HP

HPE6-A81 Exam

Aruba Certified ClearPass Expert Written

Question: 1

You art deploying Cleat Pass 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 customer's guest solution? (Select two.)

A. Install the same public certificate on all Controllers with the common name "controller.{company domain)
B. Build multiple Web Login pages with vendor settings configured for each controller
C. Build one Web Login page with vendor settings for captiveportal-controller (company domain)
D. Build one Web Login page with vendor settings for controller (company domain)
E. Install multiple public certificates with a different Common Name on each controller
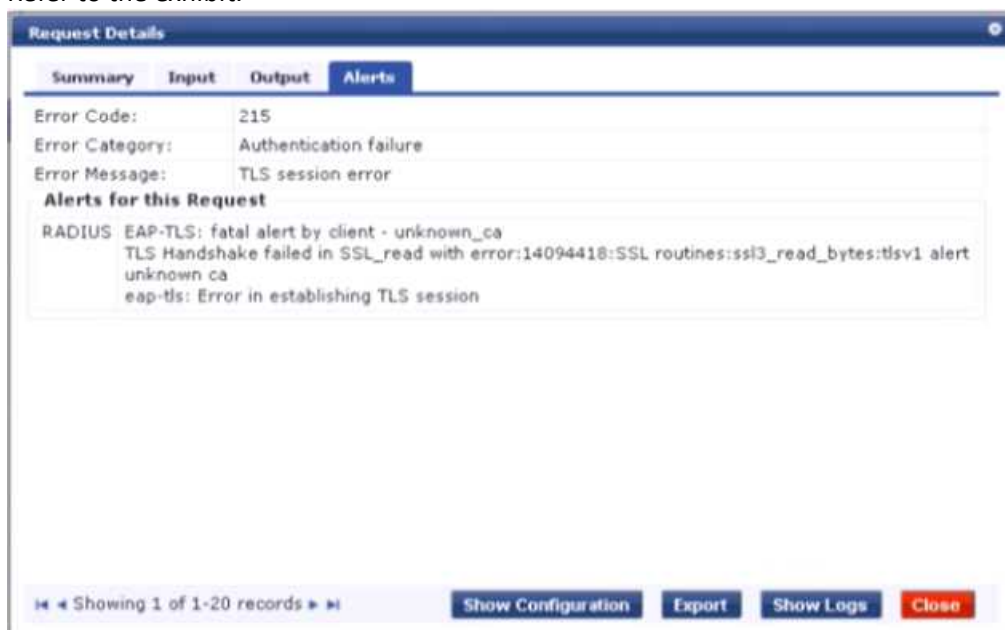
Answer: DE

Question: 2

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

B. Have all of the BYOO clients disconnect and reconnect to the network.

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

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

Answer: BCD

Question: 3

Refer to the exhibit.

A customer with multiple Aruba Controllers has just installed a new certificate for "'.customerdomain.com- on all Aruba Controllers While testing the existing guest Self-Registration page the customer noticed that the logins are failing While troubleshooting they are finding no entries in the Event Viewer or Access Tracker for the tests Suspecting that the Aruba Controllers may not be properly posting the credentials from the guest browser, they open the NAS Vendor Settings for the Guest Self-Registration Page.

A. Add PTR records on the DNS server for "securelogin arubanetworks.com".

B. Change the "Secure Login' field to "Use Vendor Default".

C. Change the 'IP Address field to" securelogin.customerdomain.com

D. Change the "IP Address field to "captiveportal-login.customerdomain.com".

Answer: D

Question: 4

Refer to the exhibit.

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 *EQUALS* HEALTHY (0))	T4-Healthy, [ArubaOS Wireless - Terminate Session]
2.	(Tips:Posture *EQUALS* 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	Configure View	-
☐	Windows Security Health Validator	Configure View	-

Posture Policies - Windows

Summary	Policy	Posture Plugins	Rules

Rules Evaluation Algorithm: First applicable

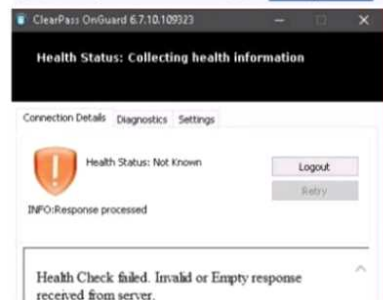|	Conditions	Posture Token
1.	Passes all SHV checks - ClearPass Windows Universal System Health Validator	HEALTHY
2.	Fails one or more SHV checks - ClearPass Windows Universal System Health Validator	QUARANTINE

Add Rule **Move Up ↑** **Move Down ↓** **Edit Rule** **Remove Rule**

Request Details ⊗

Summary	Input	Output

Login Status:	ACCEPT
Session Identifier:	W0000002e-01-5dSce4f4
Date and Time:	Aug 21, 2019 08:30:13 CEST
End-Host Identifier:	7c5cf8cb1f0b
Username:	7c5cf8cb1f0b
Access Device IP/Port:	-
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Health-Check
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	-
Enforcement Profiles:	[ArubaOS Wireless - Terminate Session]
Service Monitor Mode:	Disabled

I◄ ◄ Showing 6 of 1-173 records ► ►I **Change Status** **Show Configuration** **Export** **Show Logs** **Close**

ClearPass OnGuard 6.7.10.109323   — ☐ ✕

Health Status: Collecting health information

Connection Details	Diagnostics	Settings

Health Status: Not Known   Logout
                              Retry

INFO:Response processed

Health Check failed. Invalid or Empty response
received from server.

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 Health-Check service does not have Posture Compliance option enabled
C. The client's OnGuard Agent has not been configured with the correct Policy Manager Zone.
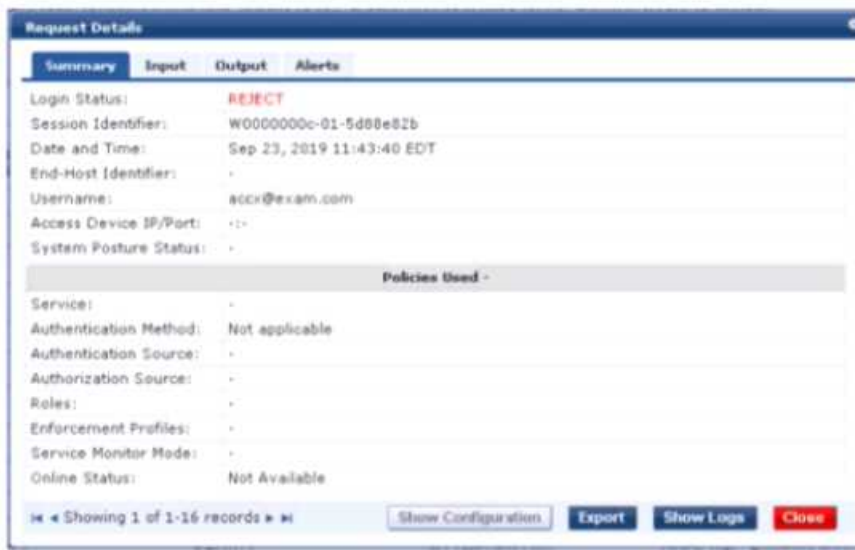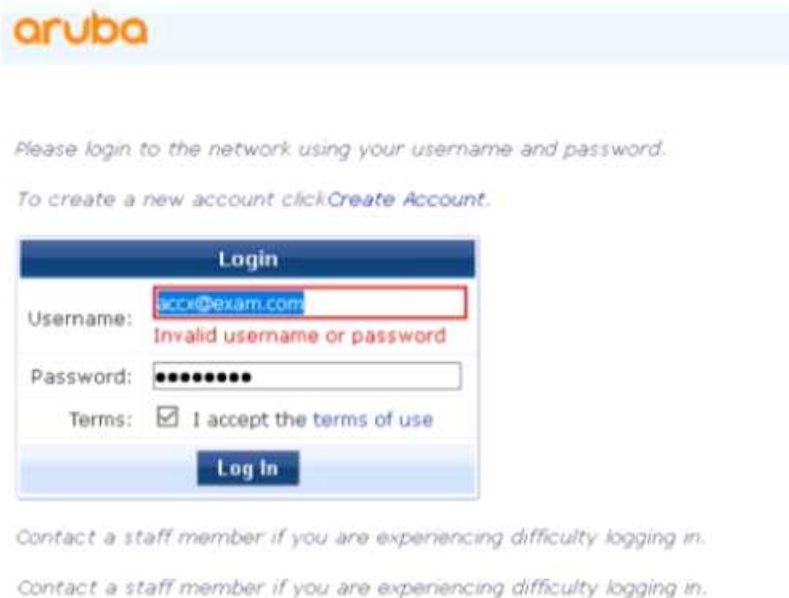D. There is a firewall policy not allowing the OnGuard Agent to connect to ClearPass

Answer: A

Question: 5

Refer to the exhibit.

Request Details

Summary	Input	Output	Alerts

Error Code:	204
Error Category:	Authentication failure
Error Message:	Failed to classify request to service
Alerts for this Request	
WebAuthService	ServiceClassification failed {No service matched}

Configuration » Services » Edit - ACCX Guest Access

Services - ACCX Guest Access

Summary	Service	Authentication	Roles	Enforcement

Service:

Name:	ACCX Guest Access
Description:	To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	Calling-Station-Id	EXISTS	
2.	Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS	guest-labtest

Authentication:

Authentication Methods:	1. [PAP] 2. [MSCHAP] 3. [CHAP]
Authentication Sources:	[Guest User Repository]
Strip Username Rules:	-
Service Certificate:	-

Roles:

Role Mapping Policy:	[Guest Roles]

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	Accx Guest Access Enforcement Policy

Home » Configuration » Pages » Web Logins

Web Login (ACCX_LabTest)

*Use this form to make changes to the Web Login **ACCX_LabTest**.*

Web Login (ACCX_LabTest)

Use this form to make changes to the Web Login **ACCX_LabTest**.

Web Login Editor	
* Name:	ACCX_LabTest Enter a name for this web login page.
Page Name:	ACCX_TestPage Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	 Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
Login Method:	Controller-initiated — Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* Address:	securelogin.arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default

Page Redirect

Options for specifying parameters passed in the initial redirect.

Security Hash:	Do not check — login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Login Form

Options for specifying the behaviour and content of the login form.

Authentication:	Credentials — Require a username and password Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.
Prevent CNA:	☐ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	☐ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	☐ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	App Authentication — check using Aruba Application Authentication Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	☐ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
Prevent CNA:	☐ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	☐ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	☐ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	App Authentication — check using Aruba Application Authentication Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	☐ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

A year ago. your customer deployed an Aruba ClearPass Policy Manager Server for a Guest SSID hosted in an IAP Cluster The customer just created a new Web Login Page for the Guest SSiD Even though the previous Web Login page worked test with the new Web Login Page are failing and the customer has forwarded you the above screenshots.

What recommendation would you give the customer to fix the issue?

A. The customer should reset the password for the username accxCdlexam.com using Guest Manage Accounts.

B. The service type configured is not correct. The Guest authentication should be an Application authentication type of service.

C. The Address filed under the WebLogin Vendor settings is not configured correctly. It should be set to instant, Aruba networks com,

D. The WebLogin Pre-Auth Check is set to Aruba Application Authentication which requires a separate application service on the policy manager

Answer: C