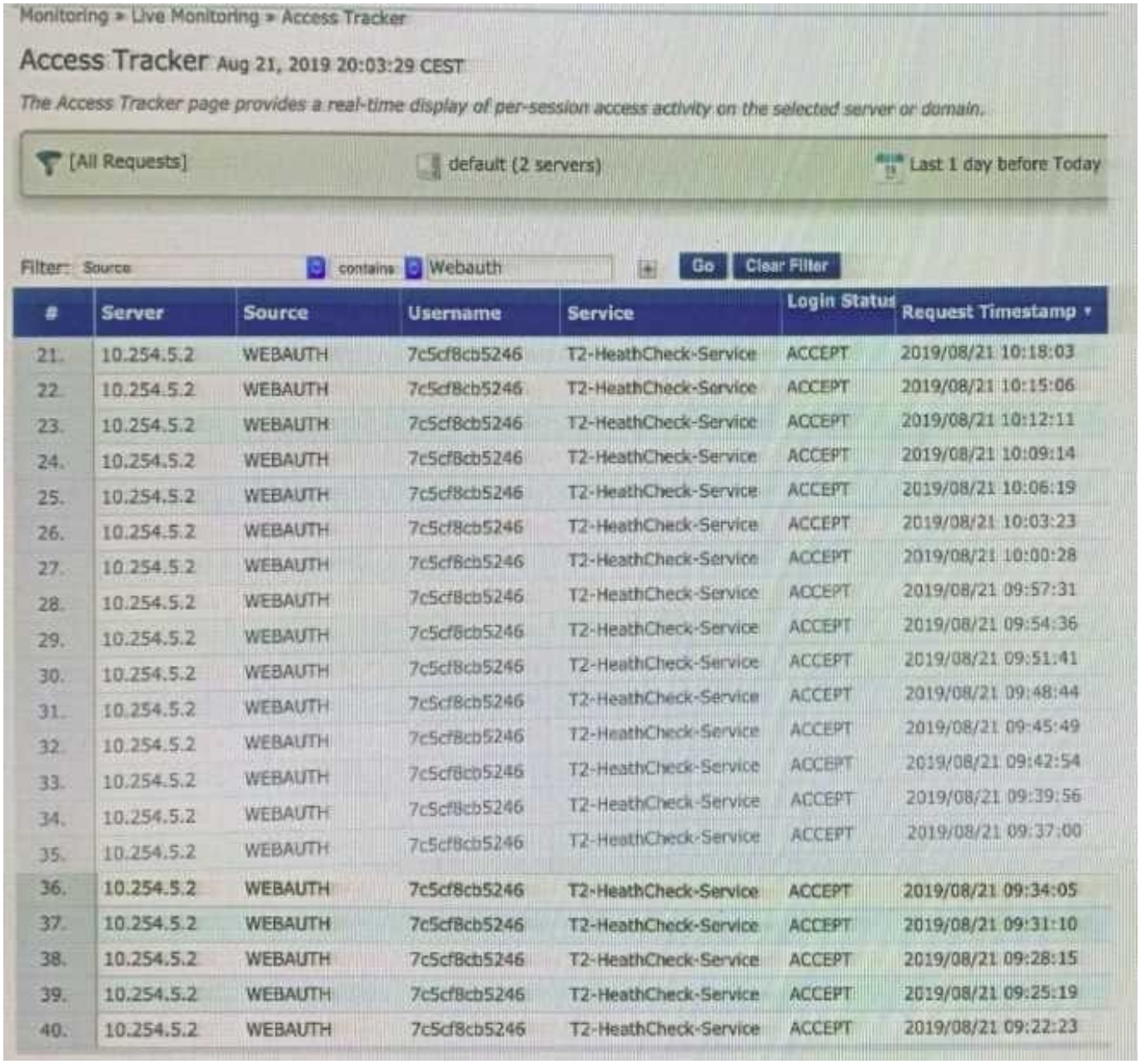
C. The guest users are assigned a firewall user role that has a rate limit.

D. The enforcement profile on ClearPass is set up with an lETF:session delay.

Correct Answer: A

QUESTION 5

Refer to the exhibit:



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

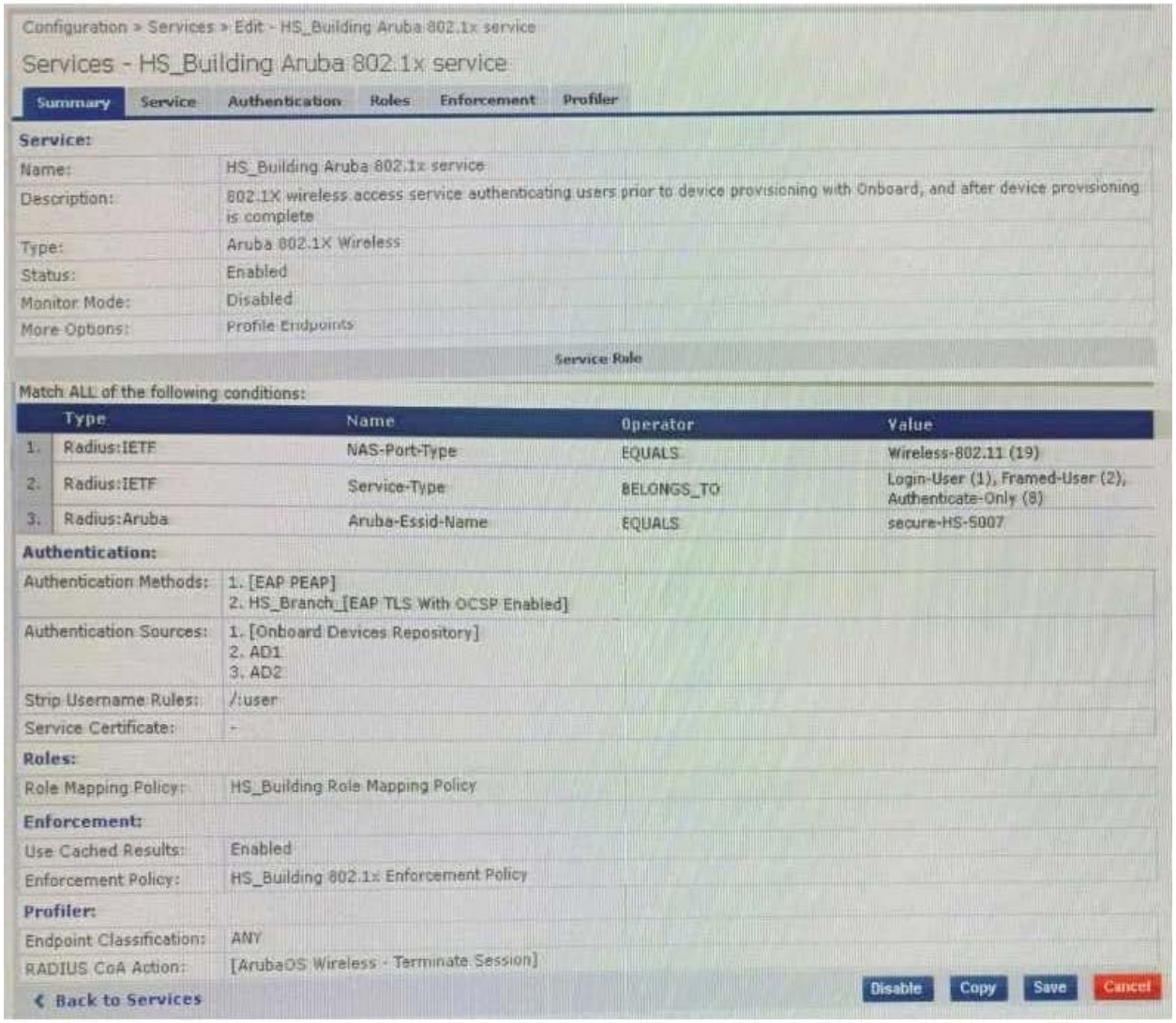
C. TCP port 6658 is not allowed between the client and the ClearPass server

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

Correct Answer: A

QUESTION 6

Refer to the exhibit:



Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Service:

Name:	HS_Building Aruba 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:	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:	-

Roles:

Role Mapping Policy:	HS_Building Role Mapping Policy

Enforcement:

Use Cached Results:	Enabled
Enforcement Policy:	HS_Building 802.1x Enforcement Policy

Profiler:

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

< Back to Services

Disable | Copy | Save | Cancel

Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Role Mapping Policy: HS_Building Role Mapping Policy | Modify | Add New Role Mapping Policy

Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(Connection:Client-Mac-Address BELONGS_TO_GROUP VIP User MAC)	VIP User
2.	(Authorization:Corp SQL:MAC EXISTS)	Corp SQL Tablet
3.	(Authorization:[Endpoints Repository]:Category EQUALS VoIP Phone)	IP Phone
4.	(Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)	Personal SmartDevice
5.	(Authorization:[Endpoints Repository]:Category EQUALS Point of Sale devices)	Vending Machine
6.	(Authorization:[Endpoints Repository]:Category EQUALS Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS CANON INC.)	Printer
7.	(Authorization:[Endpoints Repository]:Category EQUALS Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS Axis Communications AB)	IP Camera

Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: HS_Building 802.1x Enforcement Policy | Modify | Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
2.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
3.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
4.	(Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile
5.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0))	Aruba Full Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100))	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	Redirect to Aruba Quarantine Profile

Your company has a postgres SQL database with the MAC addresses of the company-owned tablets You have configured a role mapping condition to tag the SQL devices. When one of the tablets connects to the network, it does not get the correct role and receives a deny access profile.

How would you resolve the issue?

A. Remove SQL condition from role mapping policy and add it under the enforcement policy conditions.

B. Edit the SQL authentication source niter attributes and modify the SQL server filter query.

C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.

D. Enable authorization tab in the service and add the SQL server as an authorization source.

Correct Answer: B

QUESTION 7

While configuring a guest solution, the customer is requesting that guest user receive access for four hours from their first login. Which Guest Account Expiration would you select?

A. expire_after

B. do_expire

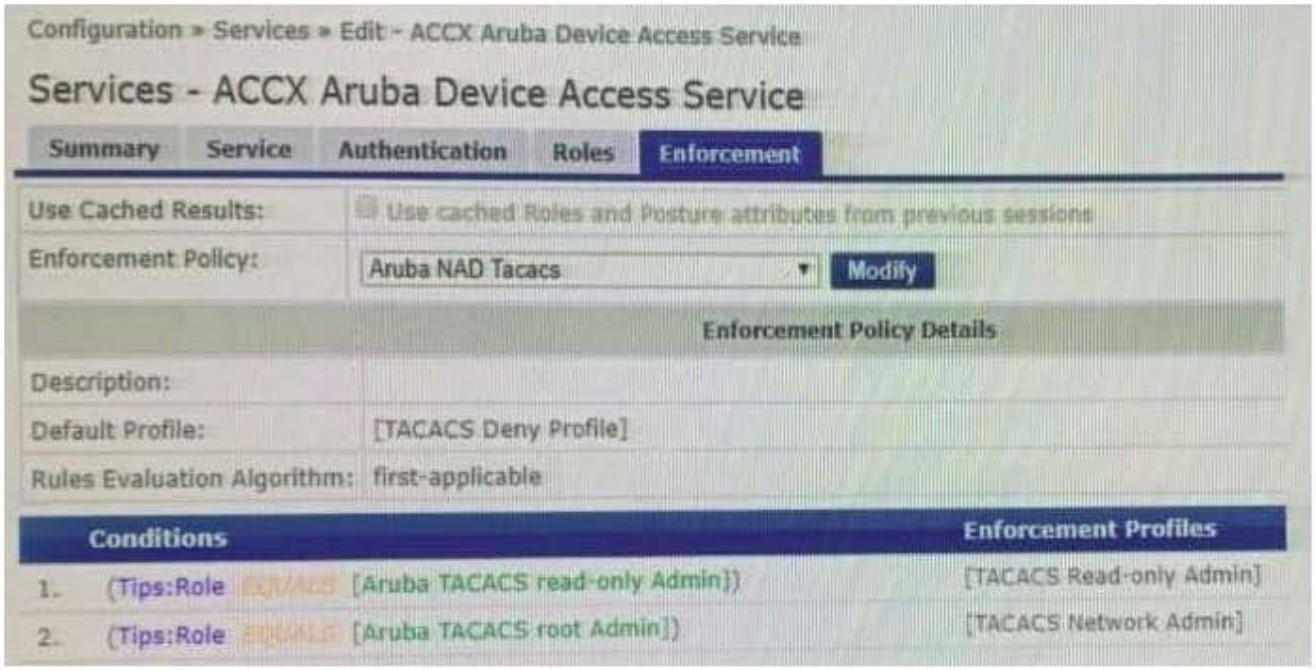
C. expire_time

D. expire_ postlogin

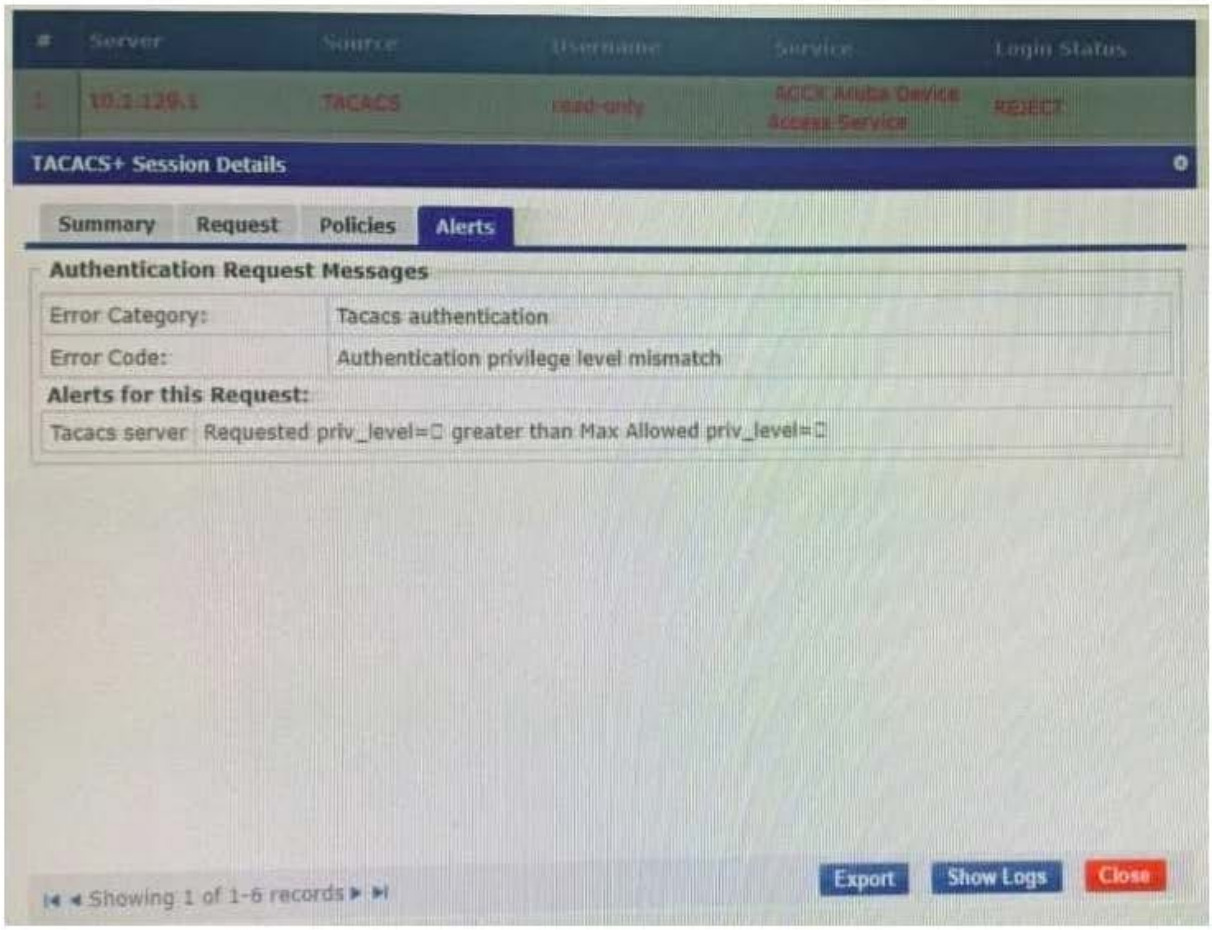
Correct Answer: A

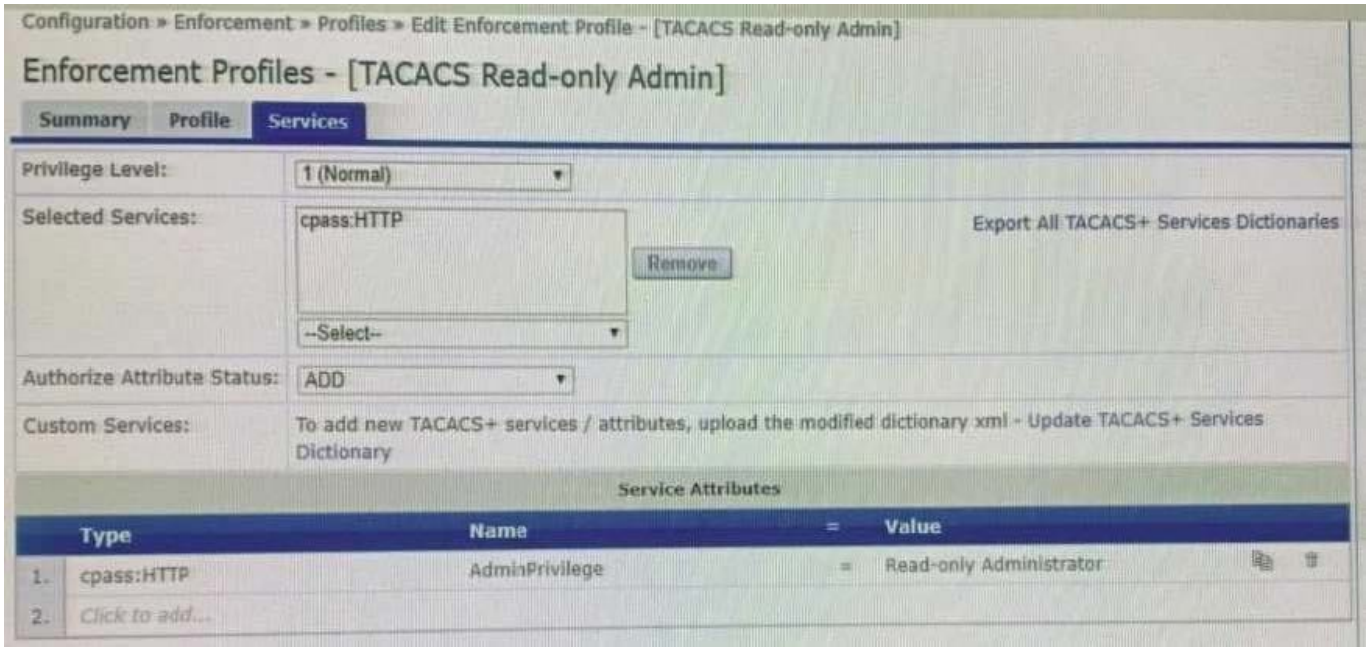
QUESTION 8

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
1
10.1.129.1
TACACS
read-only
ACCX 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 9

A corporate ClearPass Cluster with two servers located at a single site, has both Management and Data port IP addresses configured. The Management port IPs are in the DataCenter networks subnet, while the Data port IPs are in the DMZ. What is the difference between using one Virtual IP for the AAA traffic versus sending AAA requests to the physical IPs for each server? (Select two.)

A. The failover can be accomplished only by using Virtual IP.

B. The Individual IPs can provide failover and load balancing.

C. One Virtual IP can be used together with the individual server IPs for load balancing.

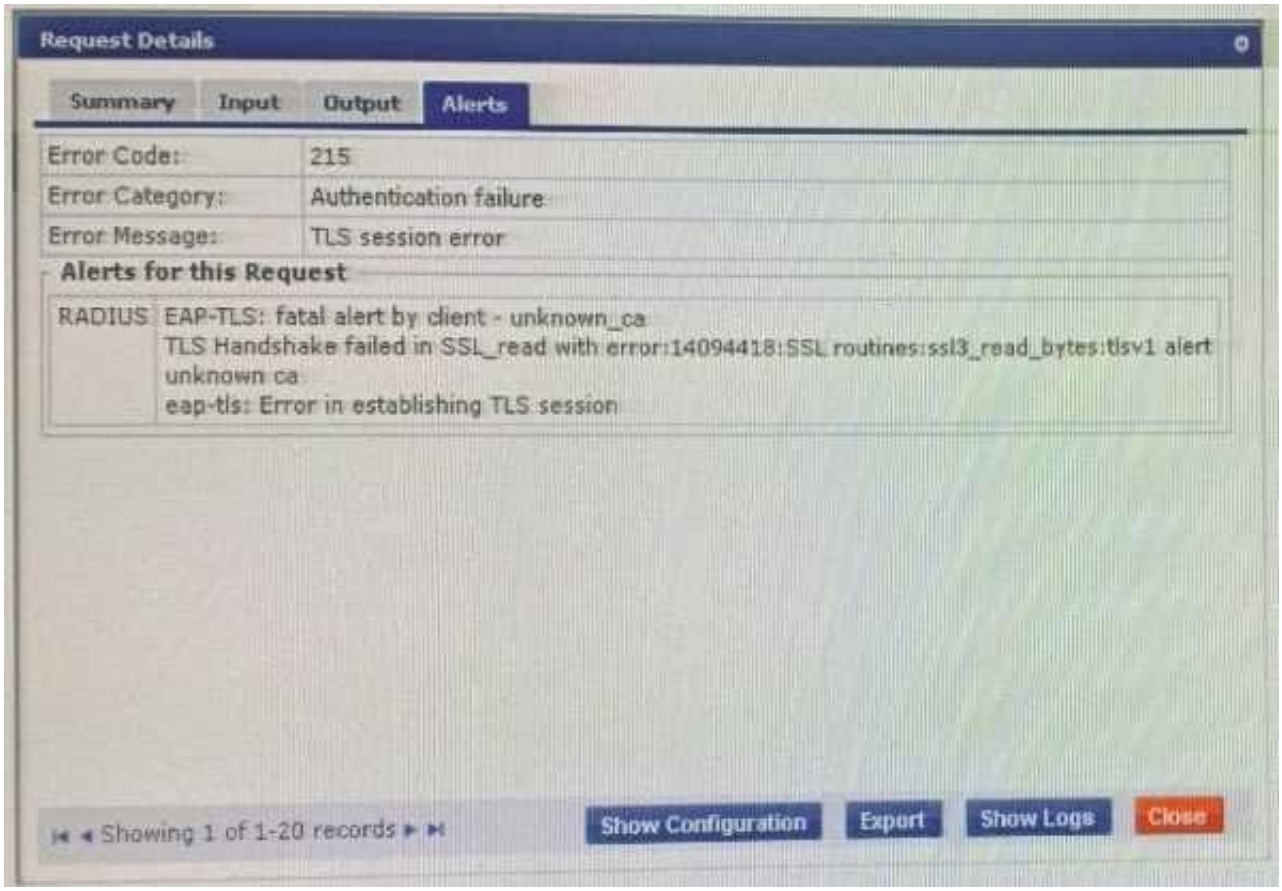
D. By using the Virtual IP, the failover convergence is faster than using individual server IPs.

E. Using the one Virtual IP can provide failover and load balancing.

Correct Answer: BE

QUESTION 10

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

QUESTION 11

You are deploying ClearPass Policy Manager with Guest functionality for a customer with multiple Aruba Networks Mobility Controllers The customer wants to avoid SSL errors during guest access but due to company security policy cannot use a wildcard certificate on ClearPass or the Controllers. What is the most efficient way to configure the customers guest solution? (Select two.)

A. Build multiple Web Login pages with vendor settings configured for each controller

B. Install the same public certificate on all Controllers with the common name "controller {company domain}"

C. Build one Web Login page with vendor settings for controller {company domain)

D. Install multiple public certificates with a different Common Name on each controller

Correct Answer: AB

QUESTION 12

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