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.passapply.com/hpe6-a81.html

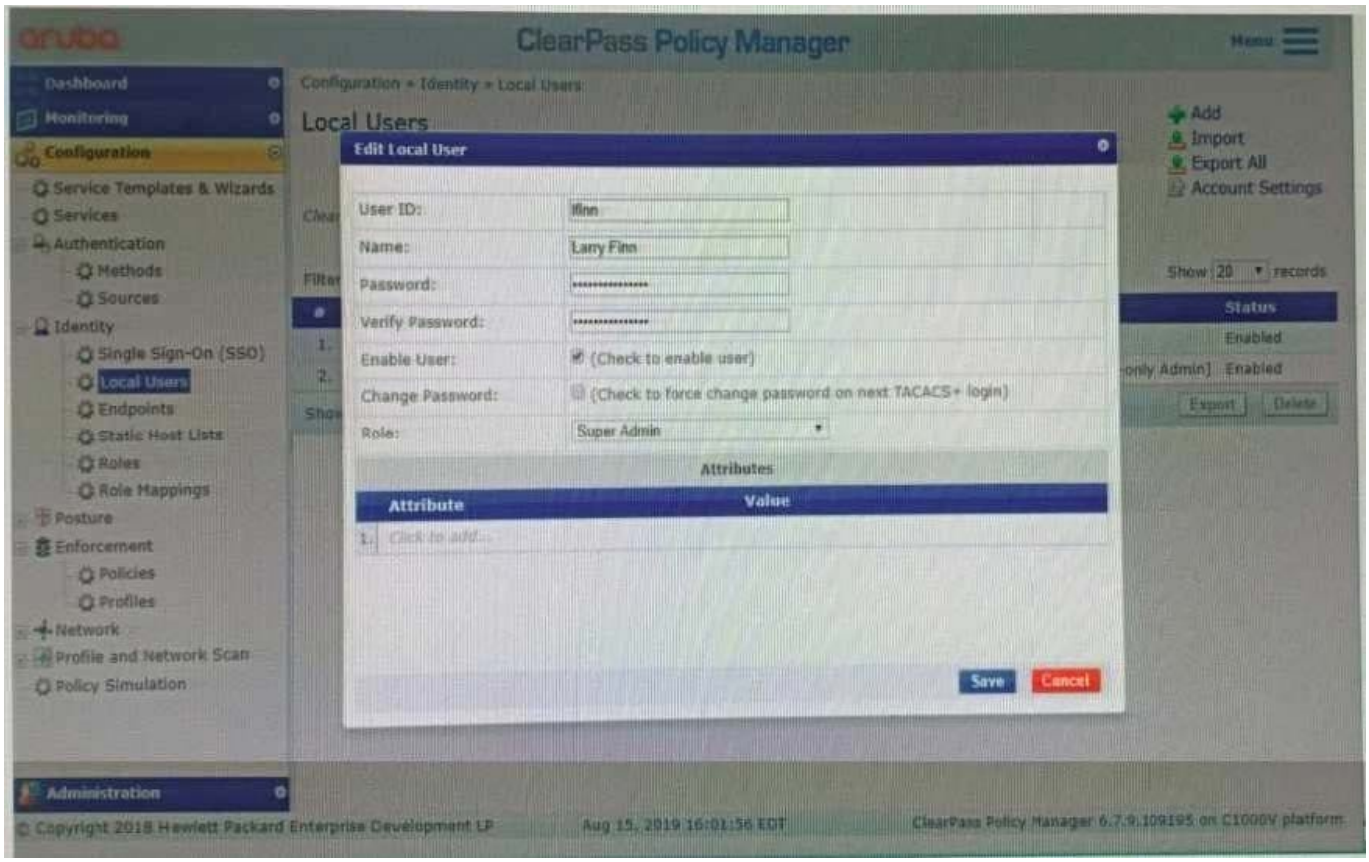
100% Passing Guarantee
100% Money Back Assurance

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:



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 2

Refer to the exhibit:


aruba
Please login to the network using your username and password.
To create a new account click Create Account.
Login
Username:
accx@exam.com
Invalid username or password
Password:
Terms:
I accept the terms of use
Log In
Contact a staff member if you are experiencing difficulty logging in

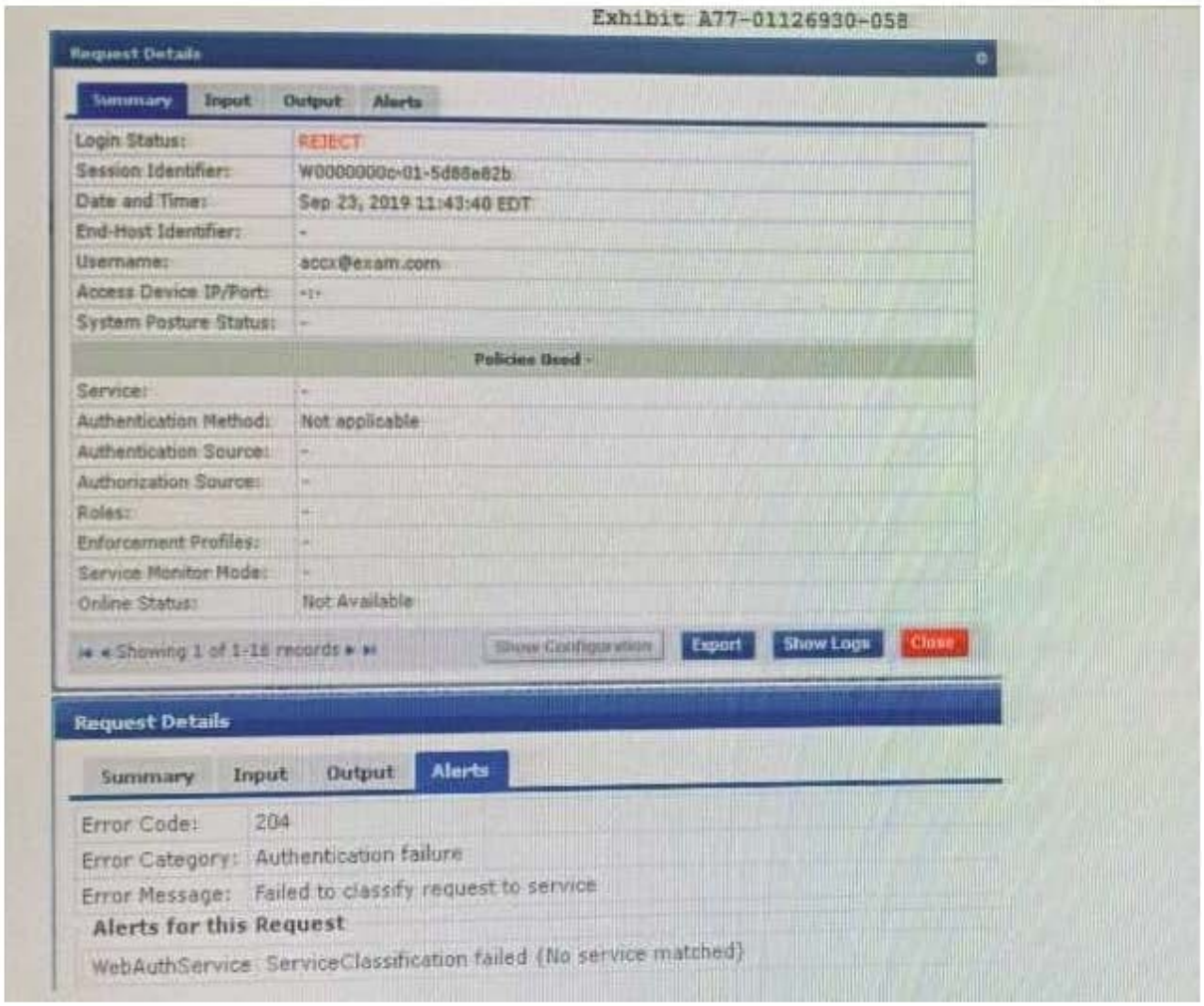


Exhibit A77-01126930-058
Request Details
Summary
Input
Output
Alerts
Login Status: REJECT
Session Identifier: W0000000c-01-5d88a82b
Date and Time: Sep 23, 2019 11:43:40 EDT
End-Host Identifier: -
Username: accx@exam.com
Access Device IP/Port: -:-
System Posture Status: -
Policies Used -
Service: -
Authentication Method: Not applicable
Authentication Source: -
Authorization Source: -
Roles: -
Enforcement Profiles: -
Service Monitor Mode: -
Online Status: Not Available
Showing 1 of 1-16 records
Export
Show Logs
Close
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
1.	Radius:IETF	Calling-Station-Id	EXISTS
2.	Connection	Client-Mac-Address	NOT_EQUALS
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS

Authentication:

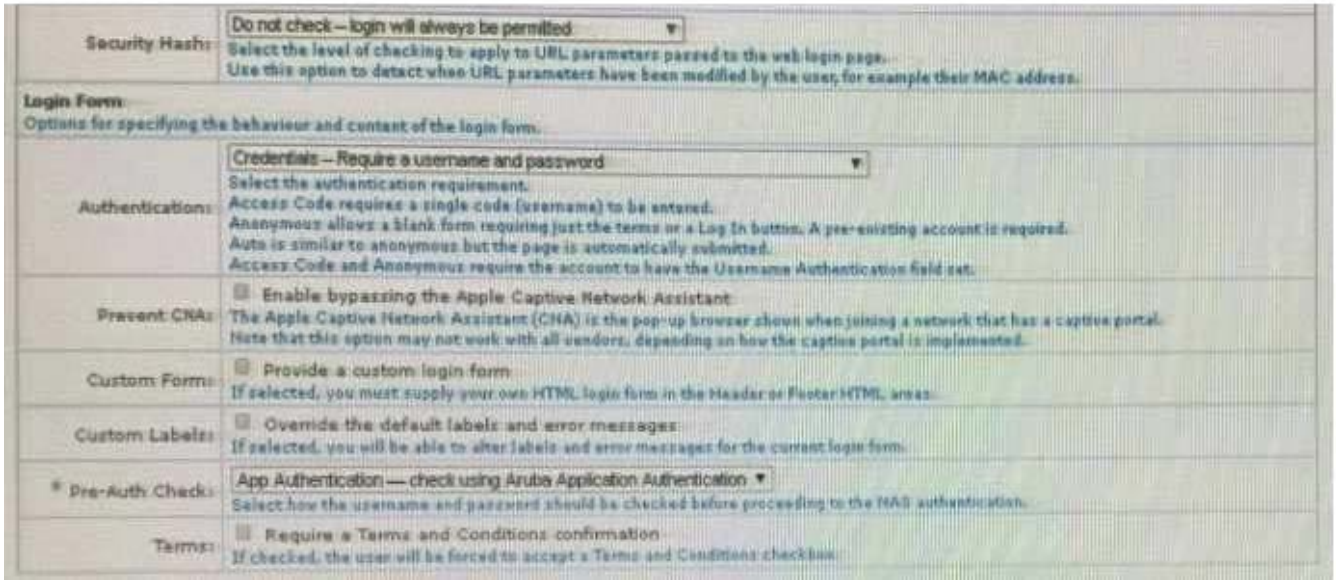
Authentication Methods:	1. [PAP] 2. [MSCHAP] 3. [CHAP]
Authentication Sources:	[Guest User Repository]
Strip Username Rules:	-
Service Certificate:	-

Roles:

Role Mapping Policy:	[Guest Roles]

Enforcement:

Use Cached Results:	Disabled



A year ago, your customer deployed an Aruba ClearPass Policy Manager Server for a Guest SSIC 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 falling and the customer has

forwarded you the above screenshots.

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

A. The service type configured is not correct. The Guest authentication should De an Application authentication type of service.

B. The customer should reset the password tor the username accx@exam com using Guest Manage Accounts

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

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

Correct Answer: A

QUESTION 3

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.

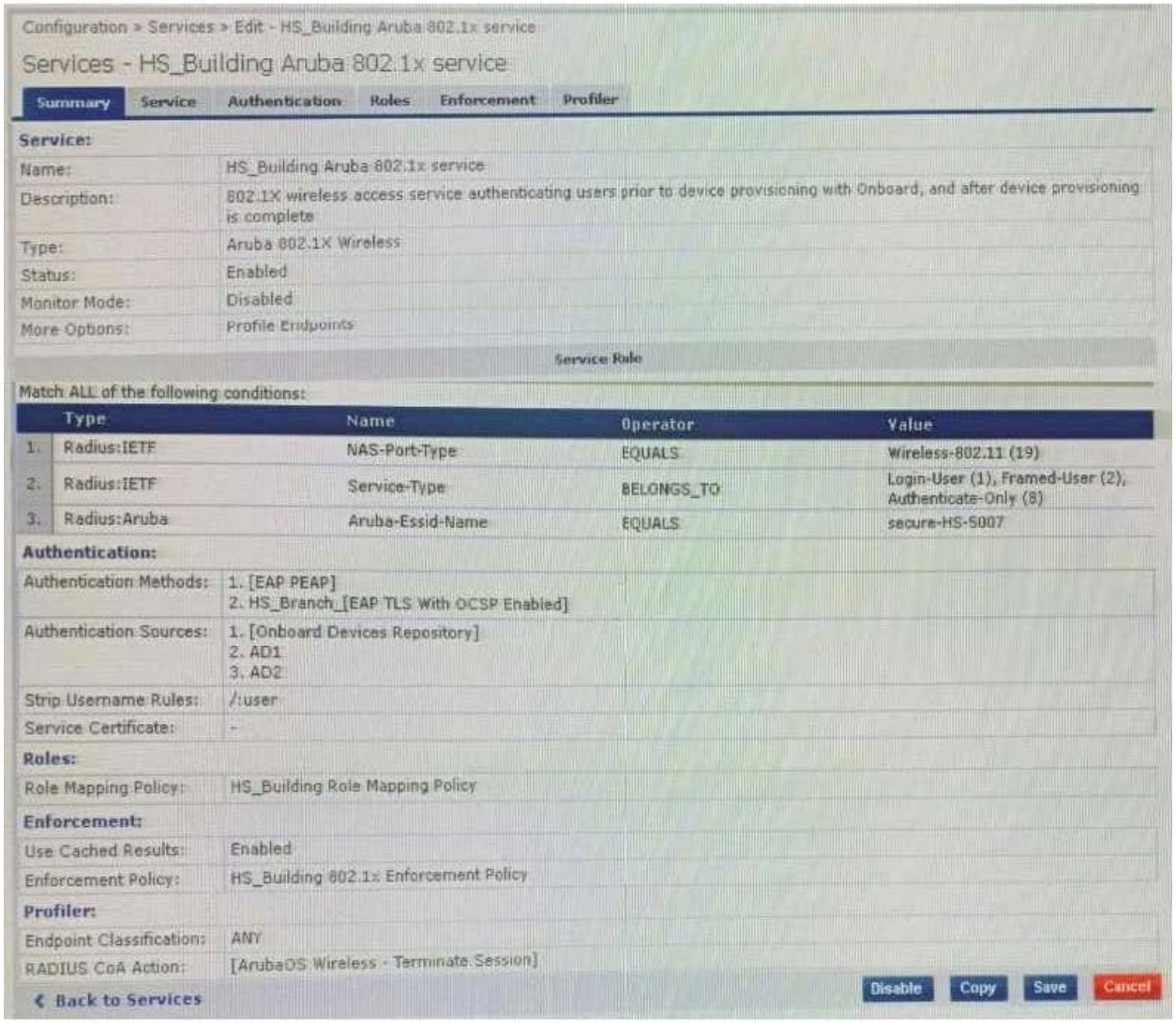
E. Using the one Virtual IP can provide failover and load balancing.

Correct Answer: BE

QUESTION 4

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Login Status: REJECT
Session Identifier: R00000218-01-5d9db68b
Date and Time: Oct 09, 2019 06:29:34 EDT
End-Host Identifier: 78D29437BD68 (Computer / Windows / Windows 10)
Username: andy07
Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: HS_Building Aruba 802.1x service
Authentication Method: EAP-PEAP,EAP-MSCHAPv2
Authentication Source: AD:AD1.aruba1.local
Authorization Source: AD1
Roles: [Other], [User Authenticated]
Enforcement Profiles: [Deny Access Profile]
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Show Configuration
Export
Show Logs
Close
Request Details
Summary
Input
Output
Alerts
Error Code: 206
Error Category: Authentication failure
Error Message: Access denied by policy
Alerts for this Request
RADIUS Applied 'Reject' profile



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 VIP User MAC) VIP User
2. (Authorization:Corp SQL:MAC) Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category VoIP Phone) IP Phone
4. (Authorization:[Endpoints Repository]:Category SmartDevice) Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category Point of Sale devices) Vending Machine
6. (Authorization:[Endpoints Repository]:Category Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor CANON INC.) Printer
7. (Authorization:[Endpoints Repository]:Category Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor 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 true) Aruba Full Access Profile
2. (Authentication:OuterMethod EAP-PEAP) AND (Tips:Role Corp SQL Tablet) Redirect to Aruba OnBoard Portal
3. (Authentication:OuterMethod EAP-TLS) AND (Tips:Role Corp SQL Tablet) Aruba Full Access Profile
4. (Tips:Role VIP User) Aruba VIP Full Access Profile
5. (Tips:Role [User Authenticated] [Machine Authenticated]) AND (Authentication:Source AD1) AND (Tips:Posture HEALTHY (0)) Aruba Full Access Profile
6. (Tips:Role [User Authenticated] [Machine Authenticated]) AND (Authentication:Source AD1) AND (Tips:Posture UNKNOWN (100)) Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7. (Tips:Role [User Authenticated] [Machine Authenticated]) AND (Authentication:Source AD1) AND (Tips:Posture 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 5

A customer has completed all the required configurations in the Windows server in order for Active Directory Certificate Services (ADCS) to sign Onboard device TLS certificates. The Onboard portal and the Onboard services are also configured. Testing shows that the Client certificates ate still signed by the Onboard Certificate Authority and not ADCS. How can you help the customer with the situation?

A. Educate the customer that, when integrating with Active Directory Certificate Services (ADCS) the Onboard CA will the same authority used for signing me final TLS certificate of the device.

B. Configure the identity certificate signer as Active Directory Certificate Services and enter the ADCS URL http://ADCSVVeoEnrollmentServemostname/certsrv in the OnBoard Provisioning settings.

C. Enable access to EST servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

D. Enable access to SCEP servers from the Certificate Authority to make ClearPass Onboard to use of the Active Directory Certificate Services (ADCS) web enrollment to sign the device TLS certificates.

Correct Answer: C