HP.HPE6-A68.by.Odin.88q

Number: HPE6-A68
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: HPE6-A68
Exam Name: Aruba Certified ClearPass Professional (ACCP) V6.7

Exam A

QUESTION 1
Under which circumstances is it necessary to use an SNMP based Enforcement profile to send a VLAN?

A. when a VLAN must be assigned to a wired user on an Aruba Mobility Controller
B. when a VLAN must be assigned to a wireless user on an Aruba Mobility Controller
C. when a VLAN must be assigned to a wired user on a third party wired switch that does not support RADIUS return attributes
D. when a VLAN must be assigned to a wired user on an Aruba Mobility Access Switch
E. when a VLAN must be assigned to a wired user on a third party wired switch that does not support RADIUS accounting

Correct Answer: C
Section:

QUESTION 2
What must be configured to enable RADIUS authentication with ClearPass on a network access device (NAD)? (Select two.)

A. the ClearPass server must have the network device added as a valid NAD
B. the ClearPass server certificate must be installed on the NAD
C. a matching shared secret must be configured on both the ClearPass server and NAD
D. an NTP server needs to be set up on the NAD
E. a bind username and bind password must be provided

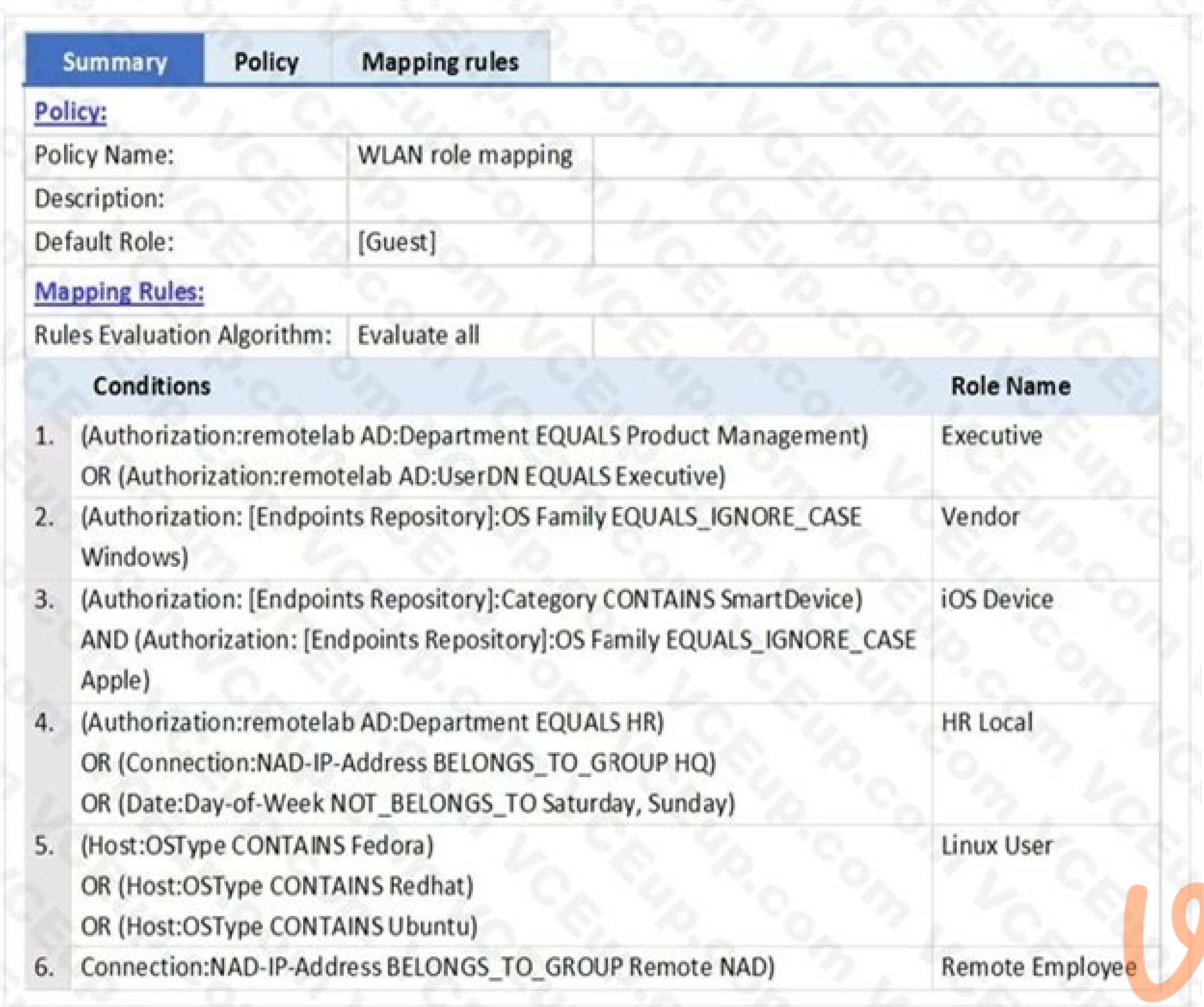
Correct Answer: A, C
Section:

QUESTION 3
If the "Alerts" tab in an access tracker entry shows the following error message: "Access denied by policy", what could be a possible cause for authentication failure?

A. Configuration of the Enforcement Policy.
B. An error in the role mapping policy.
C. Failure to select an appropriate authentication method for the authentication request.
D. Implementation of a firewall policy on ClearPass.
E. Failure to find an appropriate service to process the authentication request.

Correct Answer: A
Section:

QUESTION 4
Refer to the exhibit.



Policy:

Policy Name:	WLAN role mapping
Description:	
Default Role:	[Guest]

Mapping Rules:

Rules Evaluation Algorithm:	Evaluate all

	Conditions	Role Name
1.	(Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive
2.	(Authorization: [Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Windows)	Vendor
3.	(Authorization: [Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization: [Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Apple)	iOS Device
4.	(Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	HR Local
5.	(Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User
6.	Connection:NAD-IP-Address BELONGS_TO_GROUP Remote NAD)	Remote Employee

An AD user's department attribute is configured as "HR". The user connects on Monday using an Android phone to an Aruba Controller that belongs to the Device Group Remote NAD. Which roles are assigned to the user in ClearPass? (Select two.)

A. Executive
B. iOS Device
C. Vendor
D. Remote Employee
E. HR Local

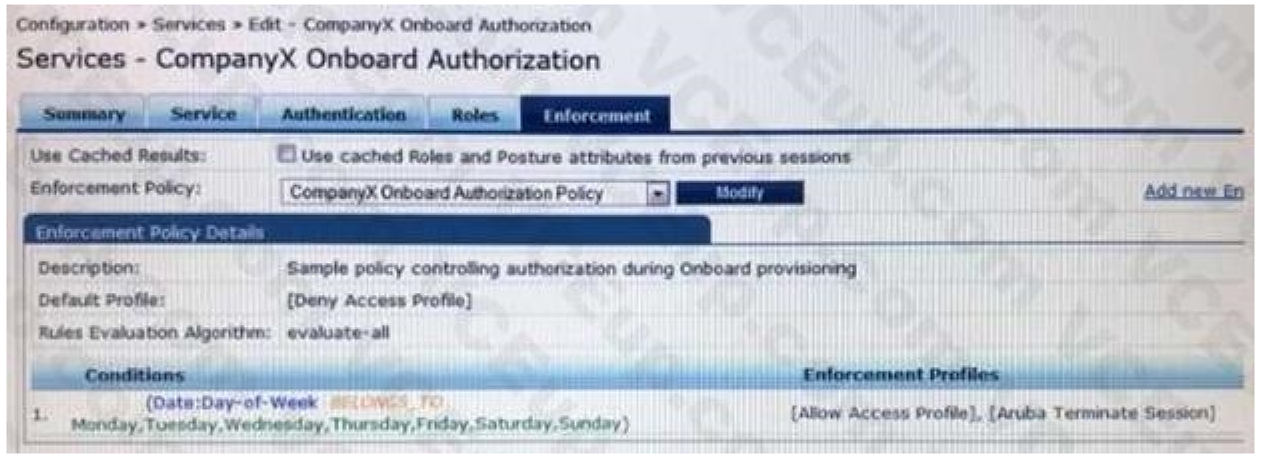
Correct Answer: D, E
Section:

QUESTION 5
When is the RADIUS server certificate used? (Select two.)

A. During dual SSID onboarding, when the client connects to the Guest network
B. During EAP-PEAP authentication in single SSID onboarding
C. During post-Onboard EAP-TLS authentication, when the client verifies the server certificate
D. During Onboard Web Login Pre-Auth, when the client loads the Onboarding web page
E. During post-Onboard EAP-TLS authentication, when the server verifies the client certificate

Correct Answer: C, D
Section:

QUESTION 6
Refer to the exhibit.



Configuration » Services » Edit - CompanyX Onboard Authorization

Services - CompanyX Onboard Authorization

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

Enforcement Policy: CompanyX Onboard Authorization Policy

Enforcement Policy Details

Description: Sample policy controlling authorization during Onboard provisioning

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

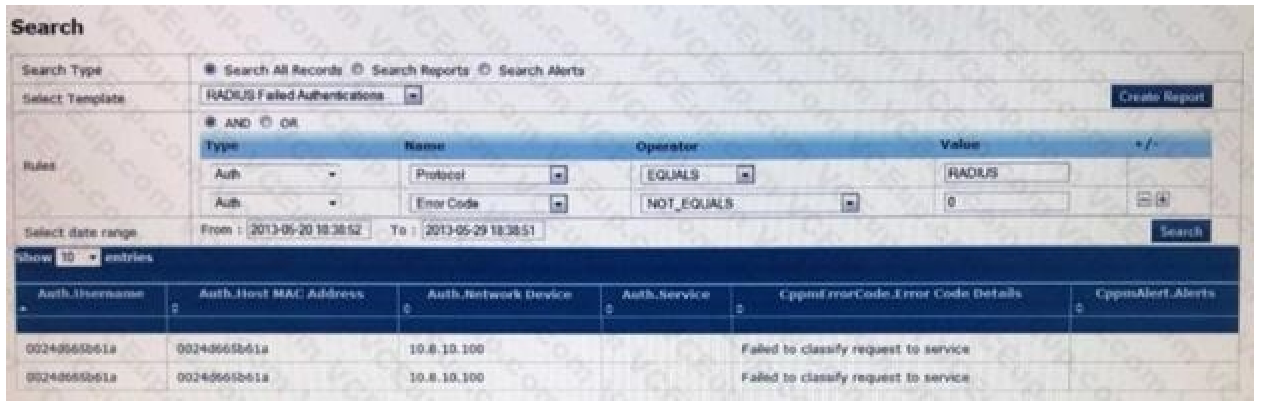
	Conditions	Enforcement Profiles
1.	(Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	[Allow Access Profile], [Aruba Terminate Session]

Based on the configuration of the Enforcement Profiles in the Onboard Authorization service shown, which Onboarding action will occur?

A. The device will be disconnected from the network after Onboarding so that an EAP-TLS authentication is not performed.
B. The device will be disconnected from and reconnected to the network after Onboarding is completed.
C. The device's onboard authorization request will be denied.
D. The device will be disconnected after post-Onboarding EAP-TLS authentication, so a second EAPTLS authentication is performed.
E. After logging in on the Onboard web login page, the device will be disconnected form and reconnected to the network before Onboard begins.

Correct Answer: B
Section:

QUESTION 7
Refer to the exhibit.



Search

Search Type: ● Search All Records ○ Search Reports ○ Search Alerts

Select Template: RADIUS Failed Authentications

Rules: ● AND ○ OR

Type	Name	Operator	Value
Auth	Protocol	EQUALS	RADIUS
Auth	Error Code	NOT_EQUALS	0

Select date range: From : 2013-05-20 18:38:52 To : 2013-05-29 18:38:51

Auth.Username	Auth.Host MAC Address	Auth.Network Device	Auth.Service	CppmErrorCode.Error Code Details	CppmAlert.Alerts
0024d665b61a	0024d665b61a	10.8.10.100		Failed to classify request to service	
0024d665b61a	0024d665b61a	10.8.10.100		Failed to classify request to service	

An administrator configured a service and tested authentication, but was unable to complete authentication successfully. The administrator performs a Search using insight and the information displays as shown.
What is a possible reason for the ErrorCode 'Failed to classify request to service' shown?

A. The user failed authentication due to an incorrect password.
B. ClearPass could not match the authentication request to a service, but the user passed authentication.
C. ClearPass service authentication sources were not configured correctly.
D. The NAD did not send the authentication request.
E. ClearPass service rules were not configured correctly.

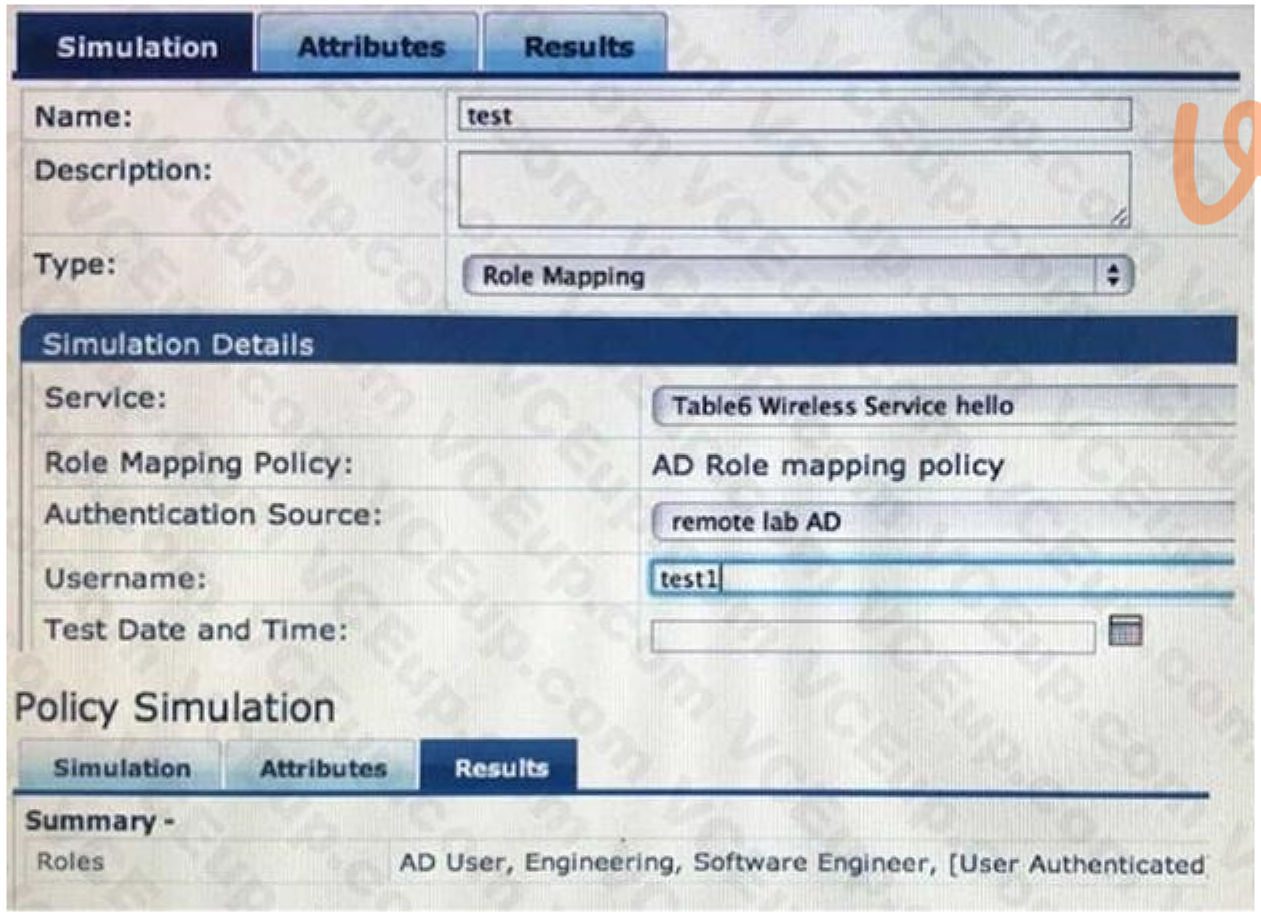
Correct Answer: E
Section:

QUESTION 8
What is the purpose of RADIUS CoA (RFC 3576)?

A. to force the client to re-authenticate upon roaming to a new Controller
B. to apply firewall policies based on authentication credentials
C. to validate a host MAC address against a whitelist or a blacklist
D. to authenticate users or devices before granting them access to a network
E. to transmit messages to the NAD/NAS to modify a user's session status

Correct Answer: E
Section:
Explanation:
CoA messages modify session authorization attributes such as data filters.
Reference: https://tools.ietf.org/html/rfc3576

QUESTION 9
Refer to the exhibit.



Name: test

Description:

Type: Role Mapping

Simulation Details

Service: Table6 Wireless Service hello

Role Mapping Policy: AD Role mapping policy

Authentication Source: remote lab AD

Username: test1

Test Date and Time:

Policy Simulation

Summary -

Roles AD User, Engineering, Software Engineer, [User Authenticated

Which statement accurately reflects the status of the Policy Simulation test figure shown?

A. The test verifies that a client with username test1 can authenticate using EAP-PEAP.
B. Role mapping simulation verifies if the remote lab AD has the ClearPass server certificate.
C. Role mapping simulation verifies that the client certificate is valid during EAP-TLS authentication.

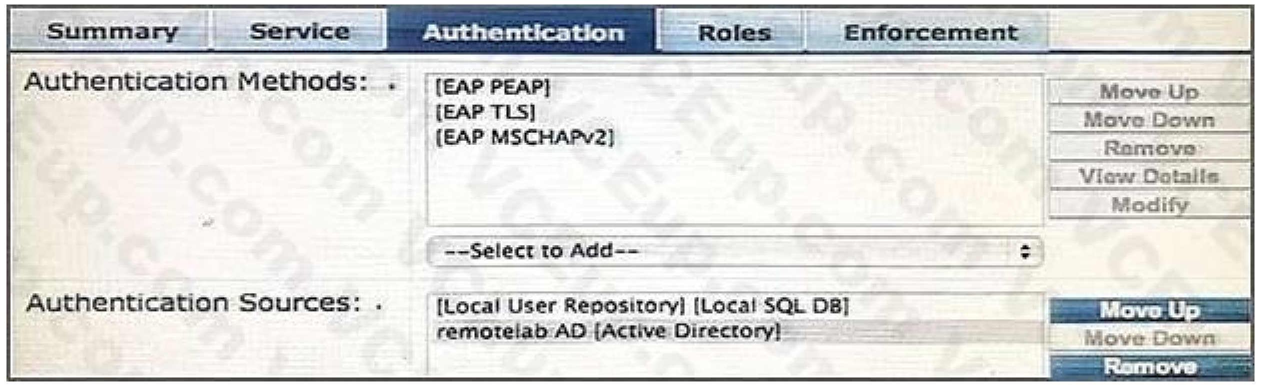
D. The simulation test result shows the firewall roles assigned to the client by the Aruba Controller.

E. The roles assigned in the results tab are based on rules matched in the AD Role Mapping Policy.

Correct Answer: E
Section:

QUESTION 10

Refer to the exhibit.



Authentication Methods:
[EAP PEAP]
[EAP TLS]
[EAP MSCHAPv2]
--Select to Add--

Authentication Sources:
[Local User Repository] [Local SQL DB]
remotelab AD [Active Directory]

Based on the Authentication sources configuration shown, which statement accurately describes the outcome if the user is not found?

A. If the user is not found in the remotelab AD but is present in the local user repository, a reject message is sent back to the NAD.

B. If the user is not found in the local user repository but is present in the remotelab AD, a reject message is sent back to the NAD.

C. If the user is not found in the local user repository a reject message is sent back to the NAD.

D. If the user is not found in the local user repository and remotelab AD, a reject message is sent back to the NAD.

E. If the user is not found in the local user repository a timeout message is sent back to the NAD.

Correct Answer: D
Section:
Explanation:
Policy Manager looks for the device or user by executing the first filter associated with the authentication source.
After the device or user is found, Policy Manager then authenticates this entity against this authentication source. The flow is outlined below:
* On successful authentication, Policy Manager moves on to the next stage of policy evaluation, which collects role mapping attributes from the authorization sources.
* Where no authentication source is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this service.
* If Policy Manager does not find the connecting entity in any of the configured authentication sources, it rejects the request.
Reference: ClearPass Policy Manager 6.5 User Guide (October 2015), page 134
https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

QUESTION 11

Which authorization servers are supported by ClearPass? (Select two.)

A. Aruba Controller

B. LDAP server

C. Cisco Controller

D. Active Directory

E. Aruba Mobility Access Switch

Correct Answer: B, D
Section:

Explanation:
Authentication Sources can be one or more instances of the following examples:
* Active Directory
* LDAP Directory
* SQL DB
* Token Server
* Policy Manager local DB
Reference: ClearPass Policy Manager 6.5 User Guide (October 2015), page 114
https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

QUESTION 12
Which CLI command is used to upgrade the image of a ClearPass server?

A. Image update
B. System upgrade
C. Upgrade image
D. Reboot
E. Upgrade software

Correct Answer: B
Section:
Explanation:
When logged in as appadmin, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands:
* system update (for patches)
* system upgrade (for upgrades)
Reference: ClearPass Policy Manager 6.5 User Guide (October 2015), page 564
https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

QUESTION 13
Which steps are required to use ClearPass as a TACACS+ Authentication server for a network device?
(Select two.)

A. Configure a TACACS Enforcement Profile on ClearPass for the desired privilege level.
B. Configure a RADIUS Enforcement Profile on ClearPass for the desired privilege level.
C. Configure ClearPass as an Authentication server on the network device.
D. Configure ClearPass roles on the network device.
E. Enable RADIUS accounting on the NAD.

Correct Answer: A, C
Section:
Explanation:
You need to make sure you modify your policy (Configuration » Enforcement » Policies » Edit - [Admin Network Login Policy]) and add your AD group settings in to the corresponding privilege level.

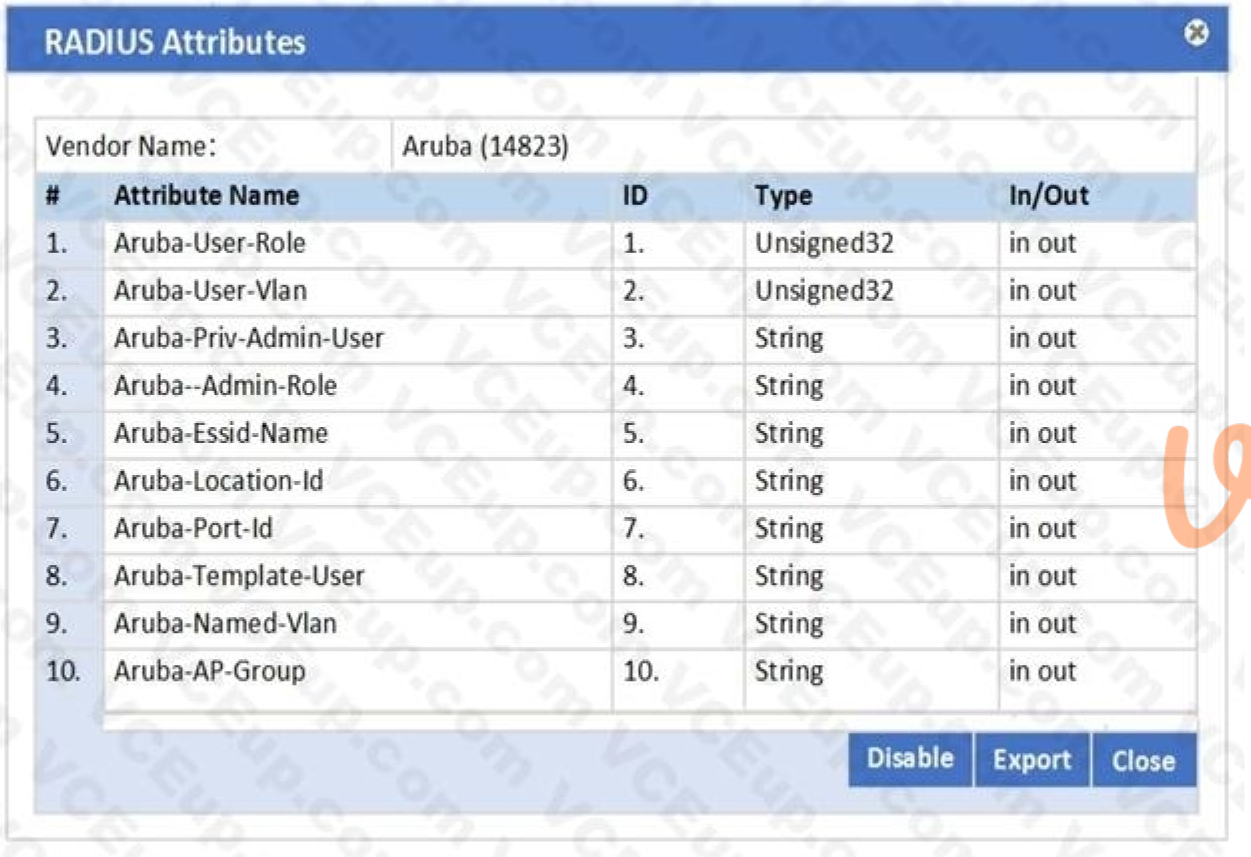
QUESTION 14
What are Operator Profiles used for?

A. to enforce role based access control for Aruba Controllers
B. to enforce role based access control for ClearPass Policy Manager admin users

C. to enforce role based access control for ClearPass Guest Admin users
D. to assign ClearPass roles to guest users
E. to map AD attributes to admin privilege levels in ClearPass Guest

Correct Answer: C
Section:
Explanation:
An operator profile determines what actions an operator is permitted to take when using ClearPass Guest.
Reference: http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/OperatorLog ins/OperatorProfiles.htm

QUESTION 15
Refer to the exhibit.



Vendor Name: Aruba (14823)

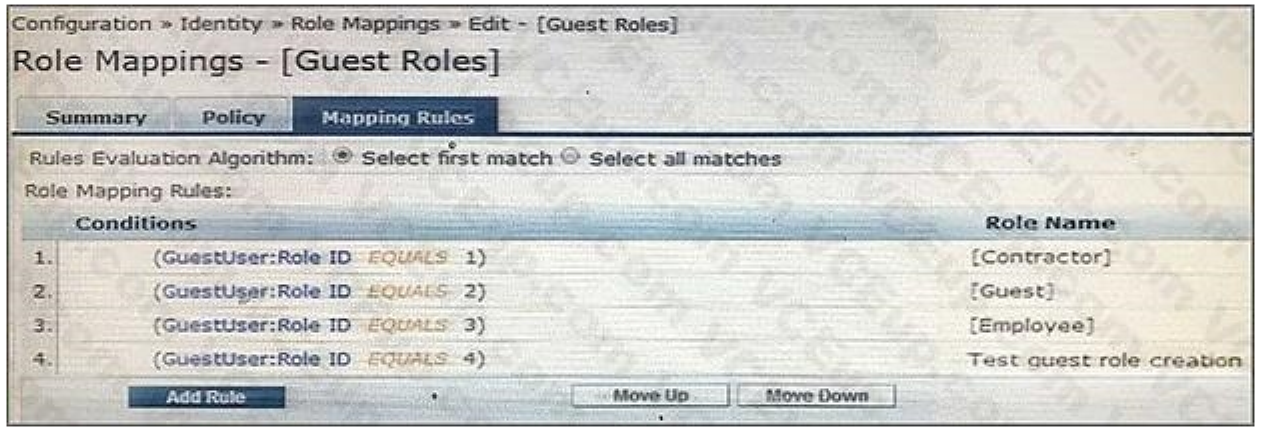
#	Attribute Name	ID	Type	In/Out
1.	Aruba-User-Role	1.	Unsigned32	in out
2.	Aruba-User-Vlan	2.	Unsigned32	in out
3.	Aruba-Priv-Admin-User	3.	String	in out
4.	Aruba--Admin-Role	4.	String	in out
5.	Aruba-Essid-Name	5.	String	in out
6.	Aruba-Location-Id	6.	String	in out
7.	Aruba-Port-Id	7.	String	in out
8.	Aruba-Template-User	8.	String	in out
9.	Aruba-Named-Vlan	9.	String	in out
10.	Aruba-AP-Group	10.	String	in out

In the Aruba RADIUS dictionary shown, what is the purpose of the RADIUS attributes?
In the Aruba RADIUS dictionary shown, what is the purpose of the RADIUS attributes?

A. to send information via RADIUS packets to Aruba NADs
B. to gather and send Aruba NAD information to ClearPass
C. to send information via RADIUS packets to clients
D. to gather information about Aruba NADs for ClearPass
E. to send CoA packets from ClearPass to the Aruba NAD

Correct Answer: C
Section:

QUESTION 16
Refer to the exhibit.



Configuration » Identity » Role Mappings » Edit - [Guest Roles]

Role Mappings - [Guest Roles]

Summary | Policy | Mapping Rules

Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Role Mapping Rules:

	Conditions	Role Name
1.	(GuestUser:Role ID EQUALS 1)	[Contractor]
2.	(GuestUser:Role ID EQUALS 2)	[Guest]
3.	(GuestUser:Role ID EQUALS 3)	[Employee]
4.	(GuestUser:Role ID EQUALS 4)	Test guest role creation

Based on the Guest Role Mapping Policy shown, what is the purpose of the Role Mapping Policy?

A. to display a role name on the Self-registration receipt page
B. to send a firewall role back to the controller based on the Guest User's Role ID
C. to assign Controller roles to guests
D. to assign three roles of [Contractor], [Guest] and [Employee] to every guest user
E. to create additional account roles for guest administrators to assign to guest accounts

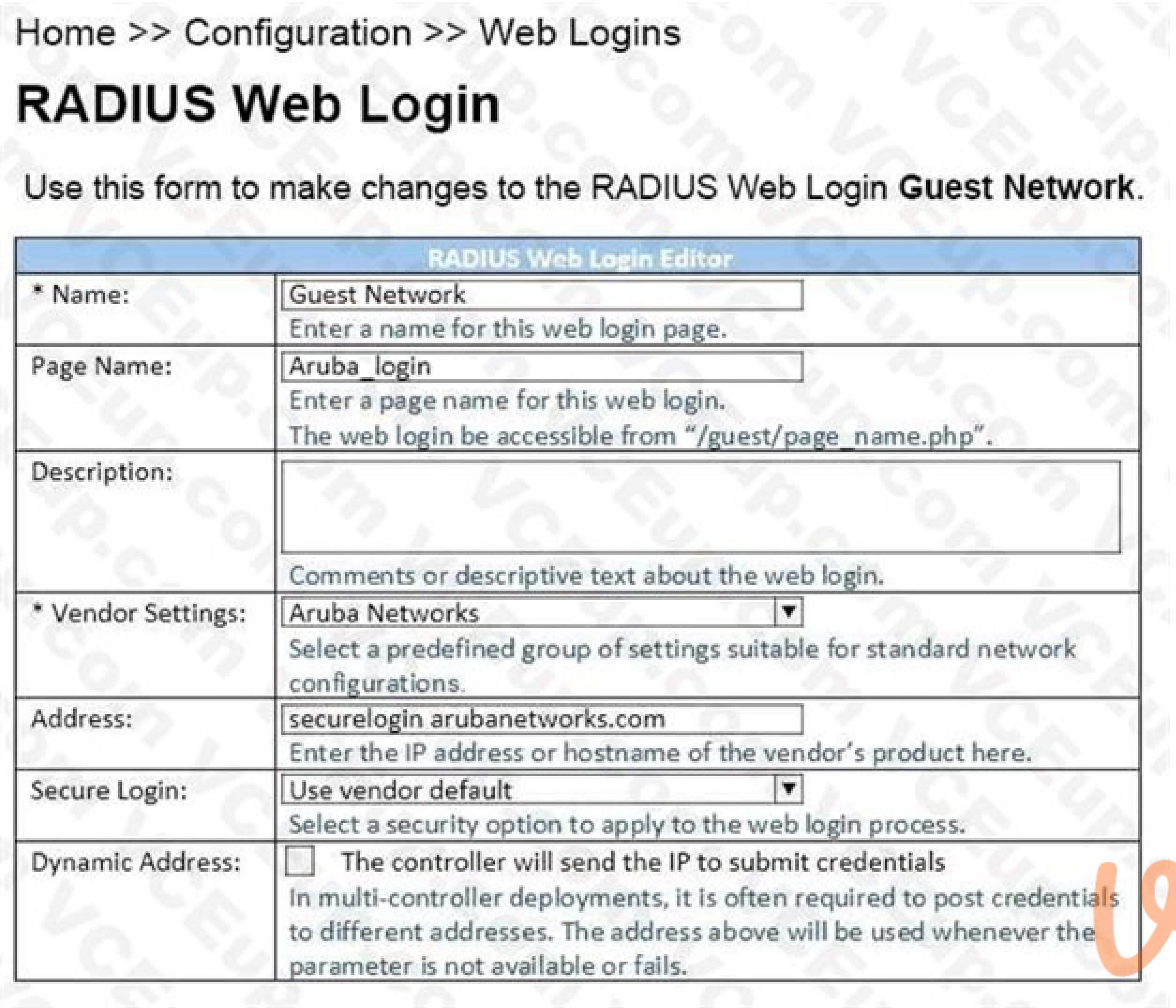
Correct Answer: C
Section:

QUESTION 17
A customer wants all guests who access a company's guest network to have their accounts approved by the receptionist, before they are given access to the network.
How should the network administrator set this up in ClearPass? (Select two.)

A. Enable sponsor approval confirmation in Receipt actions.
B. Configure SMTP messaging in the Policy Manager.
C. Configure a MAC caching service in the Policy Manager.
D. Configure a MAC auth service in the Policy Manager.
E. Enable sponsor approval in the captive portal authentication profile on the NAD.

Correct Answer: A, D
Section:
Explanation:
A: Sponsored self-registration is a means to allow guests to self-register, but not give them full access until a sponsor (could even be a central help desk) has approved the request. When the registration form is completed by the guest/user, an on screen message is displayed for the guest stating the account requires approval.
Guests are disabled upon registration and need to wait on the receipt page for the confirmation until the login button gets enabled.
D: Device Mac Authentication is designed for authenticating guest devices based on their MAC address.
Reference: ClearPass Policy Manager 6.5 User Guide (October 2015), page 94
https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

QUESTION 18
Refer to the exhibit.



Home >> Configuration >> Web Logins

RADIUS Web Login

Use this form to make changes to the RADIUS Web Login **Guest Network**.

RADIUS Web Login Editor	
* Name:	Guest Network Enter a name for this web login page.
Page Name:	Aruba_login Enter a page name for this web login. The web login 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.
Address:	securelogin arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default ▼ Select a security option to apply to the web login process.
Dynamic Address:	□ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses. The address above will be used whenever the parameter is not available or fails.

When configuring a Web Login Page in ClearPass Guest, the information shown is displayed.
What is the page name field used for?

A. for forming the Web Login Page URL

B. for Administrators to access the PHP page, but not guests

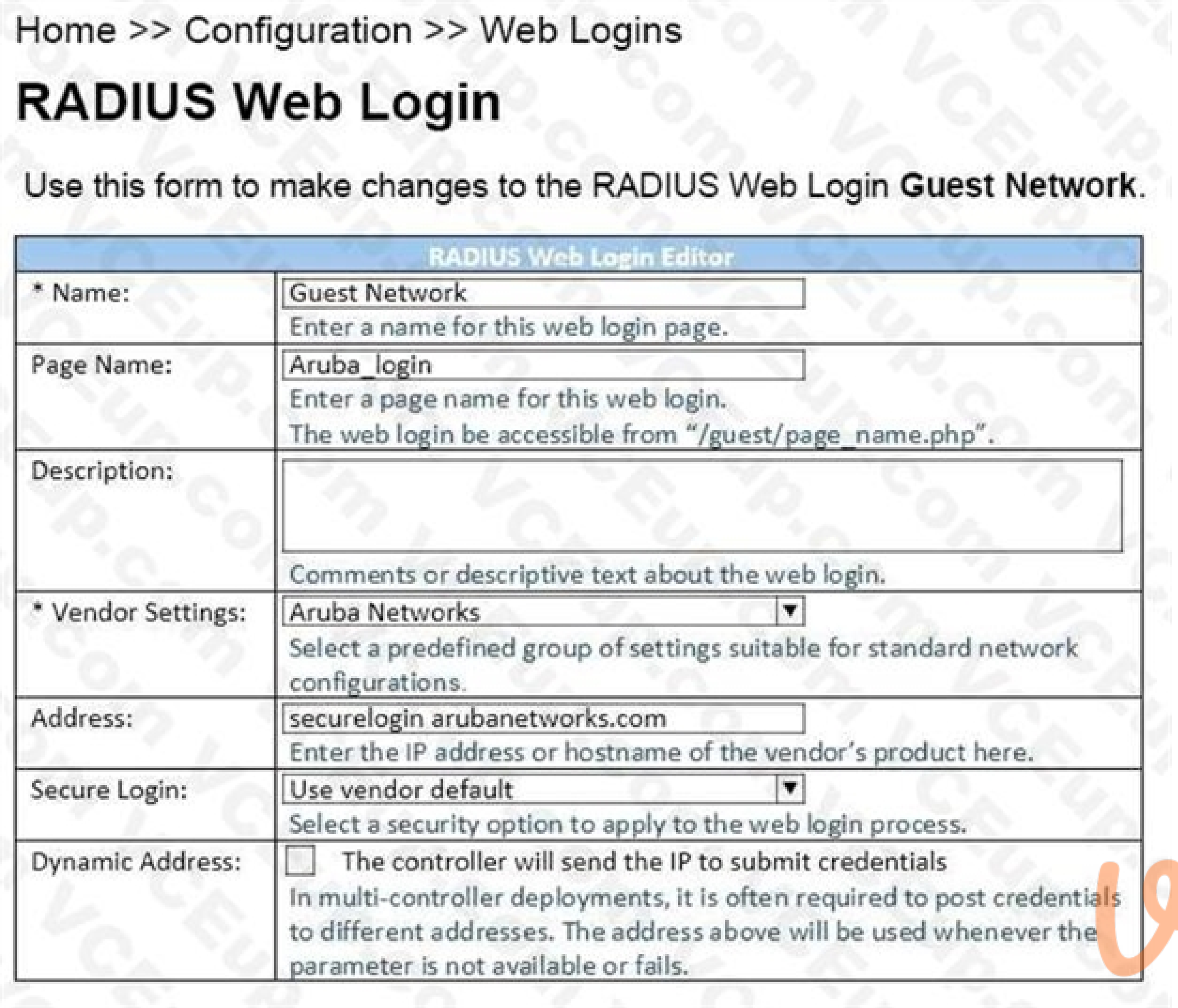
C. for Administrators to reference the page only

D. for forming the Web Login Page URL where Administrators add guest users

E. for informing the Web Login Page URL and the page name that guests must configure on their laptop wireless supplicant.

Correct Answer: A
Section:
Explanation:
The Page Name is an identifier page name that will appear in the URL -- for example, "/guest/page_name.php".
Reference: http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/Configuratio n/CreateEditWebLogin.htm

QUESTION 19
Refer to the exhibit.



Home >> Configuration >> Web Logins

RADIUS Web Login

Use this form to make changes to the RADIUS Web Login **Guest Network**.

RADIUS Web Login Editor	
* Name:	Guest Network Enter a name for this web login page.
Page Name:	Aruba_login Enter a page name for this web login. The web login 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.
Address:	securelogin arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default Select a security option to apply to the web login process.
Dynamic Address:	□ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses. The address above will be used whenever the parameter is not available or fails.

When configuring a Web Login Page in ClearPass Guest, the information shown is displayed.
What is the Address field value 'securelogin.arubanetworks.com' used for?

A. for ClearPass to send a TACACS+ request to the NAD

B. for appending to the Web Login URL, before the page name

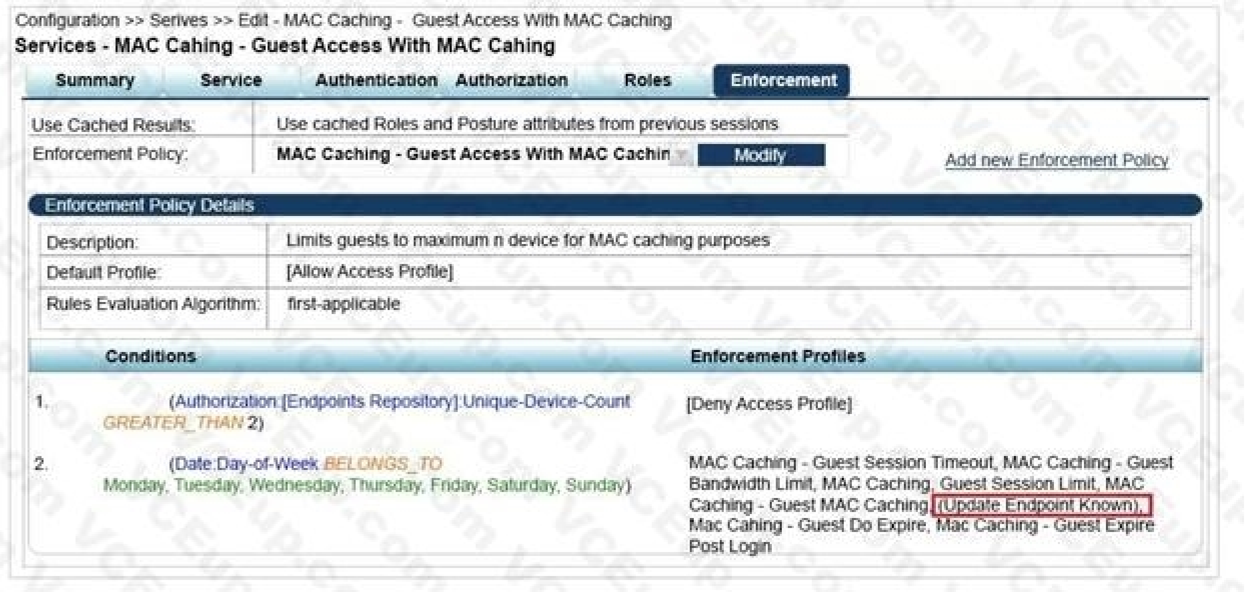
C. for the client to POST the user credentials to the NAD

D. for ClearPass to send a RADIUS request to the NAD

E. for appending to the Web Login URL, after the page name.

Correct Answer: C
Section:

QUESTION 20
Refer to the exhibit.



Configuration >> Serives >> Edit - MAC Caching - Guest Access With MAC Caching

Services - MAC Cahing - Guest Access With MAC Cahing

Use Cached Results:	Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	MAC Caching - Guest Access With MAC Cachin

Enforcement Policy Details

Description:	Limits guests to maximum n device for MAC caching purposes
Default Profile:	[Allow Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 2)	[Deny Access Profile]
2.	(Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	MAC Caching - Guest Session Timeout, MAC Caching - Guest Bandwidth Limit, MAC Caching, Guest Session Limit, MAC Caching - Guest MAC Caching, (Update Endpoint Known), Mac Cahing - Guest Do Expire, Mac Caching - Guest Expire Post Login

A guest connects to the Guest SSID and authenticates successfully using the guest.php web login page.
Based on the MAC Caching service information shown, which statement about the guests' MAC address is accurate?

A. It will be visible in the Guest User Repository with Unknown Status
B. It will be deleted from the Endpoint table.
C. It will be visible in the Guest User Repository with Known Status.
D. It will be visible in the Endpoints table with Known Status.
E. It will be visible in the Endpoints table with Unknown Status.

Correct Answer: D
Section:

QUESTION 21
A university wants to deploy ClearPass with the Guest module. The university has two types that need to use web login authentication. The first type of users are students whose accounts are in an Active Directory server. The second type of users are friends of students who need to self-register to access the network.
How should the service be set up in the Policy Manager for this network?

A. Guest User Repository and Active Directory server both as authentication sources
B. Active Directory server as the authentication source, and Guest User Repository as the authorization source
C. Guest User Repository as the authentication source, and Guest User Repository and Active Directory server as authorization sources
D. Either the Guest User Repository or Active Directory server should be the single authentication source
E. Guest User Repository as the authentication source and the Active Directory server as the authorization source

Correct Answer: A
Section:

QUESTION 22
An administrator enabled the Pre-auth check for their guest self-registration.
At what stage in the registration process in this check performed?

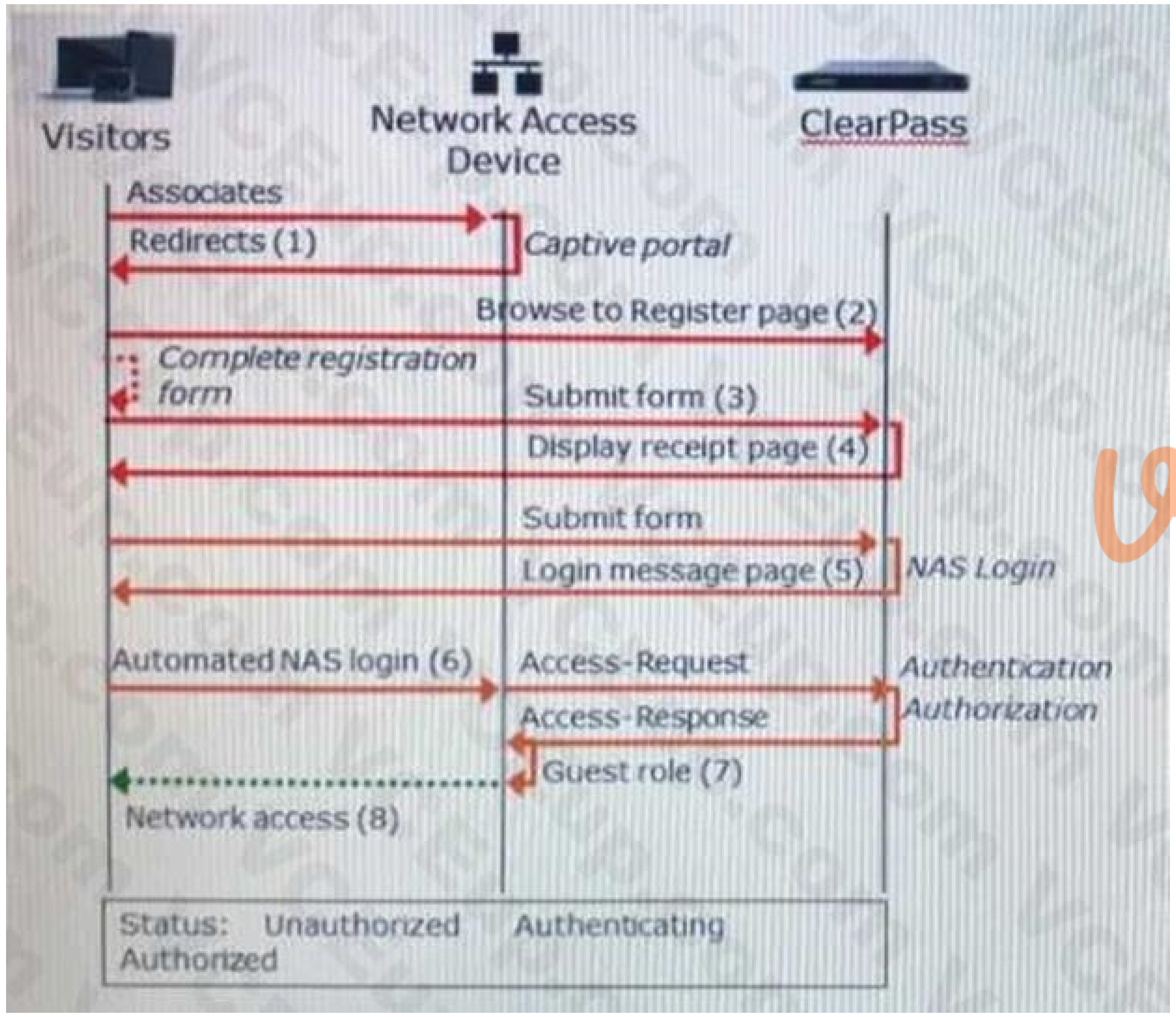
A. after the user clicks the login button and after the NAD sends an authentication request
B. after the user self-registers but before the user logs in
C. after the user clicks the login button but before the NAD sends an authentication request

D. when a user is re-authenticating to the network

E. before the user self-registers

Correct Answer: C
Section:
Explanation:
The Onboard template is designed for configuration that allows to perform checks before allowing Onboard provisioning for Bring Your Own Device (BYOD) use-cases. This service creates an Onboard Pre-Auth service to check the user's credentials before starting the device provisioning process. This also creates an authorization service that checks whether a user's device can be provisioned using Onboard.

QUESTION 23
Refer to the exhibit.



Based on the guest Self-Registration with Sponsor Approval workflow shown, at which stage is an email request sent to the sponsor?

A. after 'Guest Role (7)'

B. after 'Login Message page (5)'

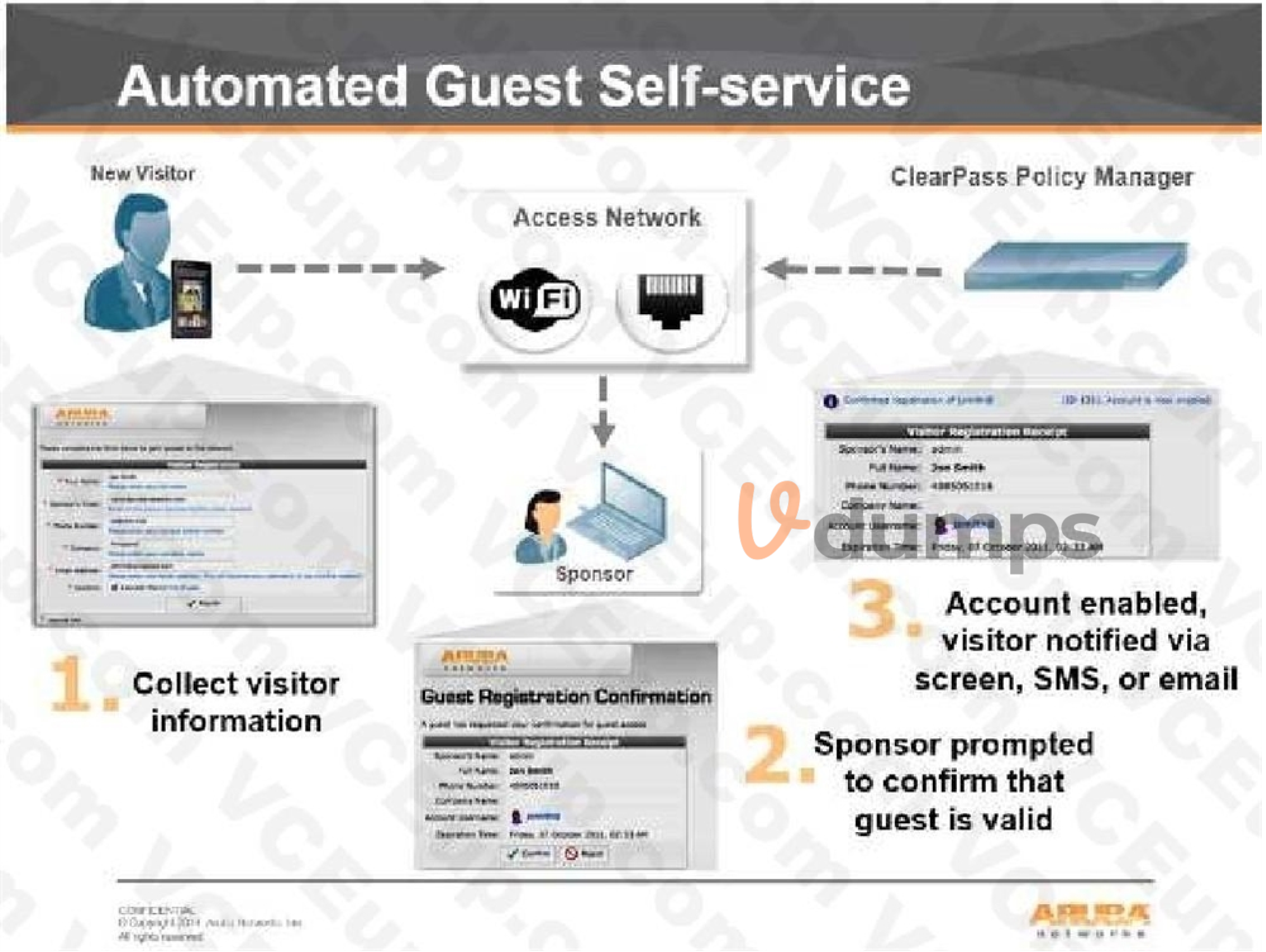
C. after 'Submit form (3)'

D. after 'Automated NAS login (6)'

E. after 'Redirects (1)'

Correct Answer: C
Section:

Explanation:
There's the Self Service part of provisioning one's information.
Then the sponsor/operator part to confirm that guest is valid.
Then the enablement via the sponsor/operator clicking 'confirm'.



Automated Guest Self-service

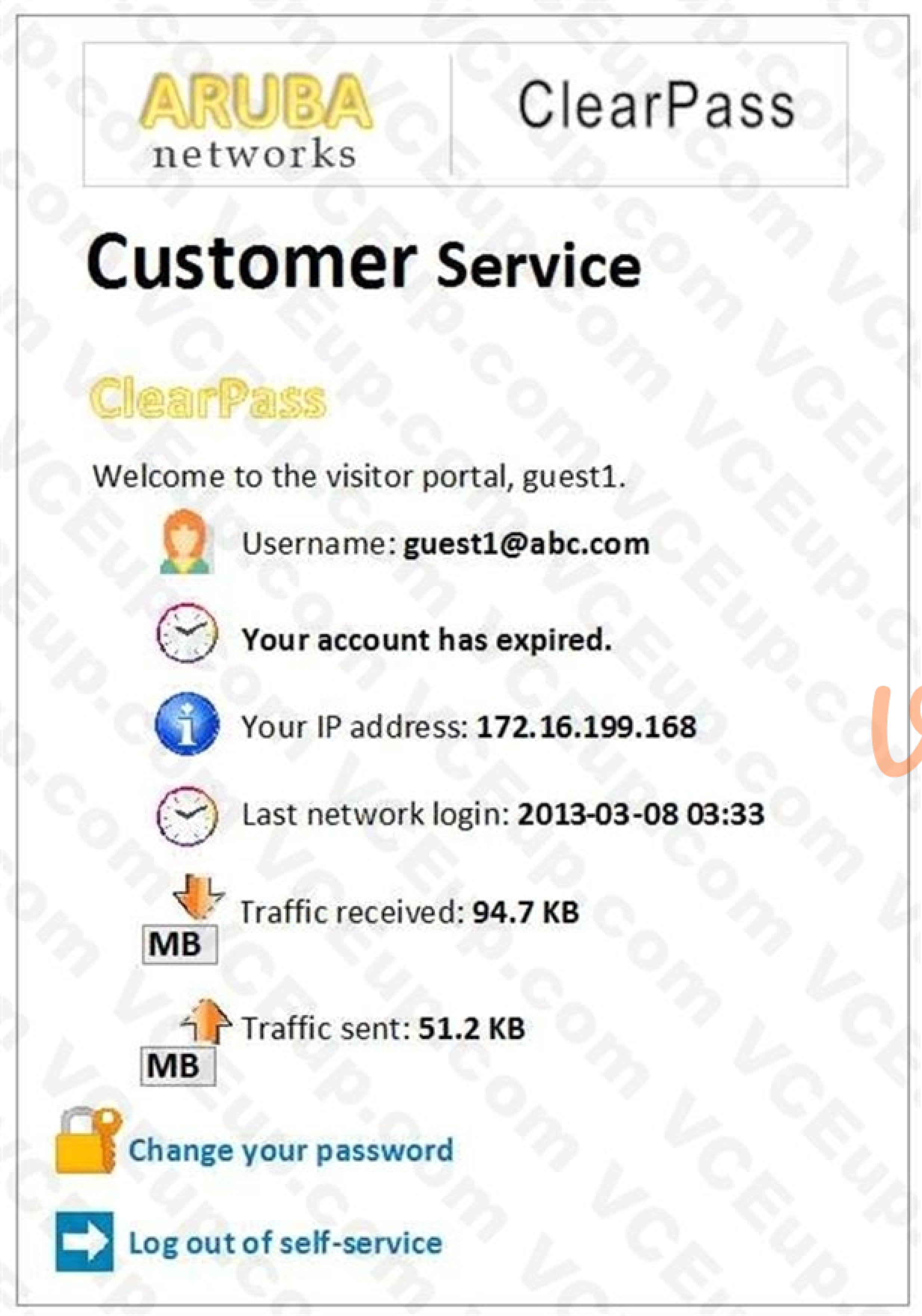
1. Collect visitor information

2. Sponsor prompted to confirm that guest is valid

3. Account enabled, visitor notified via screen, SMS, or email

Reference: https://community.arubanetworks.com/t5/Security/Guest-Captive-Portal-sponsorapproval-architecture/td-p/267625

QUESTION 24
Refer to the exhibit.



ARUBA networks | ClearPass

Customer Service

ClearPass

Welcome to the visitor portal, guest1.

Username: **guest1@abc.com**

Your account has expired.

Your IP address: **172.16.199.168**

Last network login: **2013-03-08 03:33**

Traffic received: **94.7 KB**

MB

Traffic sent: **51.2 KB**

MB

Change your password

Log out of self-service

A user logged in to the Self-Service Portal as shown.
What do the traffic received and sent statistics present?

A. These show the total amount of traffic the guest transmitted, as seen through RADIUS CoA packets from the NAD to ClearPass.

B. These show the total amount of traffic the NAD transmitted to ClearPass, as seen through RADIUS accounting messages from the NAD to ClearPass.

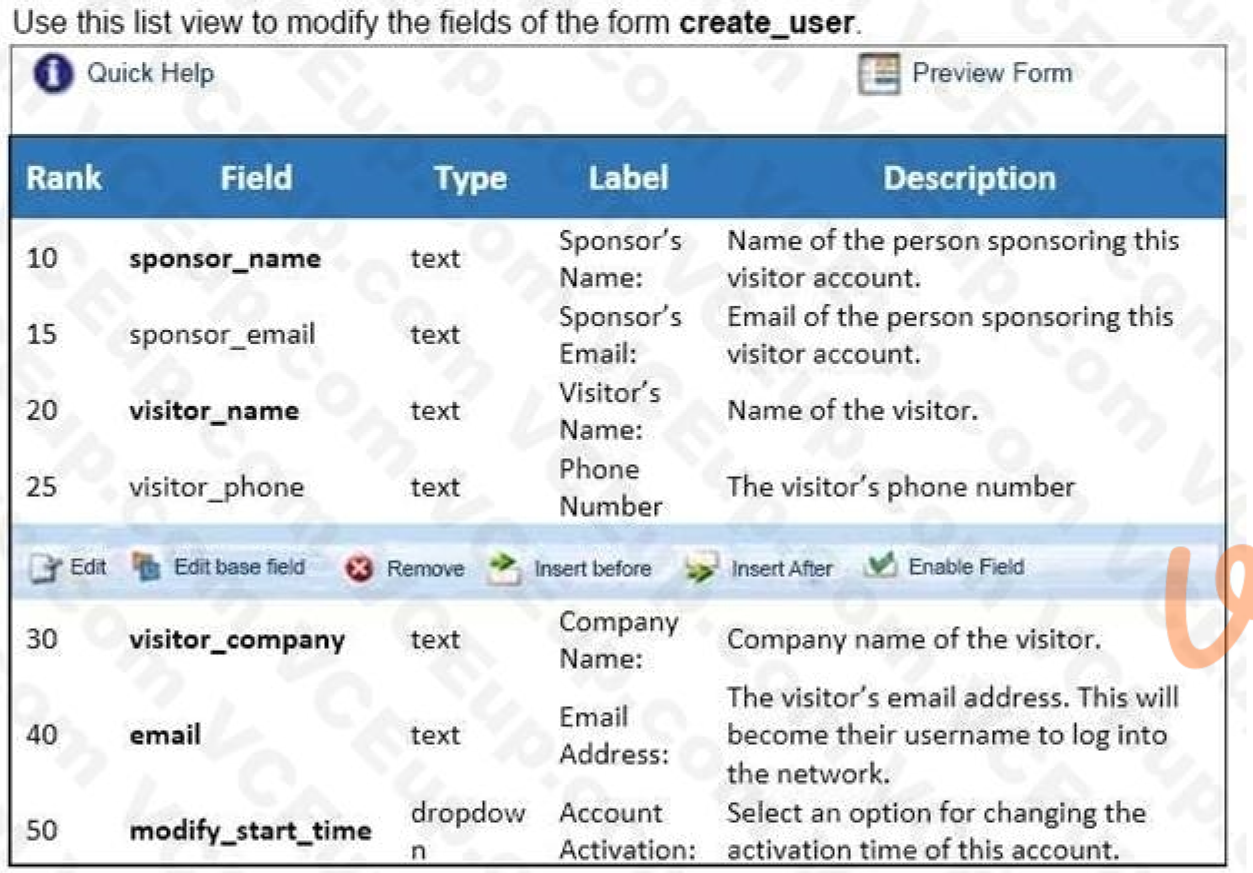
C. These show the total amount of traffic the guest transmitted after account expiration, as seen through RADIUS accounting messages sent from the NAD to ClearPass.

D. These show the total amount of traffic the guest transmitted, as seen through RADIUS CoA packets from the client to ClearPass.

E. These show the total amount of traffic the guest transmitted, as seen through RADIUS accounting messages sent from the NAD to ClearPass.

Correct Answer: E
Section:

QUESTION 25
Refer to the exhibit.



Use this list view to modify the fields of the form **create_user**.

Rank	Field	Type	Label	Description
10	**sponsor_name**	text	Sponsor's Name:	Name of the person sponsoring this visitor account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this visitor account.
20	**visitor_name**	text	Visitor's Name:	Name of the visitor.
25	visitor_phone	text	Phone Number	The visitor's phone number
30	**visitor_company**	text	Company Name:	Company name of the visitor.
40	**email**	text	Email Address:	The visitor's email address. This will become their username to log into the network.
50	**modify_start_time**	dropdown	Account Activation:	Select an option for changing the activation time of this account.

Based on the configuration of the create_user form shown, which statement accurately describes the status?

A. The email field will be visible to guest users when they access the web login page.

B. The visitor_company field will be visible to operators creating the account.

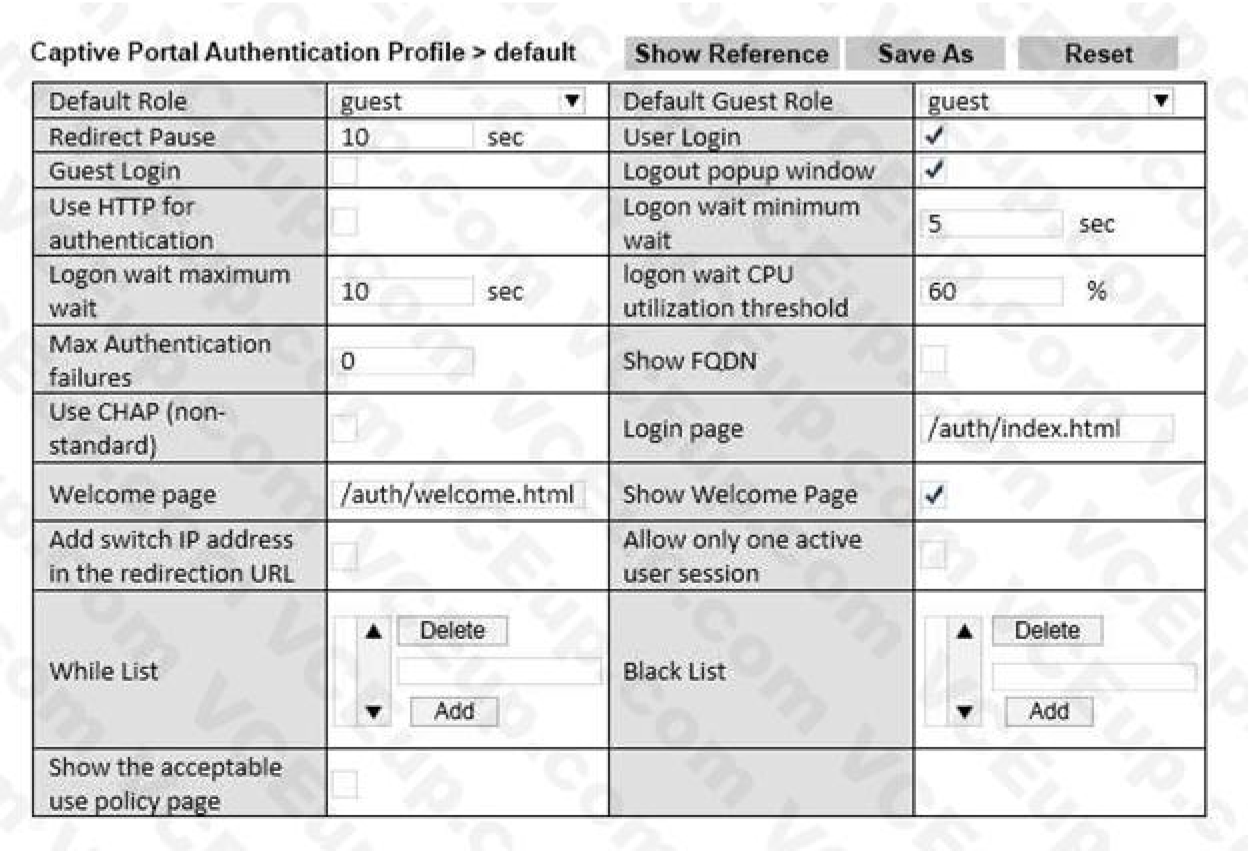
C. The visitor_company field will be visible to the guest users when they access the web login page.

D. The visitor_phone field will be visible to the guest users in the web login page.

E. The visitor_phone field will be visible to operators creating the account.

Correct Answer: A
Section:
Explanation:
Reference: https://community.arubanetworks.com/t5/AAA-NAC-Guest-Access-BYOD/expiretimezone-field-is-not-showing-up-on-the-create-user-form/ta-p/250230

QUESTION 26
Refer to the exhibit.



Captive Portal Authentication Profile > default

Default Role	guest ▼	Default Guest Role	guest ▼
Redirect Pause	10 sec	User Login	✓
Guest Login	□	Logout popup window	✓
Use HTTP for authentication	□	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	□
Use CHAP (non-standard)	□	Login page	/auth/index.html
Welcome page	/auth/welcome.html	Show Welcome Page	✓
Add switch IP address in the redirection URL	□	Allow only one active user session	□
While List	▲ Delete ▼ Add	Black List	▲ Delete ▼ Add
Show the acceptable use policy page	□		

Based on the information shown, which field in the Captive Portal Authentication profile should be changed so that guest users are redirected to a page on ClearPass when they connect to the Guest SSID?

A. both Login and Welcome Page

B. Default Role

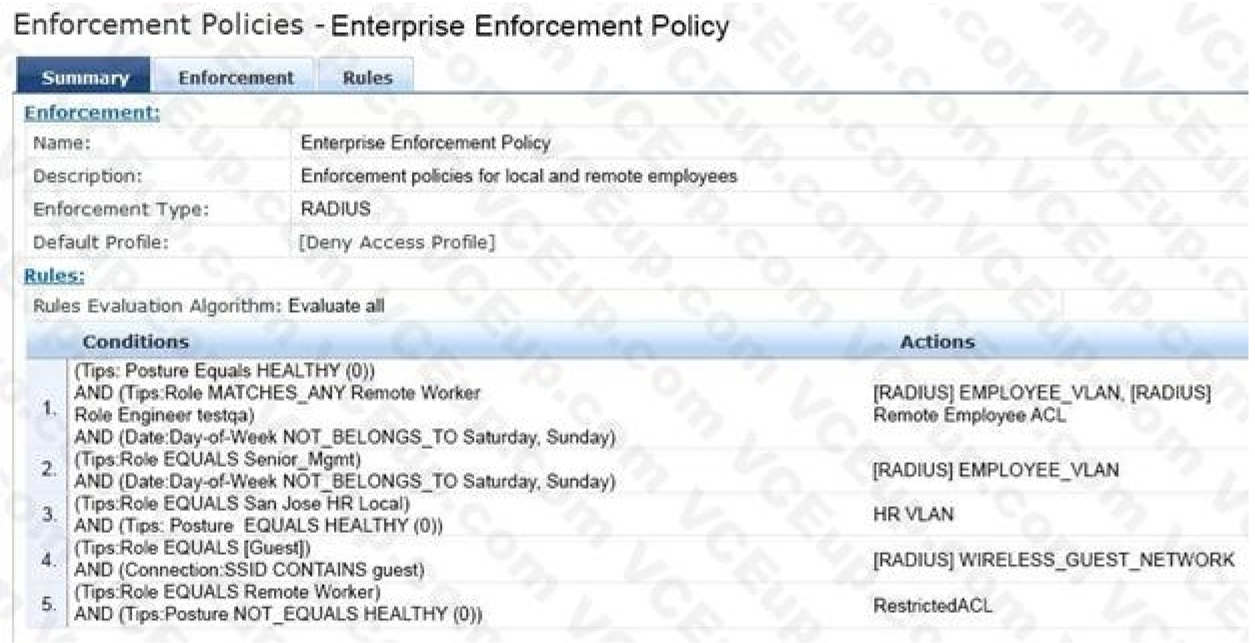
C. Welcome Page

D. Default Guest Role

E. Login Page

Correct Answer: E
Section:
Explanation:
The Login page is the URL of the page that appears for the user logon. This can be set to any URL.
The Welcome page is the URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.
Reference: http://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Cap tive_Portal/Captive_Portal_Authentic.htm

QUESTION 27
Refer to the exhibit.



Enforcement Policies - Enterprise Enforcement Policy

Enforcement:

Name:	Enterprise Enforcement Policy
Description:	Enforcement policies for local and remote employees
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm: Evaluate all

	Conditions	Actions
1.	(Tips: Posture Equals HEALTHY (0)) AND (Tips:Role MATCHES_ANY Remote Worker Role Engineer testqa) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN, [RADIUS] Remote Employee ACL
2.	(Tips:Role EQUALS Senior_Mgmt) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN
3.	(Tips:Role EQUALS San Jose HR Local) AND (Tips: Posture EQUALS HEALTHY (0))	HR VLAN
4.	(Tips:Role EQUALS [Guest]) AND (Connection:SSID CONTAINS guest)	[RADIUS] WIRELESS_GUEST_NETWORK
5.	(Tips:Role EQUALS Remote Worker) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	RestrictedACL

Based on the Enforcement Policy configuration shown, when a user with Role Remote Worker connects to the network and the posture token assigned is quarantine, which Enforcement Profile will be applied?

A. RestrictedACL

B. Remote Employee ACL

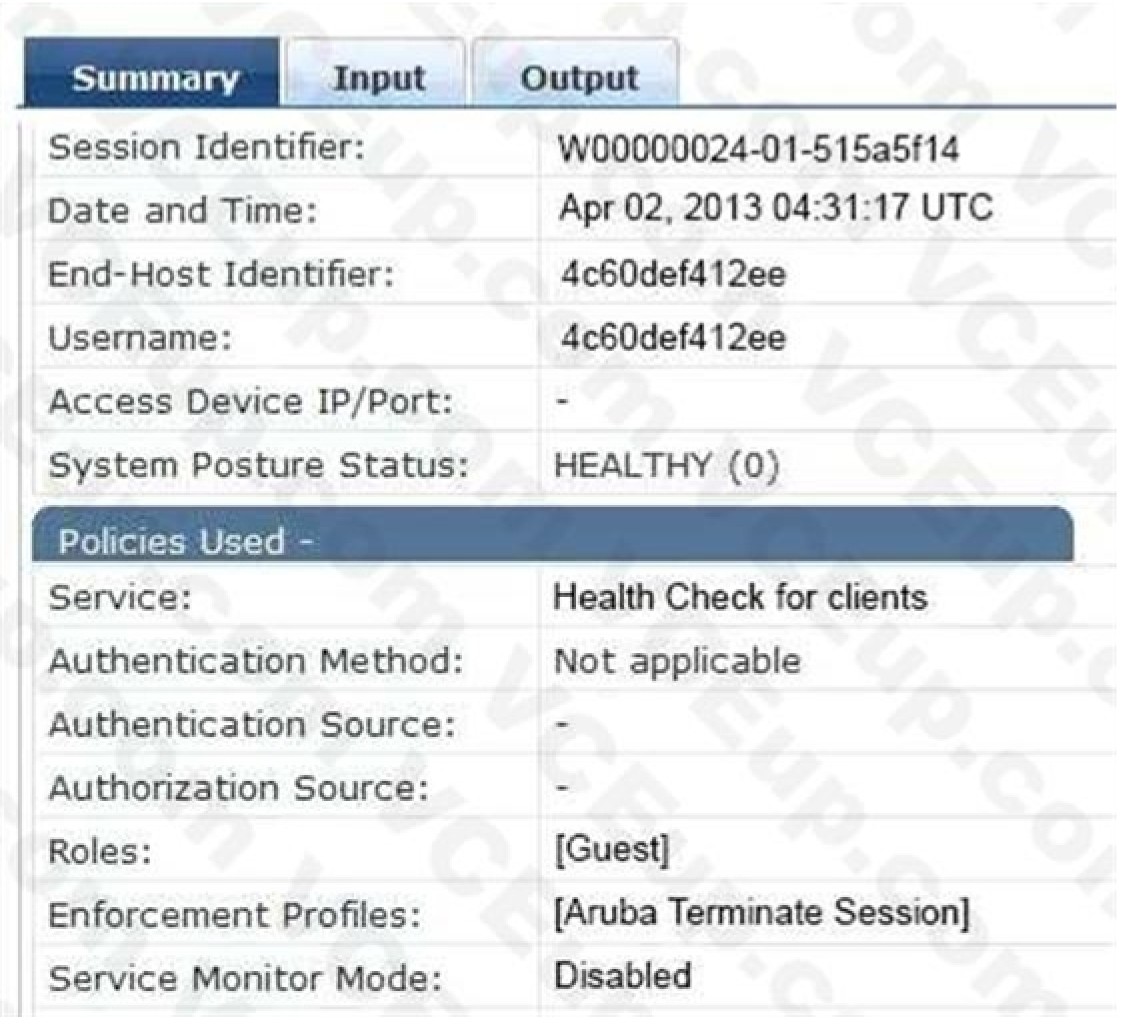
C. [Deny Access Profile]

D. EMPLOYEE_VLAN

E. HR VLAN

Correct Answer: B
Section:
Explanation:
The first rule will match, and the Remote Employee ACL will be used.

QUESTION 28
Refer to the exhibit.



Session Identifier:	W00000024-01-515a5f14
Date and Time:	Apr 02, 2013 04:31:17 UTC
End-Host Identifier:	4c60def412ee
Username:	4c60def412ee
Access Device IP/Port:	-
System Posture Status:	HEALTHY (0)
Policies Used -	
Service:	Health Check for clients
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	[Guest]
Enforcement Profiles:	[Aruba Terminate Session]
Service Monitor Mode:	Disabled

Based on the Access Tracker output for the user shown, which statement describes the status?

A. The Aruba Terminate Session enforcement profile as applied because the posture check failed.
B. A Healthy Posture Token was sent to the Policy Manager.
C. A RADIUS-Access-Accept message is sent back to the Network Access Device.
D. The authentication method used is EAP-PEAP.
E. A NAP agent was used to obtain the posture token for the user.

Correct Answer: B
Section:
Explanation:
We see System Posture Status: HEALTHY(0)
End systems that pass all SHV tests receive a Healthy Posture Token, if they fail a single test they receive a Quarantine Posture Token.
Reference: CLEARPASS ONGUARD CONFIGURATION GUIDE (July 2015), page 13
https://community.arubanetworks.com/aruba/attachments/aruba/aaa-nac-guest-accessbyod/21122/1/OnGuard%20config%20Tech%20Note%20v1.pdf

QUESTION 29
Why can the Onguard posture check not be performed during 802.1x authentication?

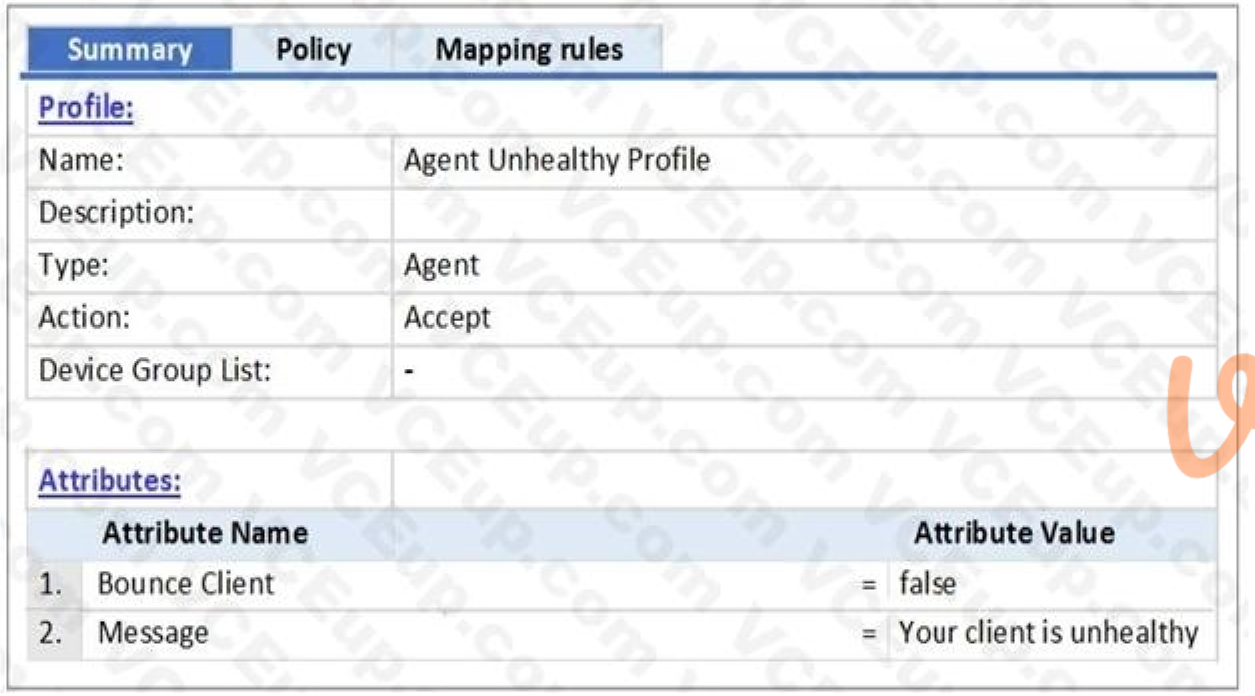
A. Health Checks cannot be used with 802.1x.
B. Onguard uses RADIUS, so an additional service must be created.
C. Onguard uses HTTPS, so an additional service must be created.

D. Onguard uses TACACS, so an additional service must be created.

E. 802.1x is already secure, so Onguard is not needed.

Correct Answer: C
Section:
Explanation:
OnGuard uses HTTPS to send posture information to the ClearPass appliance. For OnGuard to use
HTTPS, it must have access to the network. If a customer requires 802.1x authentication on the wiredswitch, a separate 802.1x authentication must be used prior to the OnGuard posture check. In thisexample, an 802.1x PEAP-EAP-
MSCHAPv2 authentication is completed first. A separate WebAuthservice must be setup with posture checks to use the OnGuard agent.
Reference: MAC Authentication and OnGuard Posture Enforcement using Dell WSeries ClearPass and Dell Networking Switches (August 2013), page 21

QUESTION 30
Refer to the exhibit.



Profile:

Name:	Agent Unhealthy Profile
Description:	
Type:	Agent
Action:	Accept
Device Group List:	-

Attributes:

	Attribute Name		Attribute Value
1.	Bounce Client	=	false
2.	Message	=	Your client is unhealthy

Based on the Enforcement Profile configuration shown, which statement accurately describes what is sent?

A. A limited access VLAN value is sent to the Network Access Device.

B. An unhealthy role value is sent to the Network Access Device.

C. A message is sent to the Onguard Agent on the client device.

D. A RADIUS CoA message is sent to bounce the client.

E. A RADIUS access-accept message is sent to the Controller

Correct Answer: C
Section:
Explanation:
The OnGuard Agent enforcement policy retrieves the posture token. If the token is HEALTHY it returns a healthy message to the agent and bounces the session. If the token is UNHEALTHY it returns an unhealthy message to the agent and bounces the session.
Reference: CLEARPASS ONGUARD CONFIGURATION GUIDE (July 2015), page 27

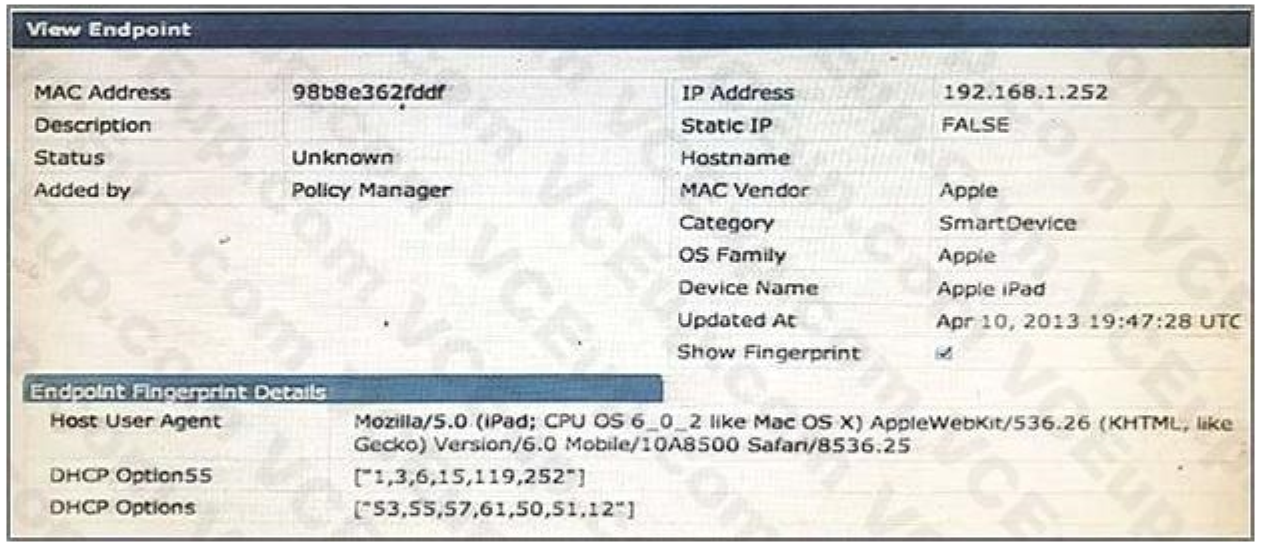
QUESTION 31
A ClearPass administrator wants to make Enforcement decisions during 802.1x authentication based on a client's Onguard posture token.

Which Enforcement profile should be used on the health check service?

A. RADIUS CoA
B. Quarantine VLAN
C. Full Access VLAN
D. RADIUS Accept
E. RADIUS Reject

Correct Answer: A
Section:
Explanation:
The Health Check Service requires a profile to terminate the session so that the RADIUS 802.1X authentication Service can use the posture token in a new authentication routine. The terminate session profile will utilize the Change of
Authorization feature to force a re-authentication.
See step 6) below.
Navigate to the list of Enforcement Profiles by selecting, Configuration > Enforcement > Profiles.
2. Click the + Add link in the upper right hand corner.
3. From the Template dropdown menu, choose RADIUS Change of Authorization (CoA).
4. Name the policy.
This example uses Dell Terminate Session as the profile name.
5. Leave all the other settings as default, and click Next > to move to the Attributes tab.
6. On the dropdown menu for Select RADIUS CoA Template, choose IETF-Terminate-Session-IETF.
7. Click Next > and review the Summary tab (Figure 22).
8. Click Save.
Reference: ClearPass NAC and Posture Assessment for Campus Networks Configuring ClearPass OnGuard, Switching, and Wireless (v1.0) (September 2015), page 22 http://en.community.dell.com/cfs-file/__key/telligent-evolution-components-attachments/13-4629- 00-00-20-44-16-18/
ClearPass-NAC-and-Posture-Assessment-for-Campus- Networks.pdf?forcedownload=true

QUESTION 32
Refer to the exhibit.



View Endpoint

MAC Address	98b8e362fddf	IP Address	192.168.1.252
Description		Static IP	FALSE
Status	Unknown	Hostname	
Added by	Policy Manager	MAC Vendor	Apple
		Category	SmartDevice
		OS Family	Apple
		Device Name	Apple iPad
		Updated At	Apr 10, 2013 19:47:28 UTC
		Show Fingerprint	☑

Endpoint Fingerprint Details

Host User Agent	Mozilla/5.0 (iPad; CPU OS 6_0_2 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A8500 Safari/8536.25
DHCP Option55	["1,3,6,15,119,252"]
DHCP Options	["53,55,57,61,50,51,12"]

Based on the Endpoint information shown, which collectors were used to profile the device as Apple iPad? (Select two.)

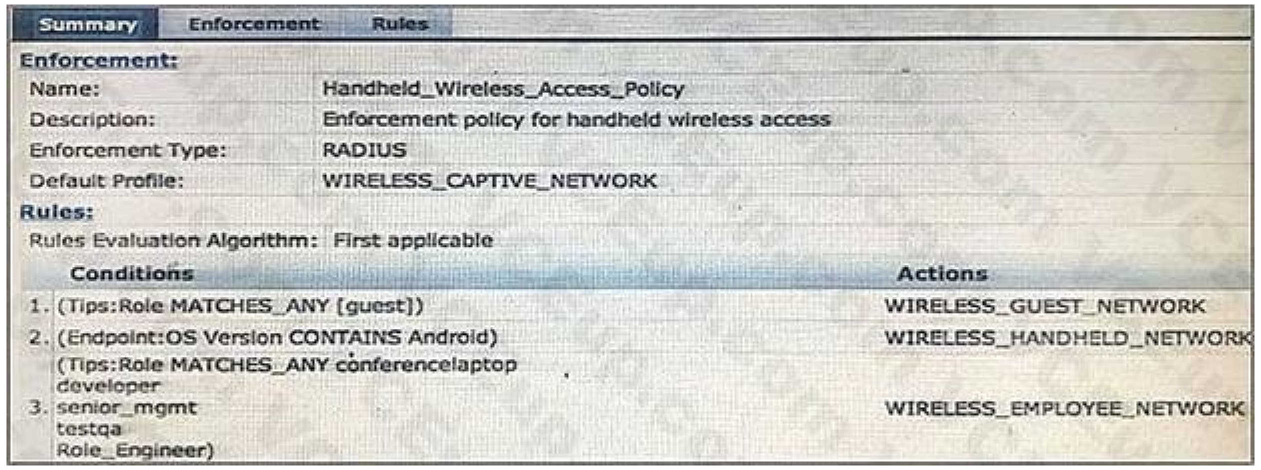
A. HTTP User-Agent
B. SNMP
C. DHCP fingerprinting

D. SmartDevice

E. Onguard Agent

Correct Answer: A, C
Section:
Explanation:
HTTP User-Agent
In some cases, DHCP fingerprints alone cannot fully classify a device. A common example is the Apple family of smart devices; DHCP fingerprints cannot distinguish between an Apple iPad and an iPhone. In these scenarios, User-Agent strings sent by browsers in the HTTP protocol are useful to further refine classification results.
User-Agent strings are collected from:
* ClearPass Guest
* ClearPass Onboard
* Aruba controller through IF-MAP interface
Note: Collectors are network elements that provide data to profile endpoints.
The following collectors send endpoint attributes to Profile:
* DHCP
DHCP snooping
Span ports
* ClearPass Onboard
* HTTP User-Agent
*MAC OUI – Acquired via various auth mechanisms such as 802.1X, MAC auth, etc.
* ActiveSync plugin
* CPPM OnGuard
*SNMP
* Subnet Scanner
* IF-MAP
* Cisco Device Sensor (Radius Accounting)
* MDM
Reference: Tech Note: ClearPass Profiling (2014), page 11
https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf

QUESTION 33
Refer to the exhibit.



Enforcement:

Name:	Handheld_Wireless_Access_Policy
Description:	Enforcement policy for handheld wireless access
Enforcement Type:	RADIUS
Default Profile:	WIRELESS_CAPTIVE_NETWORK

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role MATCHES_ANY (guest))	WIRELESS_GUEST_NETWORK
2.	(Endpoint:OS Version CONTAINS Android)	WIRELESS_HANDHELD_NETWORK
3.	(Tips:Role MATCHES_ANY conferencelaptop developer senior_mgmt testqa Role_Engineer)	WIRELESS_EMPLOYEE_NETWORK

A user who is tagged with the ClearPass roles of Role_Engineer and developer, but not testqa, connects to the network with a corporate Windows laptop.
Which Enforcement Profile is applied?

A. WIRELESS_GUEST_NETWORK

B. WIRELESS_CAPTIVE_NETWORK

C. WIRELESS_HANDHELD_NETWORK
D. Deny Access
E. WIRELESS_EMPLOYEE_NETWORK

Correct Answer: E
Section:
Explanation:
MATCHES_ANY: For list data types, true if any of the run-time values in the list match one of the configured values.
Example: Tips:Role MATCHES_ANY HR,ENG,FINANCE
Reference: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_User Guide/Rules/Operators.htm

QUESTION 34
An SNMP probe is sent from ClearPass to a network access device, but ClearPass is unable to obtain profiling information.
What are likely causes? (Select three.)

A. Only SNMP read has been configured but SNMP write is needed for profiling information.
B. An external firewall is blocking SNMP traffic.
C. SNMP is not enabled on the NAD.
D. SNMP community string in the ClearPass and NAD configuration is mismatched.
E. SNMP probing is not supported between ClearPass and NADs.

Correct Answer: B, C, D
Section:
Explanation:
Verify firewall port 162 (default) is open between AMP and the controller.
SNMP must be enabled on the NAD.
The community string that ClearPass is using to access the NAD might be wrong.
Reference: https://community.arubanetworks.com/t5/Monitoring-Management-Location/SNMPGet-Failed-quot-error-message/ta-p/169774

QUESTION 35
Which database in the Policy Manager contains the device attributes derived by profiling?

A. Endpoints Repository
B. Client Repository
C. Local Users Repository
D. Onboard Devices Repository
E. Guest User Repository

Correct Answer: A
Section:
Explanation:
Configure [Endpoints Repository] as Authorization Source. Endpoint profile attributes derived by Profile are available through the '[Endpoint Repository]' authorization source.
These attributes can be used in role-mapping or enforcement policies to control network access. Available attributes are:
Authorization:[Endpoints Repository]:MAC Vendor
Authorization:[Endpoints Repository]:Category
Authorization:[Endpoints Repository]:OS Family
Authorization:[Endpoints Repository]:Name
Reference: ClearPass Profiling TechNote (2014), page 29

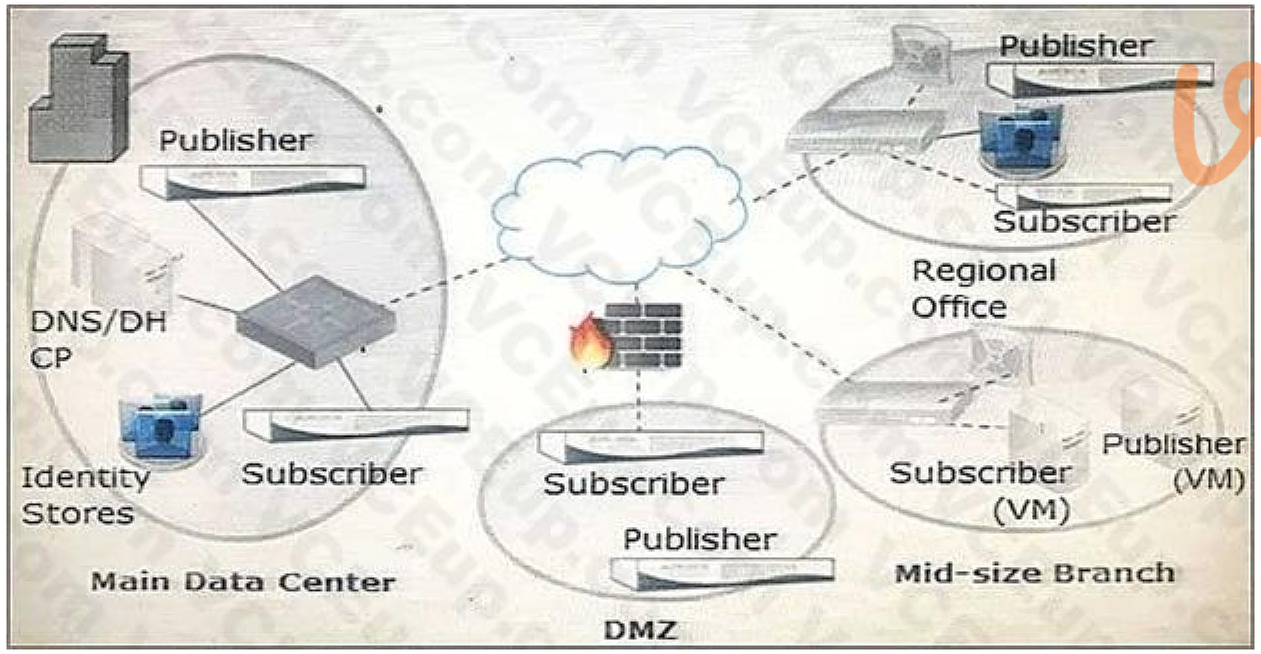
https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf

QUESTION 36
When a third party Mobile Device Management server is integrated with ClearPass, where is the endpoint information from the MDM server stored in ClearPass?

A. Endpoints repository
B. Onboard Device repository
C. MDM repository
D. Guest User repository
E. Local User repository

Correct Answer: A
Section:
Explanation:
A service running in CPPM periodically polls MDM servers using their exposed APIs. Device attributes obtained from MDM are added as endpoint tags. Profiler related attributes are send to profiler which uses these attributes to derive final profile.
Reference: ClearPass Profiling TechNote (2014), page 23
https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf

QUESTION 37
Refer to the exhibit.



Based on the network topology diagram shown, how many clusters are needed for this deployment?

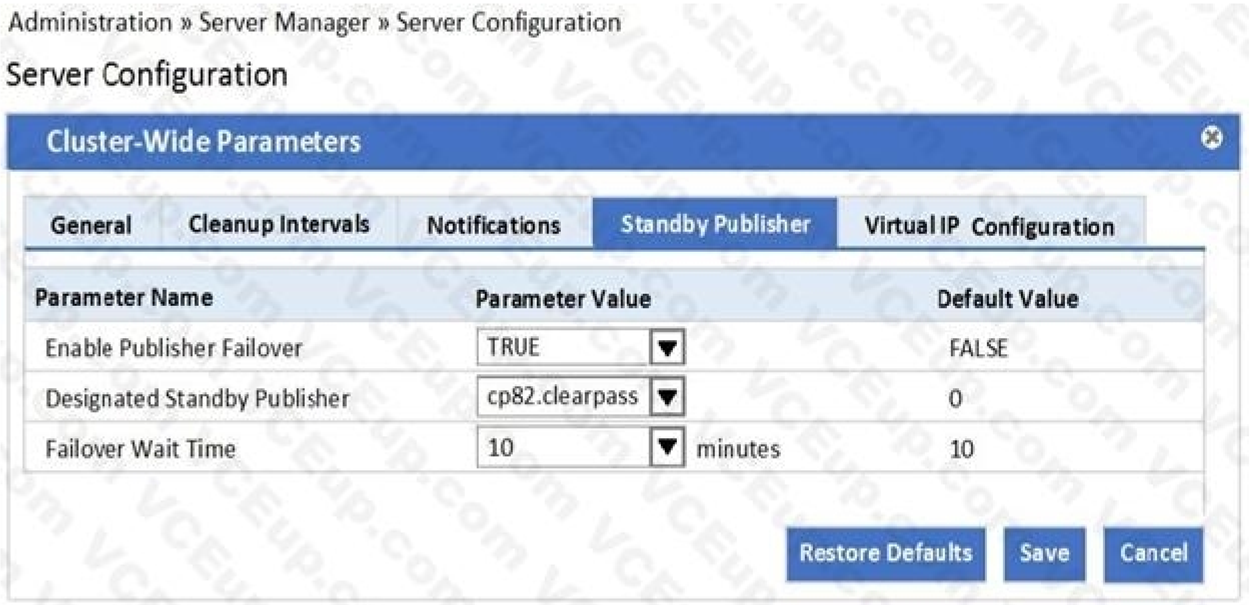
A. 1
B. 2
C. 3
D. 4
E. 8

Correct Answer: D
Section:
Explanation:

Reference: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster %20Deployment/Design_guidelines.htm

QUESTION 38

Refer to the exhibit.



Parameter Name	Parameter Value	Default Value
Enable Publisher Failover	TRUE	FALSE
Designated Standby Publisher	cp82.clearpass	0
Failover Wait Time	10 minutes	10

Which statements accurately describe the cp82 ClearPass node? (Select two.)

A. It becomes the Publisher when the primary Publisher fails.

B. It operates as a Publisher in the same cluster as the primary Publisher when the primary is active.

C. It operates as a Publisher in a separate cluster when the Publisher is active.

D. It operates as a Subscriber when the Publisher is active.

E. It stays as a Subscriber when the Publisher fails.

Correct Answer: A, D

Section:

Explanation:

ClearPass Policy Manager allows you to designate one of the subscriber nodes in a cluster to be the Standby Publisher, thereby providing for that subscriber node to be automatically promoted to active Publisher status in the event that the

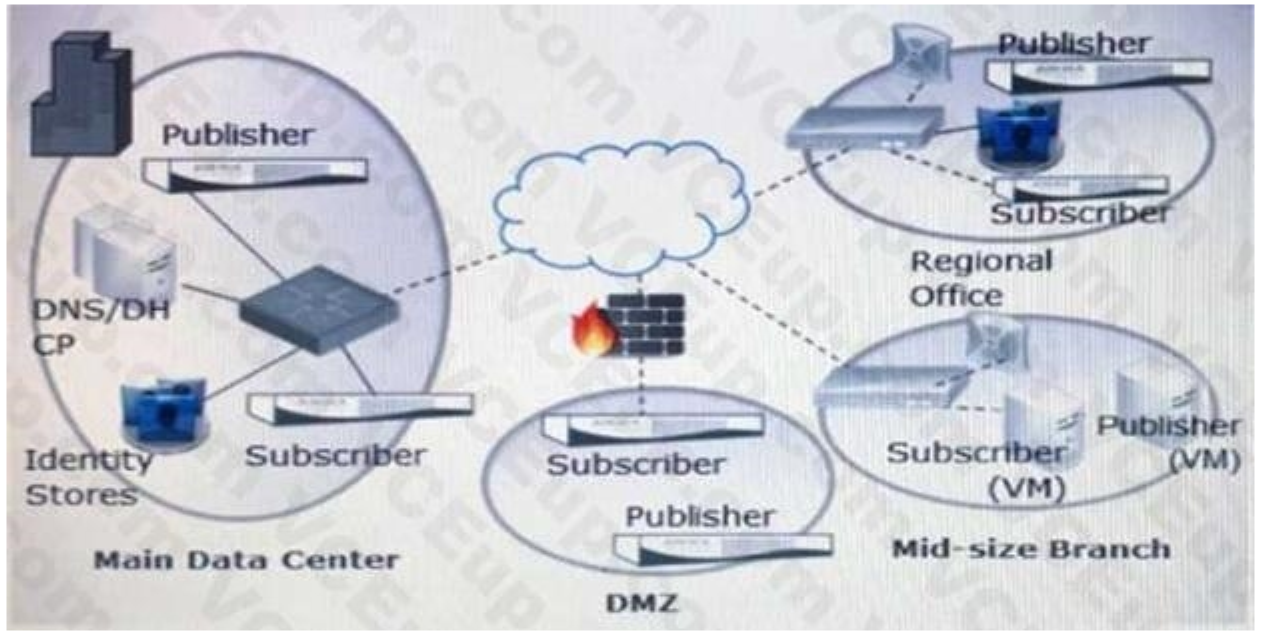
Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum.

When a Publisher failure is detected, the designated subscriber node is promoted to active Publisher status.

Reference: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster %20Deployment/Standby_publisher.htm

QUESTION 39

Refer to the exhibit.



A customer wants to enable Publisher redundancy.
Based on the network topology diagram shown, which node should the network administrator configure as the standby Publisher for the Publisher in the main data center?

A. Subscriber in the main data center
B. Publisher in the regional office
C. Any of the other three Publishers
D. Publisher in the mid-size branch
E. Publisher in the DMZ

Correct Answer: A
Section:
Explanation:
ClearPass Policy Manager allows you to designate one of the subscriber nodes in a cluster to be the Standby Publisher, thereby providing for that subscriber node to be automatically promoted to active Publisher status in the event that the
Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum.
Reference: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster %20Deployment/Standby_publisher.htm

QUESTION 40
A customer wants to implement Virtual IP redundancy, such that in case of a ClearPass server outage, 802.1x authentications will not be interrupted. The administrator has enabled a single Virtual IP address on two ClearPass servers.
Which statements accurately describe next steps? (Select two.)

A. The NAD should be configured with the primary node IP address for RADIUS authentication on the 802.1x network.
B. A new Virtual IP address should be created for each NAD.
C. Both the primary and secondary nodes will respond to authentication requests sent to the Virtual IP address when the primary node is active.
D. The primary node will respond to authentication requests sent to the Virtual IP address when the primary node is active.
E. The NAD should be configured with the Virtual IP address for RADIUS authentications on the 802.1x network.

Correct Answer: D, E
Section:
Explanation:
In an Aruba network, APs are controlled by a controller. The APs tunnel all data to the controller for processing, including encryption/decryption and bridging/forwarding data. Local controller redundancy provides APs with

failover to a backup controller if a controller becomes unavailable.
Local controller redundancy is provided by running VRRP between a pair of controllers. The APs are then configured to connect to the "virtual-IP" configured for the VRRP instance.
Reference: http://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VRR P/Redundancy_Parameters.htm

QUESTION 41
ClearPass and a wired switch are configured for 802.1x authentication with RADIUS CoA (RFC 3576) on UDP port 3799. This port has been blocked by a firewall between the wired switch and ClearPass.
What will be the outcome of this state?

A. RADIUS Authentications will fail because the wired switch will not be able to reach the ClearPass server.
B. During RADIUS Authentication, certificate exchange between the wired switch and ClearPass will fail.
C. RADIUS Authentications will timeout because the wired switch will not be able to reach the ClearPass server.
D. RADIUS Authentication will succeed, but Post-Authentication Disconnect-Requests from ClearPass to the wired switch will not be delivered.
E. RADIUS Authentication will succeed, but RADIUS Access-Accept messages from ClearPass to the wired switch for Change of Role will not be delivered.

Correct Answer: D
Section:

QUESTION 42
Which statement accurately describes configuration of Data and Management ports on the ClearPass appliance? (Select two.)

A. Static IP addresses are only allowed on the management port.
B. Configuration of the data port is mandatory.
C. Configuration on the management port is mandatory.
D. Configuration of the data port if optional.
E. Configuration of the management port is optional.

Correct Answer: C, D
Section:
Explanation:
The Management port (ethernet 0) provides access for cluster administration and appliance maintenance using the WebUI, CLI, or internal cluster communication. This configuration is mandatory.
The configuration of the data port is optional. If this port is not configured, requests are redirected to the Management port.
Reference: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/1%20About %20ClearPass/Hardware_Appliance.htm

QUESTION 43
Which licenses are included in the built-in Starter kit for ClearPass?

A. 10 ClearPass Guest licenses, 10 ClearPass Onguard licenses and 10 ClearPass Onboard licenses
B. 25 ClearPass Profiler licenses
C. 25 ClearPass Enterprise licenses
D. 10 ClearPass Enterprise licenses
E. 25 ClearPass Redundancy licenses

Correct Answer: C
Section:
Explanation:
All CPPM's comes bundled with 25 Enterprise application licenses so you can test the functionality of the Applications as this license can be used for any of them.
Reference: http://community.arubanetworks.com/t5/Security/ClearPass-licensing-explained-August-MHC/td-p/195719

QUESTION 44

An employee provisions a personal smart phone using the Onboard process. In addition, the employee has a corporate laptop provided by IT that connects to the secure network.
How many licenses does the employee consume?

A. 1 Policy Manager license, 2 Guest Licenses
B. 2 Policy Manager licenses, 1 Onboard License
C. 1 Policy Manager license, 1 Onboard License
D. 1 Policy Manager license, 1 Guest License
E. 2 Policy Manager licenses, 2 Onboard Licenses

Correct Answer: B
Section:

QUESTION 45

A customer would like to deploy ClearPass with these requirements: every day, 100 employees need to authenticate with their corporate laptops using EAP-TLS every Friday, a meeting with business partners takes place and an additional 50 devices need to authenticate using Web Login Guest Authentication What should the customer do regarding licenses? (Select two.)

A. When counting policy manager licenses, include the additional 50 business partner devices.
B. When counting policy manager licenses, exclude the additional 50 business partner devices.
C. Purchase Onboard licenses.
D. Purchase guest licenses.
E. Purchase Onguard licenses.

Correct Answer: A, C
Section:

QUESTION 46

An employee authenticates using a corporate laptop and runs the persistent Onguard agent to send a health check back the Policy Manager. Based on the health of the device, a VLAN is assigned to the corporate laptop.
Which licenses are consumed in this scenario?

A. 1 Policy Manager license, 1 Onboard License
B. 2 Policy Manager licenses, 1 Onguard License
C. 1 Policy Manager license, 1 Profile License
D. 2 Policy Manager licenses, 2 Onguard licenses
E. 1 Policy Manager license, 1 Onguard License

Correct Answer: E
Section:

QUESTION 47

A customer would like to deploy ClearPass with these requirements: between 2000 to 3000 corporate users need to authenticate daily using EAP-TLS should allow for up to 1000 employee devices to be Onboarded should allow up to 100 guest users each day to authenticate using the web login feature What is the license mix that customer will need to purchase?

A. CP-HW-2k, 1000 Onboard, 100 Guest
B. CP-HW-500, 1000 Onboard, 100 Guest
C. CP-HW-5k, 2500 Enterprise

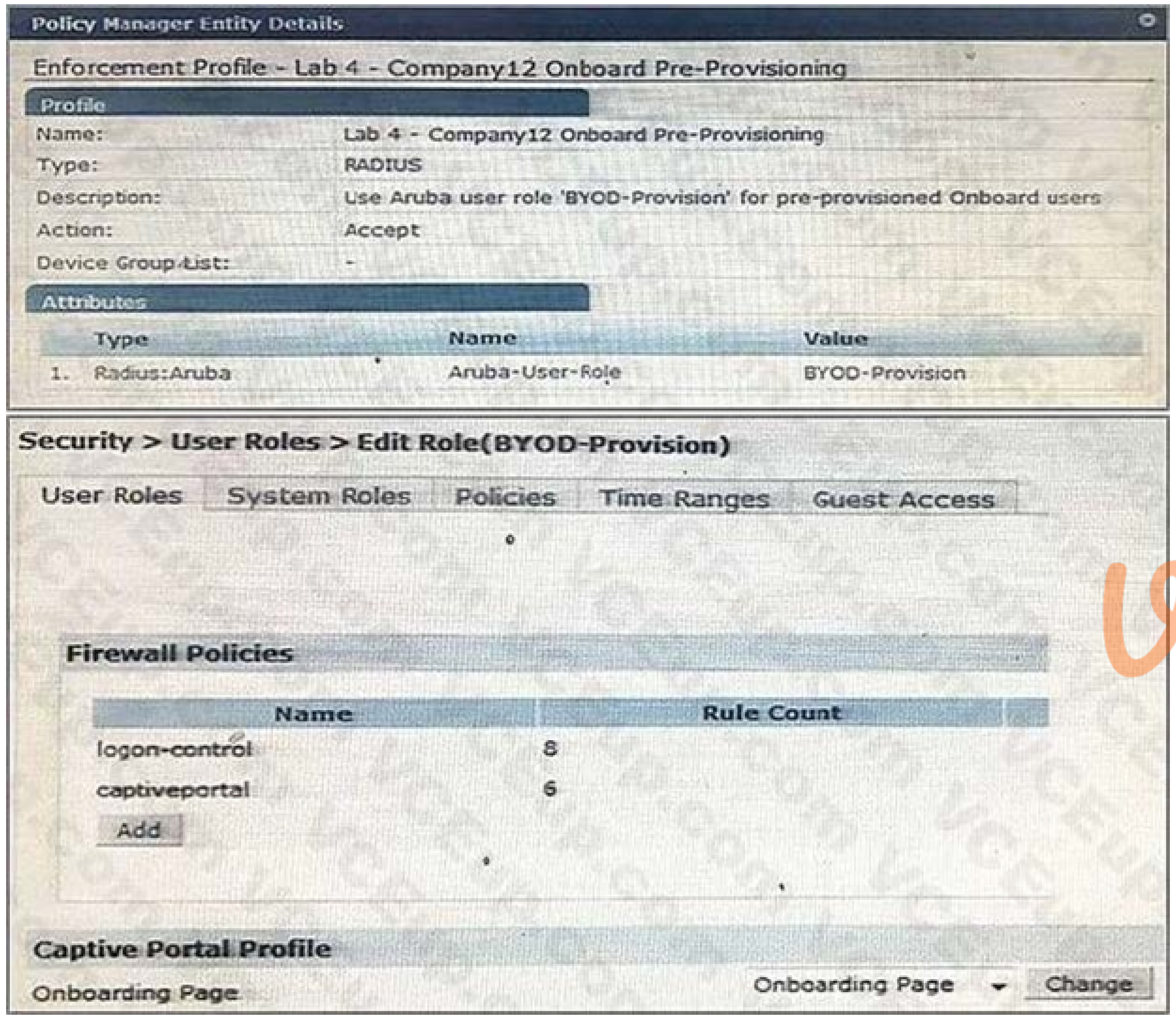
D. CP-HW-5k, 1000 Enterprise

E. CP-HW-5k, 100 Onboard, 100 Guest

Correct Answer: C
Section:

QUESTION 48

Refer to the exhibit.



Policy Manager Entity Details

Enforcement Profile - Lab 4 - Company12 Onboard Pre-Provisioning

Profile

Name:	Lab 4 - Company12 Onboard Pre-Provisioning
Type:	RADIUS
Description:	Use Aruba user role 'BYOD-Provision' for pre-provisioned Onboard users
Action:	Accept
Device Group List:	-

Attributes

	Type	Name	Value
1.	Radius:Aruba	Aruba-User-Role	BYOD-Provision

Security > User Roles > Edit Role(BYOD-Provision)

Firewall Policies

Name	Rule Count
logon-control	8
captiveportal	6

Captive Portal Profile

Onboarding Page: Onboarding Page

Based on the ClearPass and Aruba Controller configuration settings for Onboarding shown, which statement accurately describes an employee's new personal device connecting to the Onboarding network? (Select two.)

A. Post-Onboarding, the device will be assigned the BYOD-Provision firewall role in the Aruba Controller.

B. Pre-Onboarding, the device will be redirected to the 'Onboarding Page' Captive Portal.

C. The BYOD-Provision role is a ClearPass internal role and exists in ClearPass.

D. The device will not be redirected to any Onboarding page.

E. Pre-Onboarding, the device will be assigned the BYOD-Provision firewall role in the Aruba Controller.

Correct Answer: B, E
Section:
Explanation:

You can pre-provision with the Aruba controller firewall role of BYOD-Provision.
From the Firewall policies part of the exhibit, we see that the onboarding page is set to captive portal.

Reference: https://community.arubanetworks.com/t5/Security/CP-OnBoard-not-redirecting-toportal-on-single-SSID/td-p/284506

QUESTION 49
Which authentication protocols can be used for authenticating Windows clients that are Onboarded?
(Select two.)

A. EAP-GTC
B. PAP
C. EAP-TLS
D. CHAP
E. PEAP with MSCHAPv2

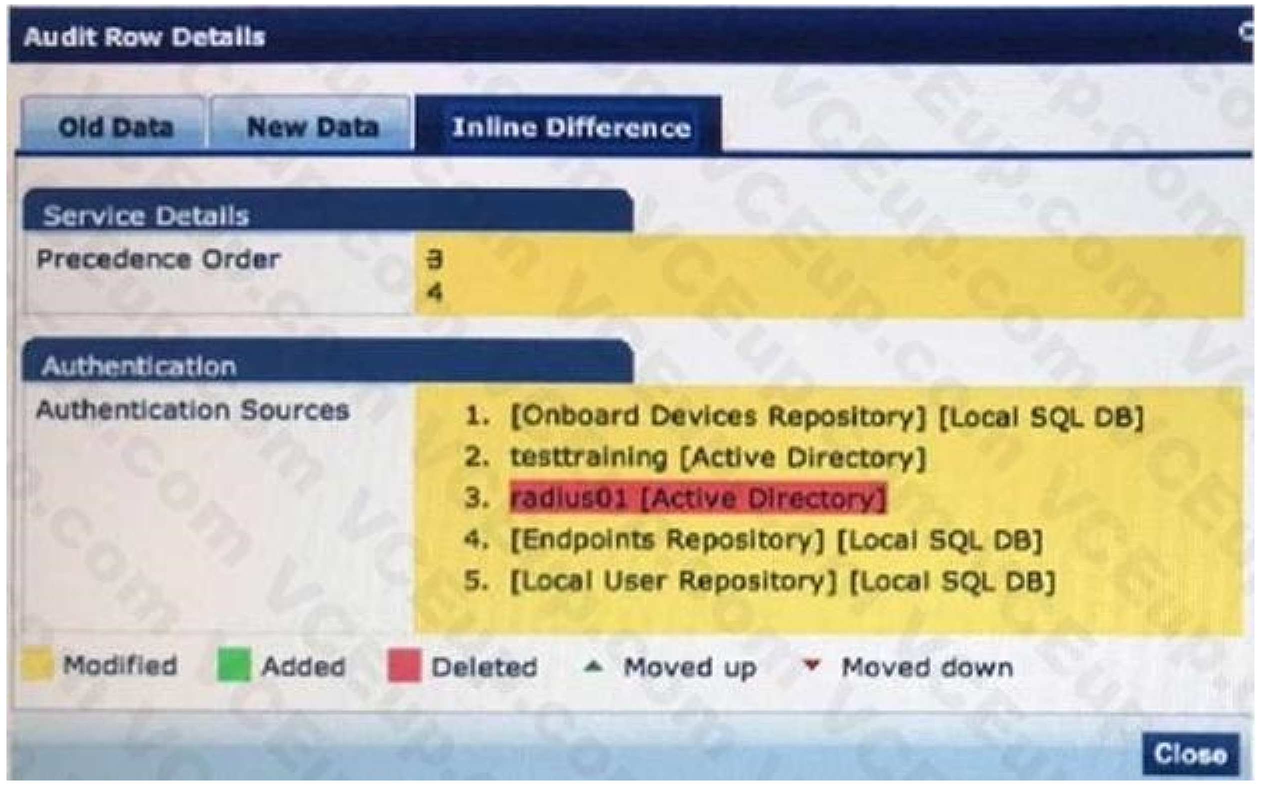
Correct Answer: C, E
Section:

QUESTION 50
Which devices support Apple over-the-air provisioning? (Select two.)

A. IOS 5
B. Laptop running Mac OS X 10.8
C. Laptop running Mac OS X 10.6
D. Android 2.2
E. Windows XP

Correct Answer: A, B
Section:
Explanation:
Apple over-the-air provisioning is supported by IOS and OSX above version 10.6.
Reference:
https://community.arubanetworks.com/aruba/attachments/aruba/tkb@tkb/286/1/BYODwithClearPass_Cameron_Esdaile.pdf

QUESTION 51
Refer to the exhibit.



Service Details

Precedence Order	3 4

Authentication

Authentication Sources

1. [Onboard Devices Repository] [Local SQL DB]
2. testtraining [Active Directory]
3. radius01 [Active Directory]
4. [Endpoints Repository] [Local SQL DB]
5. [Local User Repository] [Local SQL DB]

What information can be drawn from the audit row detail shown? (Select two.)

A. radius01 was deleted from the list of authentication sources.
B. The policy service was moved to position number 4.
C. radius01 was moved to position number 4.
D. The policy service was moved to position number 3.
E. raduis01 was added as an authentication source.

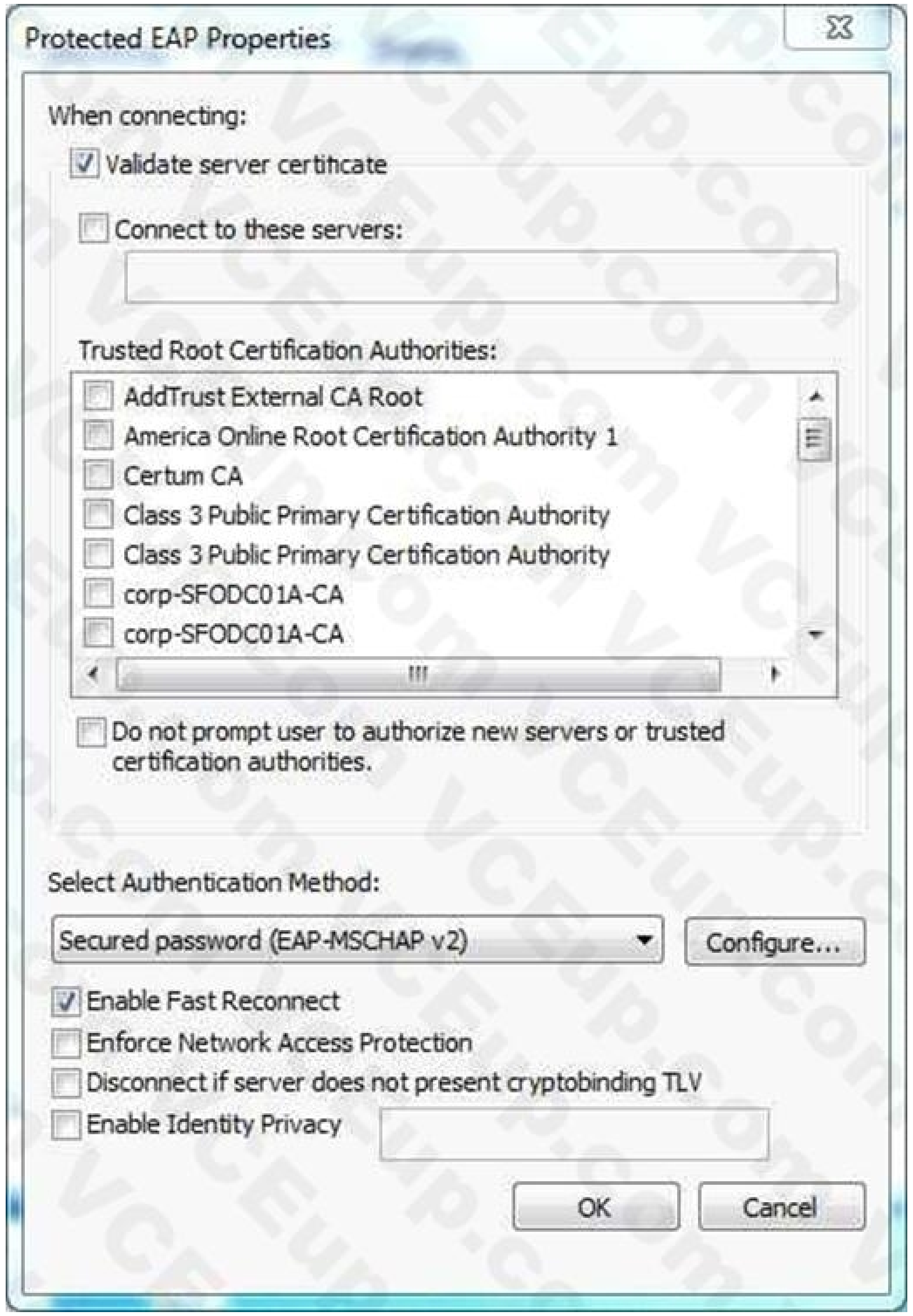
Correct Answer: A, B
Section:

QUESTION 52
What is the purpose of the Audit Viewer in the Monitoring section of ClearPass Policy Manager?

A. to audit client authentications
B. to display changes made to the ClearPass configuration
C. to display the entire configuration of the ClearPass Policy Manager
D. to audit the network for PCI compliance
E. to display system events like high CPU usage.

Correct Answer: B
Section:

QUESTION 53
Refer to the exhibit.



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ AddTrust External CA Root
□ America Online Root Certification Authority 1
□ Certum CA
□ Class 3 Public Primary Certification Authority
□ Class 3 Public Primary Certification Authority
□ corp-SFODC01A-CA
□ corp-SFODC01A-CA

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

Based on the configuration of a Windows 802.1X supplicant shown, what will be the outcome of selecting 'Validate server certificate'?

A. The server and client will perform an HTTPS SSL certificate exchange.
B. The client will verify the server certificate against a trusted CA.
C. The client will send its private key to the server for verification.
D. The server will send its private key to the client for verification.
E. The client will send its certificate to the server for verification.

Correct Answer: B
Section:

QUESTION 54

Which settings need to be validated for a successful EAP-TLS authentication? (Select two.)

A. Username and Password

B. Pre-shared key

C. WPA2-PSK

D. Server Certificate

E. Client Certificate

Correct Answer: D, E

Section:

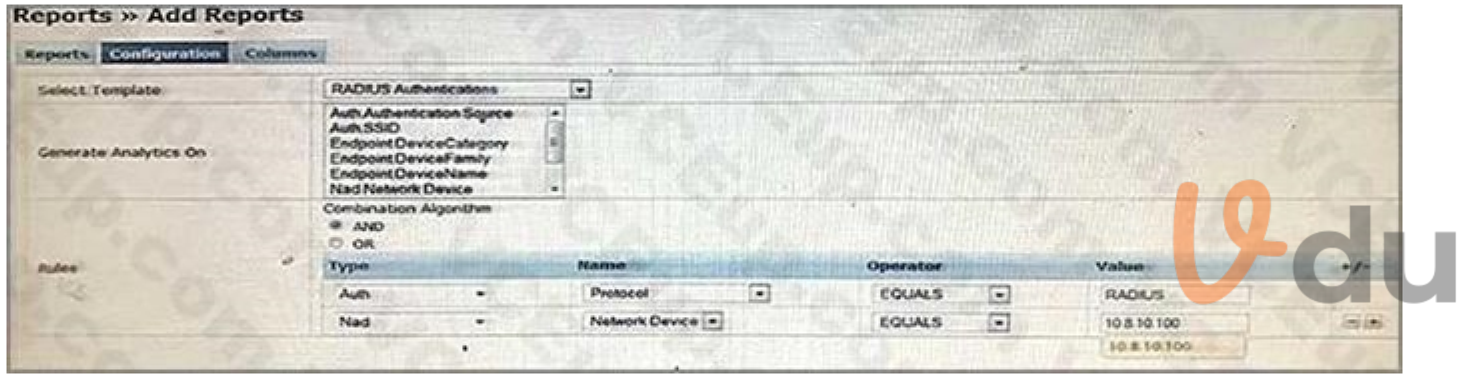
Explanation:

When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other. Certificates must meet specific requirements both on the server and on the client for successful authentication.

Reference: https://support.microsoft.com/en-us/help/814394/certificate-requirements-when-youuse-eap-tls-or-peap-with-eap-tls

QUESTION 55

Refer to the exhibit.



Reports » Add Reports

Select Template: RADIUS Authentications

Generate Analytics On:
Auth.Authentication Source
Auth.SSID
Endpoint.DeviceCategory
Endpoint.DeviceFamily
Endpoint.DeviceName
Nad.Network Device

Rules:

Combination Algorithm
● AND
○ OR

Type	Name	Operator	Value
Auth	Protocol	EQUALS	RADIUS
Nad	Network Device	EQUALS	10.8.10.100
			10.8.10.100

Which types of records will the report shown display?

A. all RADIUS authentications from the 10.8.10.100 NAD to ClearPass

B. all failed RADIUS authentications through ClearPass

C. only Windows devices that have authenticated through the 10.8.10.100 NAD

D. all successful RADIUS authentications through ClearPass

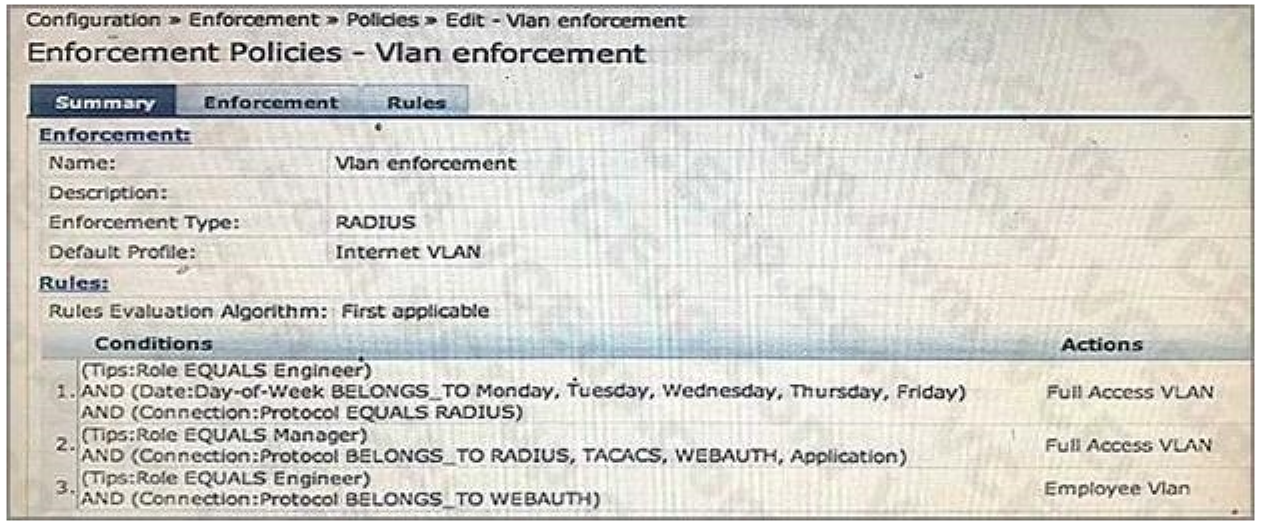
E. all successful RADIUS authentications from the 10.8.10.100 NAD to ClearPass

Correct Answer: A

Section:

QUESTION 56

Refer to the exhibit.



Configuration » Enforcement » Policies » Edit - Vlan enforcement

Enforcement Policies - Vlan enforcement

Enforcement:

Name:	Vlan enforcement
Description:	
Enforcement Type:	RADIUS
Default Profile:	Internet VLAN

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS Engineer) AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Connection:Protocol EQUALS RADIUS)	Full Access VLAN
2.	(Tips:Role EQUALS Manager) AND (Connection:Protocol BELONGS_TO RADIUS, TACACS, WEBAUTH, Application)	Full Access VLAN
3.	(Tips:Role EQUALS Engineer) AND (Connection:Protocol BELONGS_TO WEBAUTH)	Employee Vlan

Based on the Policy configuration shown, which VLAN will be assigned when a user with ClearPass role Engineer authenticates to the network successfully using connection protocol WEBAUTH?

A. Deny Access
B. Employee VLAN
C. Internet VLAN
D. Full Access VLAN

Correct Answer: B
Section:

QUESTION 57
Which statement accurately describes configuration of Data and Management ports on the ClearPass appliance? (Select two.)

A. Configuration of the management port is optional.
B. Configuration of the management port is mandatory.
C. Configuration of the data port is mandatory.
D. Configuration of the data port is optional.
E. Static IP addresses are only allowed on the management port, not the data port.

Correct Answer: B, D
Section:

QUESTION 58
What is a benefit of ClearPass Onguard?

A. It enables organizations to run advanced endpoint posture assessments.
B. It allows a receptionist in a hotel to create accounts for guest users.
C. It allows employees to self-provision their personal devices on the corporate network.
D. It offers an easy way for users to self-configure their devices to support 802.1X authentication on wired and wireless networks.
E. It allows employees to create temporary accounts for Wi-Fi access.

Correct Answer: A
Section:

QUESTION 59
A guest self-registered through a Publisher's Register page.
Which statement accurately describes how the guest's account will be stored?

A. It will be stored in the Publisher's guest user repository and the Subscriber's Onboard user repository.
B. It will be stored in the Publisher's local user repository and the Subscriber's guest user repository.
C. It will be stored in the Publisher's guest user repository permanently, but only for 14 days in the Subscriber's guest user repository,
D. It will be stored in both the Publisher's guest user repository and the Subscriber's guest user repository.
E. It will be stored in the Publisher's guest user repository, but not the Subscriber's.

Correct Answer: D
Section:

QUESTION 60
Which IP address should be set as the DHCP relay on an Aruba Controller for device fingerprinting on ClearPass?

A. DHCP server IP
B. Active Directory IP
C. Switch IP
D. Microsoft NPS server IP
E. ClearPass server IP

Correct Answer: E
Section:

QUESTION 61
Which collectors can be used for device profiling? (Select two.)

A. Username and Password
B. ActiveSync Plugin
C. Client's role on the controller
D. Onguard agent
E. Active Directory Attributes

Correct Answer: B, D
Section:

QUESTION 62
Which checks are made with Onguard posture evaluation in ClearPass? (Select three.)

A. Registry keys
B. EAP TLS certificate validity
C. Client role check
D. Peer-to-peer application checks
E. Operating System version

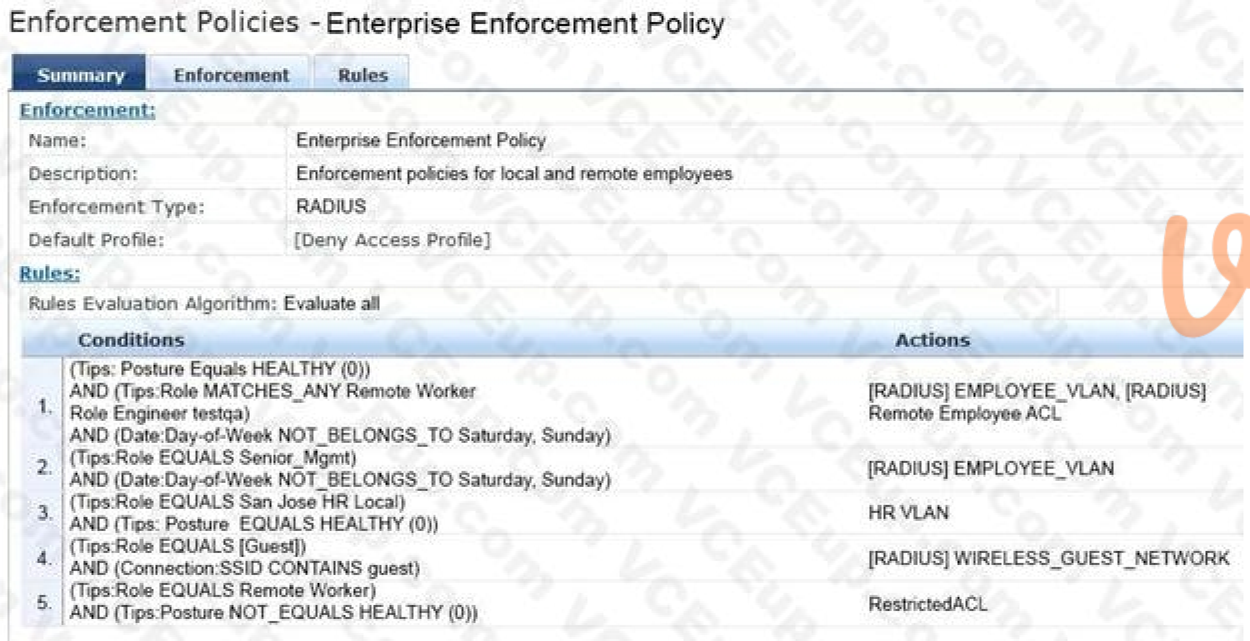
Correct Answer: A, D, E
Section:

QUESTION 63
Why is a terminate session enforcement profile used during posture checks with 802.1x authentication?

A. To send a RADIUS CoA message from the ClearPass server to the client
B. To disconnect the user for 30 seconds when they are in an unhealthy posture state
C. To blacklist the user when they are in an unhealthy posture state
D. To force the user to re-authenticate and run through the service flow again
E. To remediate the client applications and firewall do that updates can be installed

Correct Answer: A
Section:

QUESTION 64
Refer to the exhibit.



Enforcement Policies - Enterprise Enforcement Policy

Enforcement:

Name:	Enterprise Enforcement Policy
Description:	Enforcement policies for local and remote employees
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm: Evaluate all

	Conditions	Actions
1.	(Tips: Posture Equals HEALTHY (0)) AND (Tips:Role MATCHES_ANY Remote Worker Role Engineer testqa) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN, [RADIUS] Remote Employee ACL
2.	(Tips:Role EQUALS Senior_Mgmt) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	[RADIUS] EMPLOYEE_VLAN
3.	(Tips:Role EQUALS San Jose HR Local) AND (Tips: Posture EQUALS HEALTHY (0))	HR VLAN
4.	(Tips:Role EQUALS [Guest]) AND (Connection:SSID CONTAINS guest)	[RADIUS] WIRELESS_GUEST_NETWORK
5.	(Tips:Role EQUALS Remote Worker) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	RestrictedACL

Based on the Enforcement Policy configuration shown, when a user with Role Engineer connects to the network and the posture token assigned is Unknown, which Enforcement Profile will be applied?

A. EMPLOYEE_VLAN
B. RestrictedACL
C. Deny Access Profile
D. HR VLAN
E. Remote Employee ACL

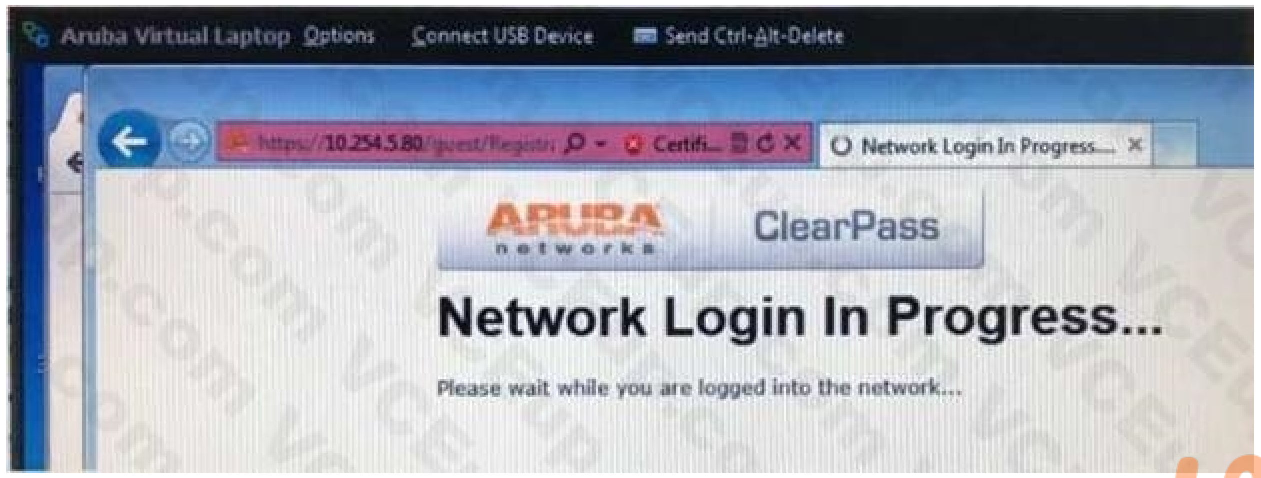
Correct Answer: C
Section:

QUESTION 65
A client's authentication is failing and there are no entries in the ClearPass Access tracker.
What is a possible reason for the authentication failure?

A. The user account has expired.
B. The client used a wrong password.
C. The shared secret between the NAD and ClearPass does not match.
D. The user's certificate is invalid.
E. The user is not found in the database.

Correct Answer: C
Section:

QUESTION 66
Refer to the exhibit.



Network Login In Progress...

Please wait while you are logged into the network...

Based on the information shown on a client's laptop, what will happen next?

A. The web login page will be displayed.
B. The client will send a NAS authentication request to ClearPass.
C. ClearPass will send a NAS authentication request to the NAD.
D. the NAD will send an authentication request to ClearPass.
E. The user will be presented with a self-registration receipt.

Correct Answer: D
Section:

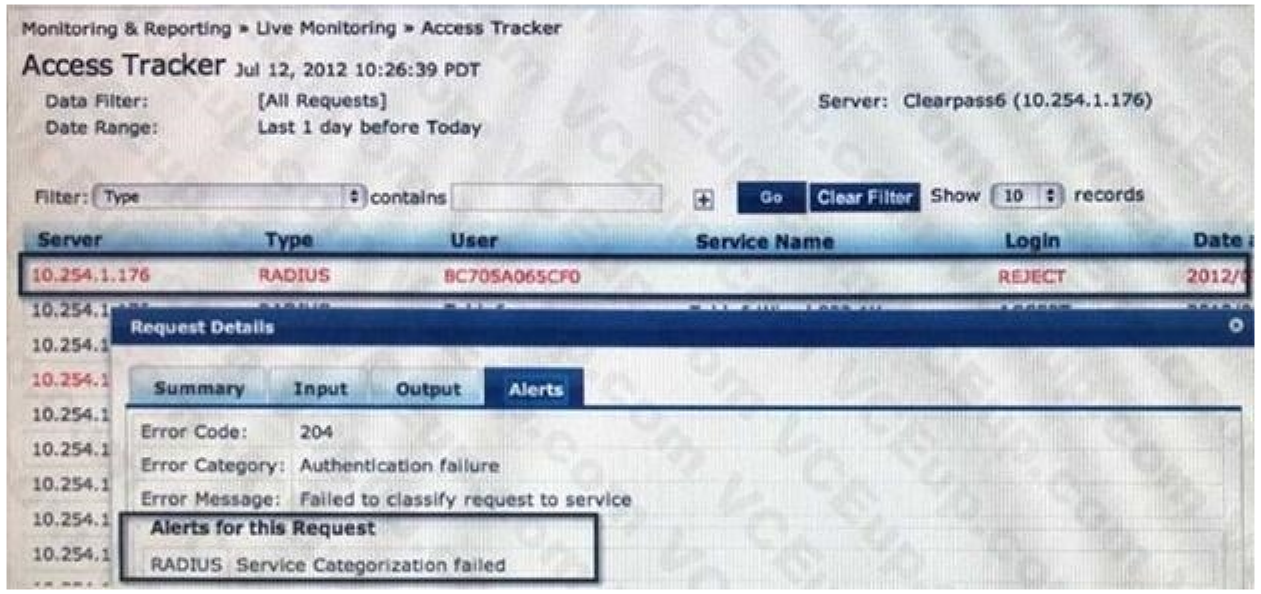
QUESTION 67
What does a Windows client need for it to perform EAS-PEAP successfully when 'Validate server Certificate' is not enabled?

A. Pre-shared key
B. Client Certificate
C. WPA2-PSK
D. Username and Password
E. Server Certificate

Correct Answer: D
Section:

QUESTION 68

Refer to the exhibit.



Monitoring & Reporting » Live Monitoring » Access Tracker

Access Tracker Jul 12, 2012 10:26:39 PDT

Data Filter: [All Requests]

Date Range: Last 1 day before Today

Server: Clearpass6 (10.254.1.176)

Server	Type	User	Service Name	Login	Date
10.254.1.176	RADIUS	BC705A065CF0		REJECT	2012/

Request Details

Error Code: 204

Error Category: Authentication failure

Error Message: Failed to classify request to service

Alerts for this Request

RADIUS Service Categorization failed

What can be concluded from the Access Tracker output shown?

A. The client used incorrect credentials to authenticate to the network.

B. ClearPass does not have a service enabled for MAC authentication.

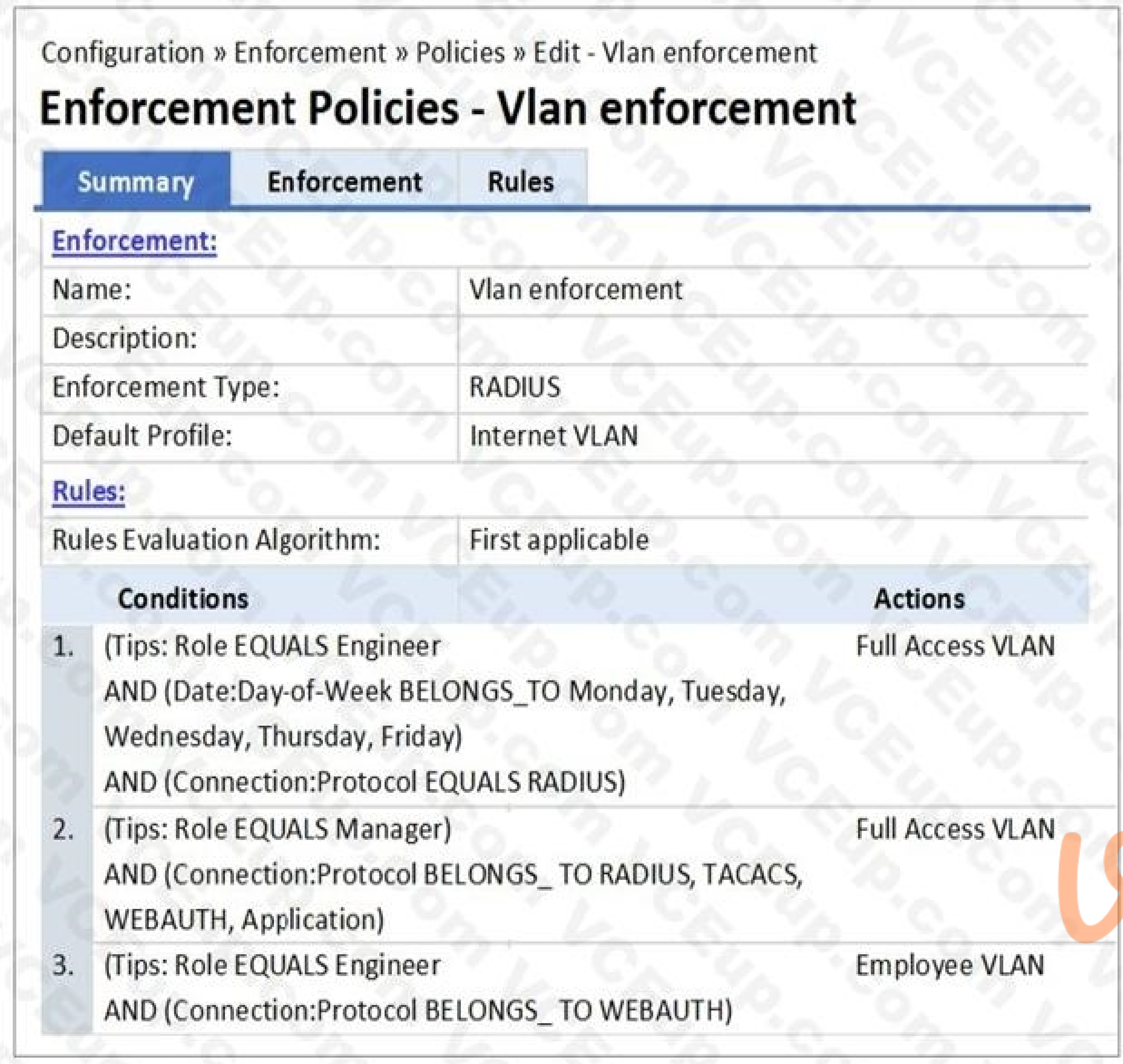
C. The client MAC address is not present in the Endpoints table in the CrearPass database.

D. The RADIUS client on the Windows server failed to categorize the service correctly.

E. The client wireless profile is incorrectly setup.

Correct Answer: B
Section:

QUESTION 69
Refer to the exhibit.



Configuration » Enforcement » Policies » Edit - Vlan enforcement

Enforcement Policies - Vlan enforcement

Enforcement:

Name:	Vlan enforcement
Description:	
Enforcement Type:	RADIUS
Default Profile:	Internet VLAN

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips: Role EQUALS Engineer AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Connection:Protocol EQUALS RADIUS)	Full Access VLAN
2.	(Tips: Role EQUALS Manager) AND (Connection:Protocol BELONGS_ TO RADIUS, TACACS, WEBAUTH, Application)	Full Access VLAN
3.	(Tips: Role EQUALS Engineer AND (Connection:Protocol BELONGS_ TO WEBAUTH)	Employee VLAN

Based on the Policy configuration shown, which VLAN will be assigned when a user with ClearPass role Engineer authenticates to the network successfully on Saturday using connection protocol WEBAUTH?

A. Full Access VLAN
B. Employee VLAN
C. Internet VLAN
D. Deny Access

Correct Answer: B
Section:

QUESTION 70
In a single SSID Onboarding, which method can be used in the Enforcement Policy to distinguish between a provisioned device and a device that has not gone through the Onboard workflow?

A. Active Directory Attributes
B. Network Access Device used
C. Endpoint OS Category
D. Onguard Agent used
E. Authentication Method used

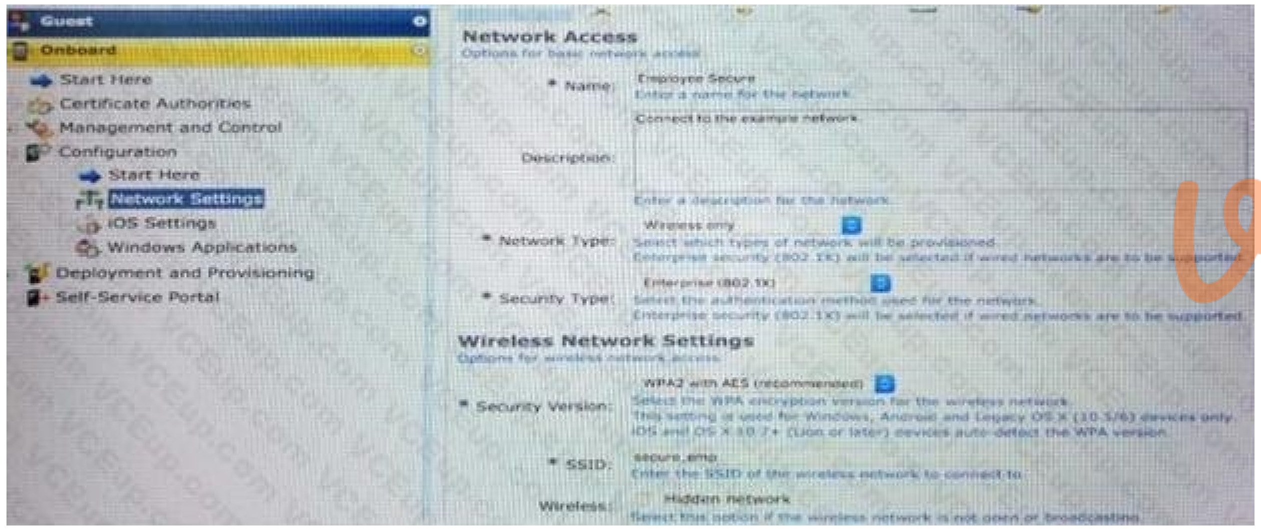
Correct Answer: E
Section:

QUESTION 71
An organization implements dual SSID Onboarding. The administrator used the Onboard service template to create services for dual SSID Onboarding. Which statement accurately describes the outcome?

A. The Onboard Provisioning service is triggered when the user connects to the provisioning SSID to Onboard their device.
B. The Onboard Authorization service is triggered when the user connects to the secure SSID.
C. The Onboard Authorization service is triggered during the Onboarding process.
D. The device connects to the secure SSID for provisioning.
E. The Onboard Authorization service is never triggered.

Correct Answer: C
Section:

QUESTION 72
Refer to the exhibit.



Network Access
Options for basic network access

* Name: Employee Secure
Enter a name for the network

Description: Connect to the example network
Enter a description for the network

* Network Type: Wireless only
Select which types of network will be provisioned
Enterprise security (802.1X) will be selected if wired networks are to be supported

* Security Type: Enterprise (802.1X)
Select the authentication method used for the network
Enterprise security (802.1X) will be selected if wired networks are to be supported

Wireless Network Settings
Options for wireless network access

* Security Version: WPA2 with AES (recommended)
Select the WPA encryption version for the wireless network
This setting is used for Windows, Android and Legacy OS X (10.5/6) devices only
iOS and OS X 10.7+ (Lion or later) devices auto-detect the WPA version

* SSID: secure_emp
Enter the SSID of the wireless network to connect to

Wireless: Hidden network
Select this option if the wireless network is not open or broadcasting

Which statements accurately describe the status of the Onboarded devices in the configuration for the network settings shown? (Select two.)

A. They will connect to Employee_Secure SSID after provisioning.
B. They will connect to Employee_Secure SSID for provisioning their devices.
C. They will use WPA2-PSK with AES when connecting to the SSID.
D. They will connect to secure_emp SSID after provisioning.
E. They will perform 802.1X authentication when connecting to the SSID.

Correct Answer: D, E
Section:

QUESTION 73
Which use cases will require a ClearPass Guest application license? (Select two.)

A. Guest device fingerprinting
B. Guest endpoint health assessment

C. Sponsor based guest user access

D. Guest user self-registration for access

E. Guest personal device onboarding

Correct Answer: C, D
Section:

QUESTION 74
A customer would like to deploy ClearPass with these requirements:
-2000 devices need to be Onboarded
-2000 corporate devices need to run posture checks daily
-500 guest users need to authenticate each day using the web login feature What is the license mix that customer will need to purchase?

A. CP-HW-5k, 2500 ClearPass Enterprise

B. CP-HW-25k, 4500 ClearPass Enterprise

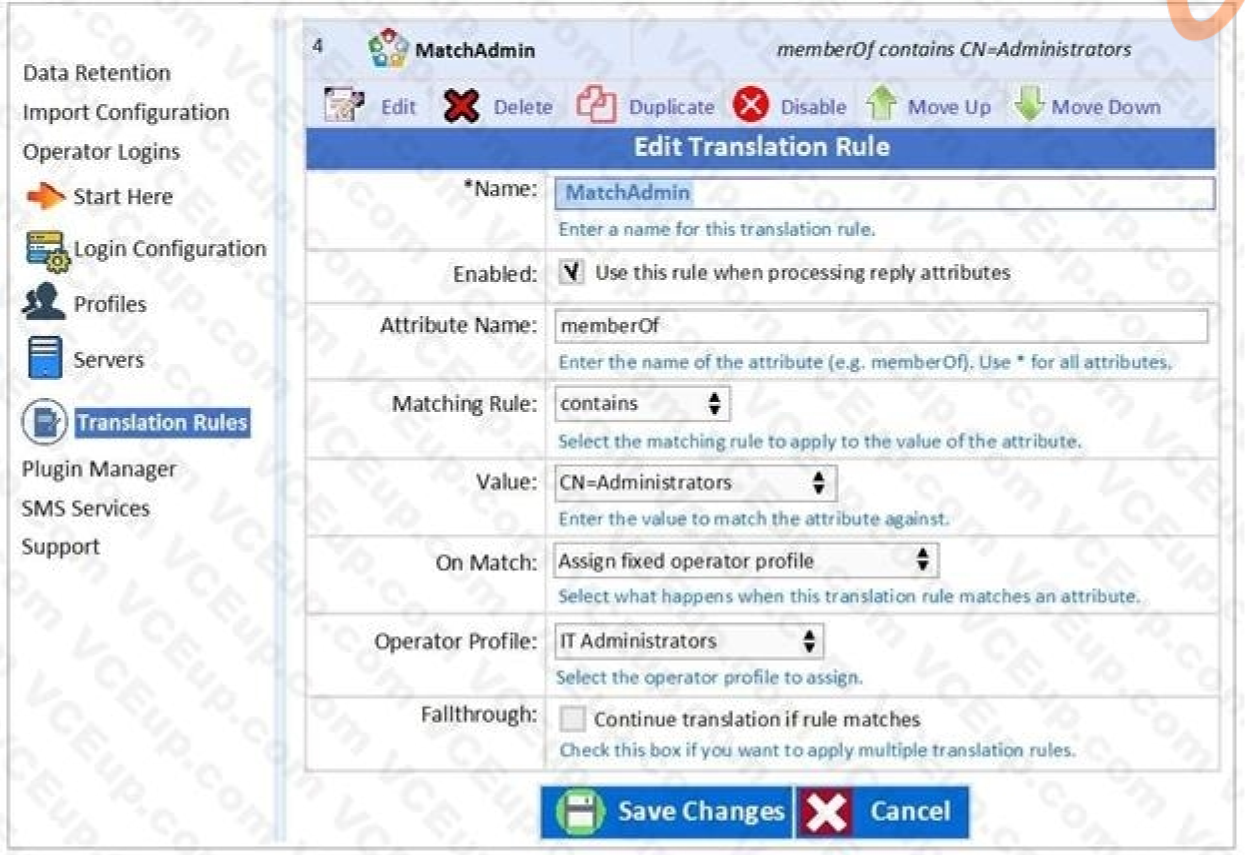
C. CP-HW-500, 2500 ClearPass Enterprise

D. CP-HW-25k, 4000 ClearPass Enterprise

E. CP-HW-5k, 4500 ClearPass Enterprise

Correct Answer: B
Section:

QUESTION 75
Refer to the exhibit.



4 MatchAdmin *memberOf contains CN=Administrators*

Edit Translation Rule

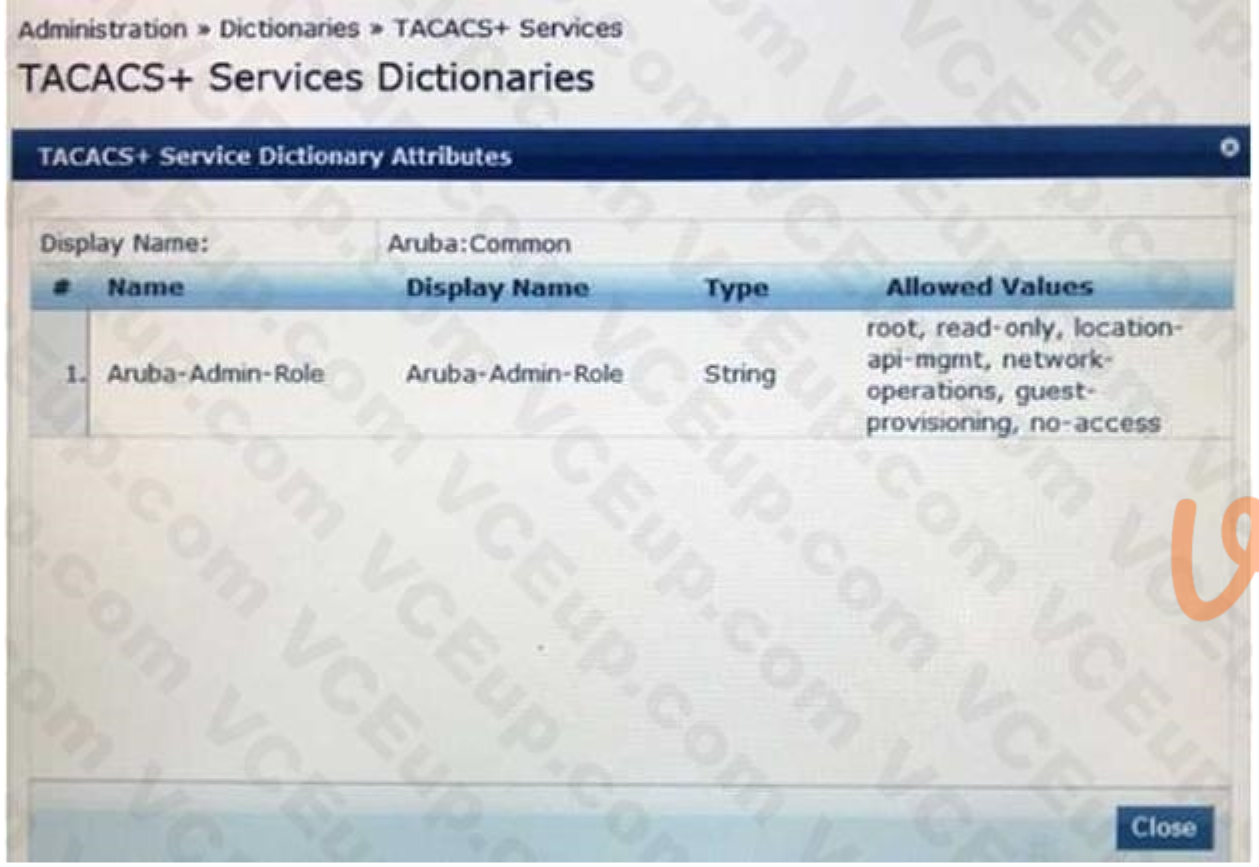
*Name:	MatchAdmin Enter a name for this translation rule.
Enabled:	☑ Use this rule when processing reply attributes
Attribute Name:	memberOf Enter the name of the attribute (e.g. memberOf). Use * for all attributes.
Matching Rule:	contains Select the matching rule to apply to the value of the attribute.
Value:	CN=Administrators Enter the value to match the attribute against.
On Match:	Assign fixed operator profile Select what happens when this translation rule matches an attribute.
Operator Profile:	IT Administrators Select the operator profile to assign.
Fallthrough:	□ Continue translation if rule matches Check this box if you want to apply multiple translation rules.

Based on the Translation Rule configuration shown, what will be the outcome?

A. An AD user from group Administrators will be assigned the operator profile of IT Administrators.
B. All ClearPass Policy Manager admin users who are members of the Administrators AD group will be assigned the TACACS profile of IT Administrators.
C. All active directory users will be assigned the operator profile of IT Administrators.
D. A user from AD group MatchAdmin will be assigned the operator profile of IT Administrators.

Correct Answer: A
Section:

QUESTION 76
Refer to the exhibit.



Administration » Dictionaries » TACACS+ Services

TACACS+ Services Dictionaries

TACACS+ Service Dictionary Attributes

Display Name: Aruba:Common

#	Name	Display Name	Type	Allowed Values
1.	Aruba-Admin-Role	Aruba-Admin-Role	String	root, read-only, location-api-mgmt, network-operations, guest-provisioning, no-access

Based on the Aruba TACACS+ dictionary shown, how is the Aruba-Role attribute used?

A. The Aruba-Admin-Role on the controller is applies to users using TACACS+ to login to the Policy Manager
B. To assign different privileges to clients during 802.1X authentication
C. To assign different privileges to administrators logging into an Aruba NAD
D. It is used by ClearPass to assign TIPS roles to clients during 802.1X authentication
E. To assign different privileges to administrators logging into ClearPass

Correct Answer: C
Section:

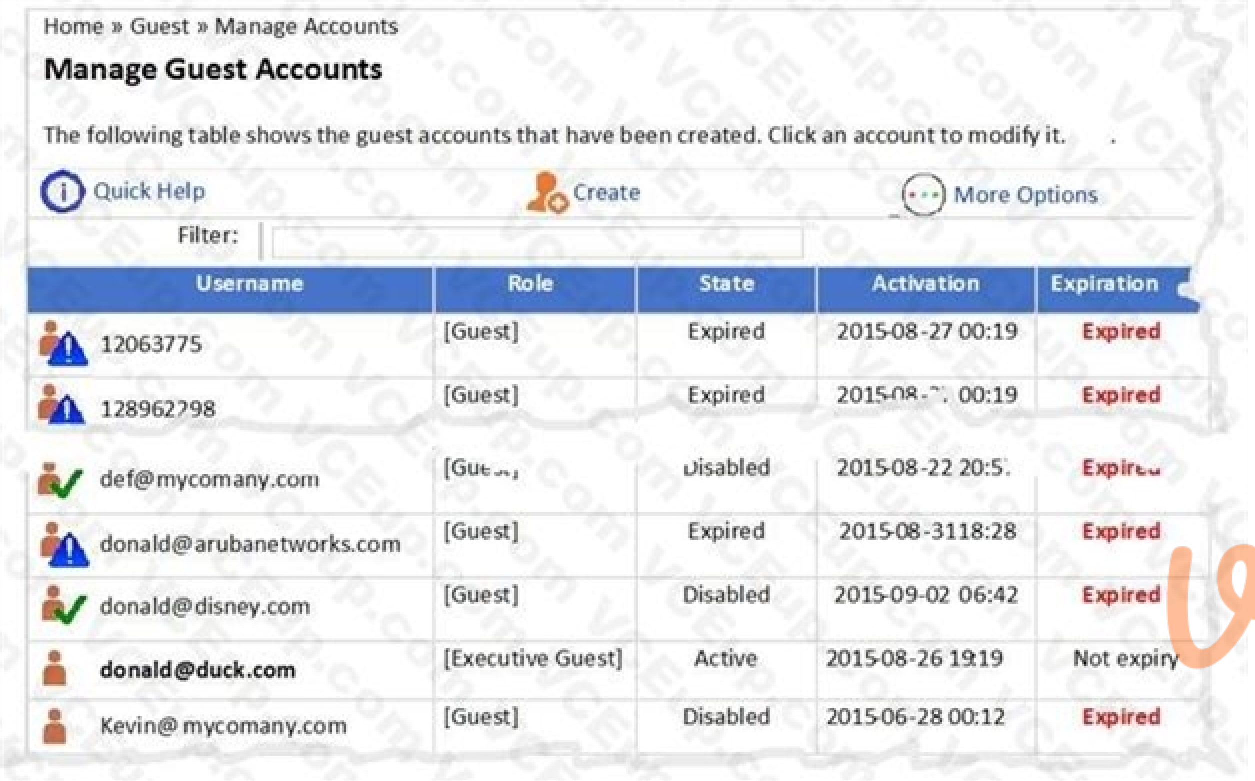
QUESTION 77
In which ways can ClearPass derive client roles during policy service processing? (Select two.)

A. From the attributes configured in Active Directory
B. From the server derivation rule in the Aruba Controller server group for the client

C. From the Aruba Network Access Device
D. From the attributes configured in a Network Access Device
E. Through a role mapping policy

Correct Answer: A, E
Section:

QUESTION 78
Refer to the exhibit.



Home » Guest » Manage Accounts

Manage Guest Accounts

The following table shows the guest accounts that have been created. Click an account to modify it.

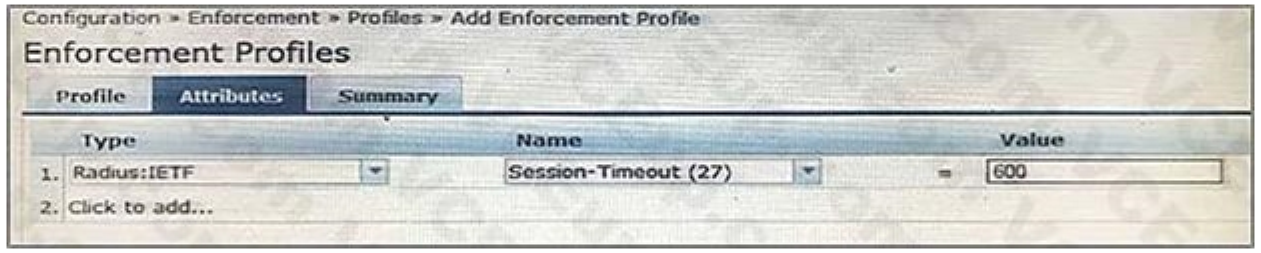
Username	Role	State	Activation	Expiration
12063775	[Guest]	Expired	2015-08-27 00:19	Expired
128962?98	[Guest]	Expired	2015-08-[illegible] 00:19	Expired
def@mycomany.com	[Guest]	Disabled	2015-08-22 20:5[illegible]	Expired
donald@arubanetworks.com	[Guest]	Expired	2015-08-31 18:28	Expired
donald@disney.com	[Guest]	Disabled	2015-09-02 06:42	Expired
donald@duck.com	[Executive Guest]	Active	2015-08-26 19:19	Not expiry
Kevin@ mycomany.com	[Guest]	Disabled	2015-06-28 00:12	Expired

An administrator logs in to the Guest module in ClearPass and 'Manage Accounts' displays as shown.
When a user with username donald@disney.com attempts to access the Web Login page, what will be the outcome?

A. The user will be able to log in and authenticate successfully but will then be immediate disconnected.
B. The user will be able to log in for the next 4.9. days, but then will no longer be able to log in.
C. The user will not be able to log in and authenticate.
D. The user will be able to log in and authenticate successfully, but will then get a quarantine role.
E. The user will not be able to access the Web Login page.

Correct Answer: C
Section:

QUESTION 79
Refer to the exhibit.



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Type	Name		Value
1.	Radius:IETF	Session-Timeout (27)	=	600
2.	Click to add...			

An Enforcement Profile has been created in the Policy Manager as shown.
Which action will ClearPass take based on the Enforcement Profile?

A. It will send the Session-Timeout attribute in the RADIUS Access-Request packet to the NAD and the NAD will end the user's session after 600 seconds.

B. It will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the User and the user's session will be terminated after 600 seconds.

C. It will count down 600 seconds and send a RADUIS CoA message to the NAD to end the user's session after this time is up.

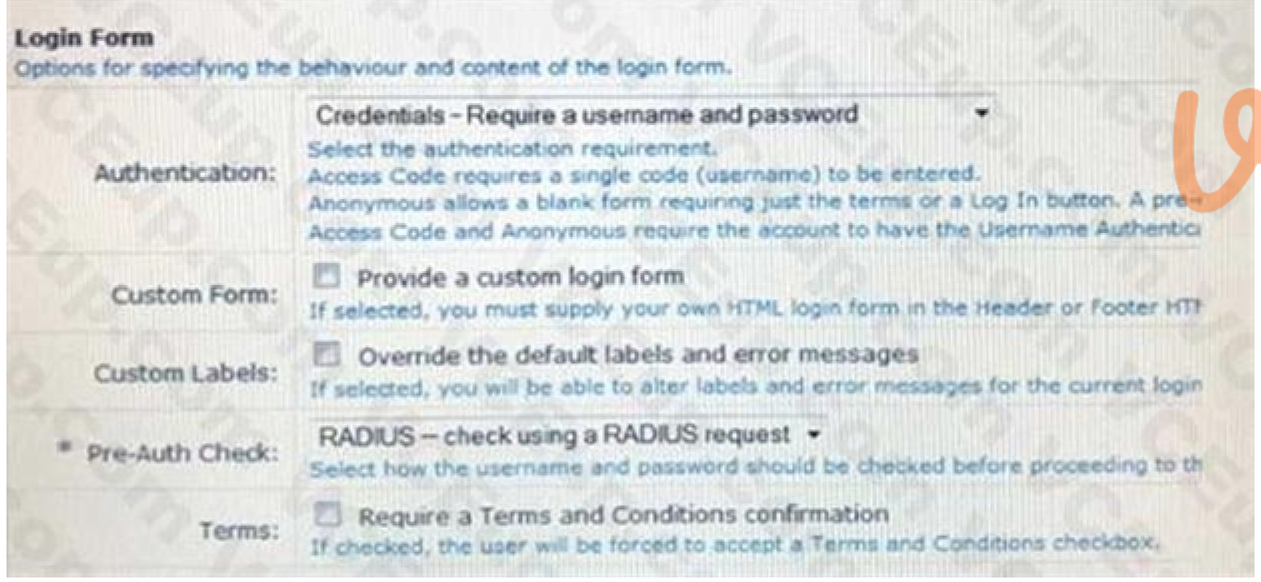
D. It will count down 600 seconds and send a RADUIUS CoA message to the user to end the user's session after this time is up.

E. It will send the session –Timeout attribute in the RADIUS Access-Accept packet to the NAD and the NAD will end the user's session after 600 seconds.

Correct Answer: E
Section:

QUESTION 80

Use this form to make changes to the RADIUS Web Login Guest Network.



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-
Access Code and Anonymous require the account to have the Username Authentic

Custom Form: □ Provide a custom login form
If selected, you must supply your own HTML login form in the Header or Footer HT

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

* Pre-Auth Check: RADIUS – check using a RADIUS request
Select how the username and password should be checked before proceeding to th

Terms: □ Require a Terms and Conditions confirmation
If checked, the user will be forced to accept a Terms and Conditions checkbox.

A Web Login page is configured in Clear Pass Guest as shown.
What is the purpose of the Pre-Auth Check?

A. To authenticate users after the NAD sends an authentication request to ClerPass

B. To authenticate users before the client sends the credentials to the NAD

C. To authenticate users when they are roaming from one NAD to another

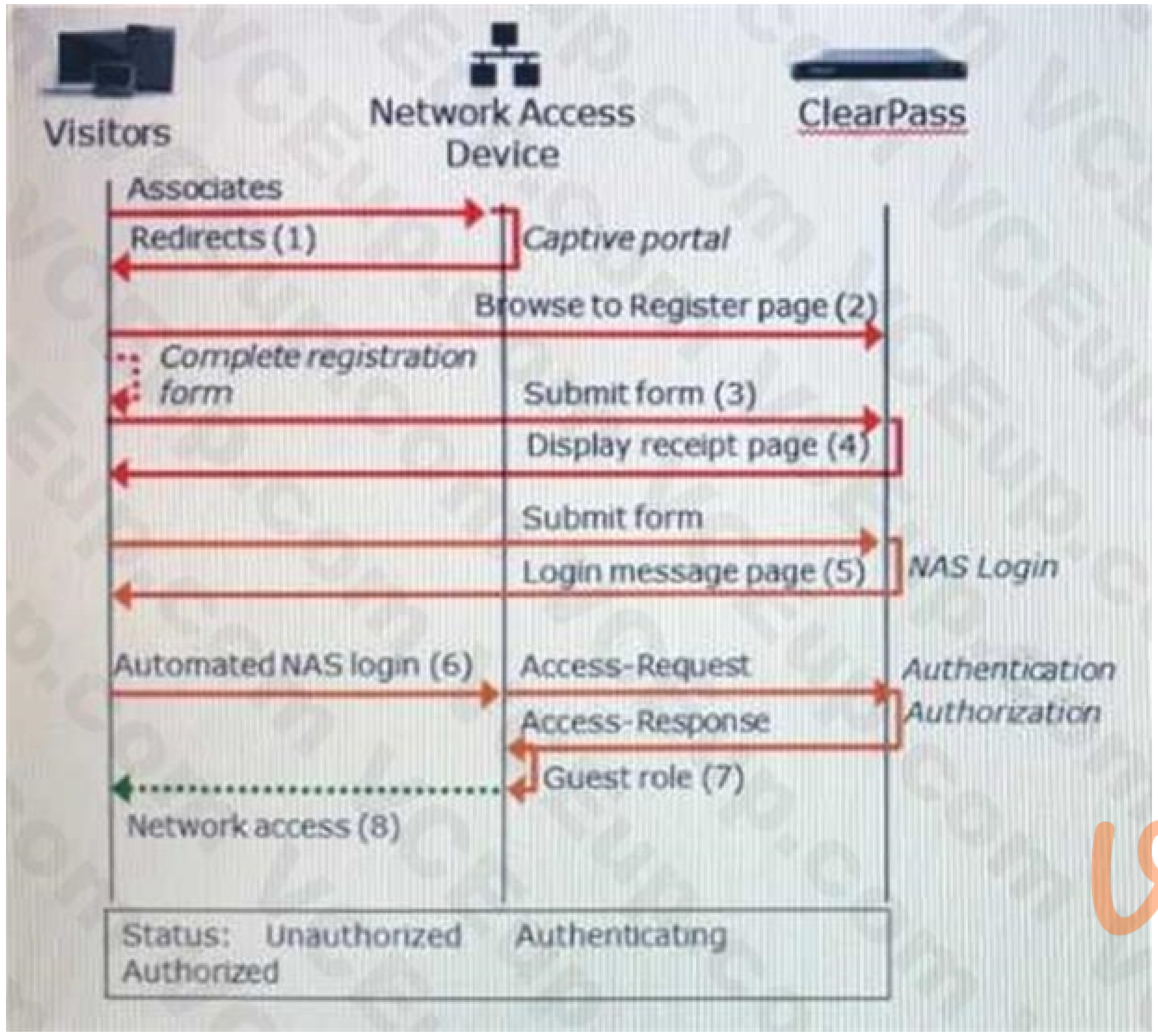
D. To authenticate users before they launch the Web Login Page

E. To replace the need for the NAD to send an authentication request to ClearPass

Correct Answer: B
Section:

QUESTION 81

Refer to the exhibit.



Based on the guest Self-Registration with Sponsor Approval workflow shown, at which stage does the sponsor approve the user's request?

A. After the RADIUS Access-Request

B. After the NAS login, but before the RADIUS Access-Request

C. Before the user can submit the registration form

D. After the RADIUS Access-Response

E. After the receipt page is displayed, before the NAS login

Correct Answer: E
Section:

QUESTION 82
What is the purpose of ClearPass Onboard?

A. to provide MAC authentication for devices that don't support 802.1x

B. to run health checks on end user devices

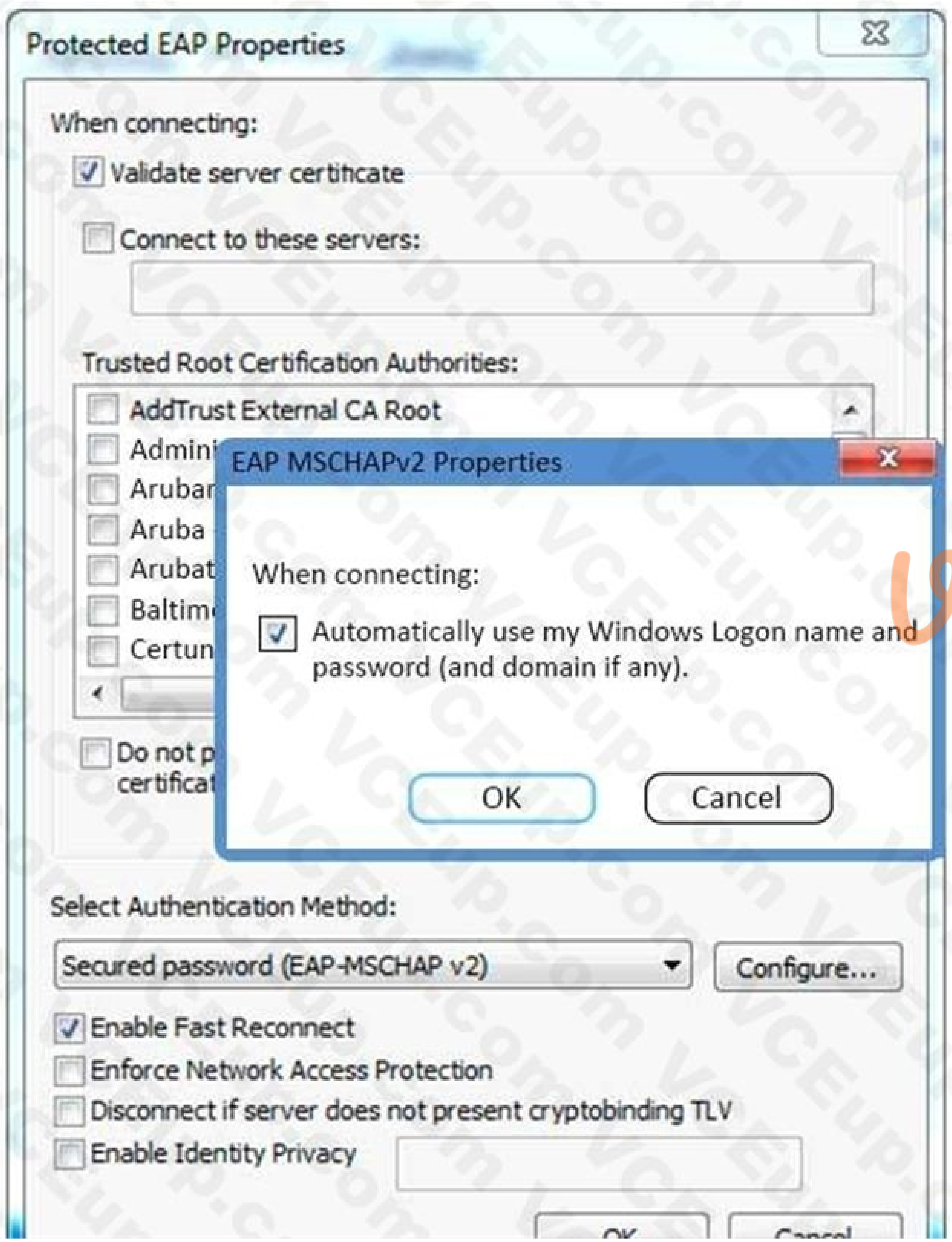
C. to provision personal devices to securely connect to the network

D. to configure self-registration pages for guest users

E. to provide guest access for visitors to connect to the network

Correct Answer: C
Section:

QUESTION 83
Refer to the exhibit.



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ AddTrust External CA Root
□ Admini
□ Arubar
□ Aruba
□ Arubat
□ Baltim
□ Certun

□ Do not p
certificat

EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows Logon name and password (and domain if any).

OK Cancel

Select Authentication Method:

Secured password (EAP-MSCHAP v2) ▾ Configure...

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

Based on the configuration of a Windows 802.1X supplicant shown, what will be the outcome when 'Automatically use my Windows logon name and password' are selected?

A. The client will use machine authentication.

B. The client's Windows login username and password will be sent inside a certificate to the Active Directory server.
C. The client's Windows login username and password will be sent to the Authentication server.
D. The client will need to re-authenticate every time they connect to the network.
E. The client will prompt the user to enter the logon username and password.

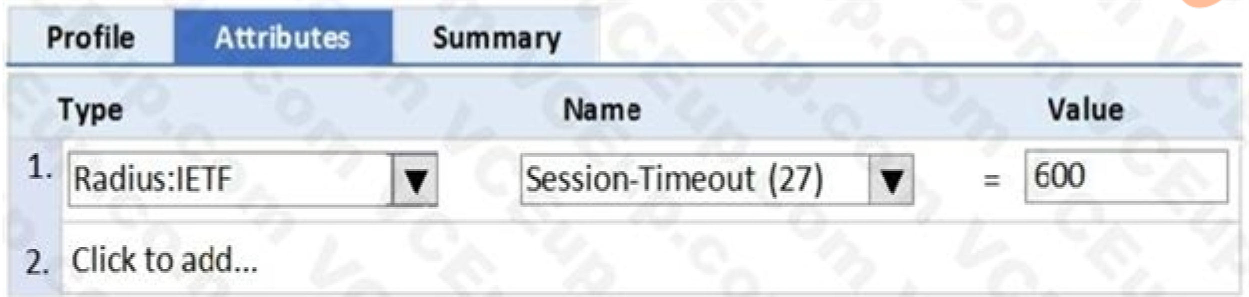
Correct Answer: C
Section:

QUESTION 84
A hotel chain deployed ClearPass Guest. When hotel guests connect to the Guest SSID, launch a web browser and enter the address www.google.com, they are unable to immediately see the web login page.
What are the likely causes of this? (Select two.)

A. The ClearPass server has a trusted server certificate issued by Verisign.
B. The ClearPass server has an untrusted server certificate issued by the internal Microsoft Certificate server.
C. The ClearPass server does not recognize the client's certificate.
D. The DNS server is not replying with an IP address for www.google.com.

Correct Answer: B, D
Section:
Explanation:
You would need a publicly signed certificate.
Reference: http://community.arubanetworks.com/t5/Security/Clearpass-Guest-certificate-error-forguest-visitors/td-p/221992

QUESTION 85
Refer to the exhibit.



	Type	Name		Value
1.	Radius:IETF	Session-Timeout (27)	=	600
2.	Click to add...			

An Enforcement Profile has been created in the Policy Manager as shown.
Which action will ClearPass take based on this Enforcement Profile?

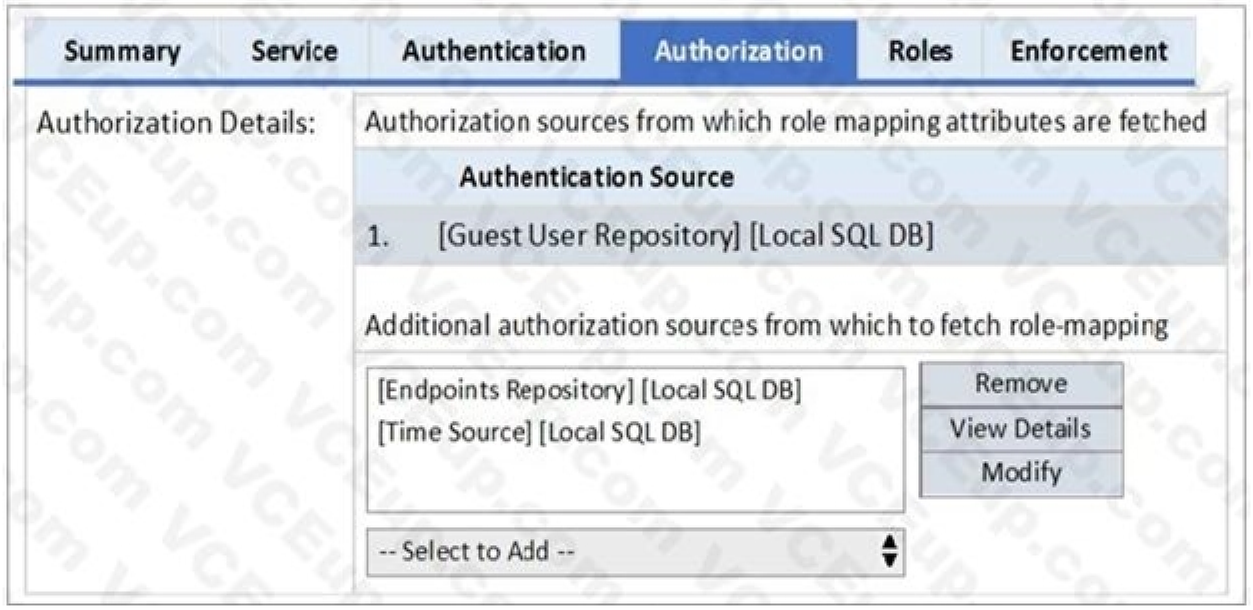
A. ClearPass will count down 600 seconds and send a RADIUS CoA message to the user to end the user's session after this time is up.
B. ClearPass will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the NAD and the NAD will end the user's session after 600 seconds.
C. ClearPass will count down 600 seconds and send a RADIUS CoA message to the NAD to end the user's session after this time is up.
D. ClearPass will send the Session-Timeout attribute in the RADIUS Access-Request packet to the NAD and the NAD will end the user's session after 600 seconds.
E. ClearPass will send the Session-Timeout attribute in the RADIUS Access-Accept packet to the User and the user's session will be terminated after 600 seconds.

Correct Answer: E
Section:
Explanation:
Session Timeout (in seconds) - Configure the agent session timeout interval to re-evaluate the system health again. OnGuard triggers auto-remediation using this value to enable or disable AV-RTP status check on endpoint.
Agent re-authentication is determined based on session-time out value.
You can specify the session timeout interval from 60 – 600 seconds. Setting the lower value for session timeout interval results numerous authentication requests in Access Tracker page. The default value is 0.

Reference: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_User Guide/Enforce/EPAgent_Enforcement.htm

QUESTION 86

Refer to the exhibit.



Authorization Details: Authorization sources from which role mapping attributes are fetched

	Authentication Source
1.	[Guest User Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping

[Endpoints Repository] [Local SQL DB]
[Time Source] [Local SQL DB]

Based on the information shown, what is the purpose of using [Time Source] for authorization?

A. to check how long it has been since the last login authentication
B. to check whether the guest account expired
C. to check whether the MAC address is in the MAC Caching repository
D. to check whether the MAC address status is known in the endpoints table
E. to check whether the MAC address status is unknown in the endpoints table

Correct Answer: D
Section:

QUESTION 87

A customer with an Aruba Controller wants it to work with ClearPass Guest.
How should the customer configure ClearPass as an authentication server in the controller so that guests are able to authenticate successfully?

A. Add ClearPass as a RADIUS CoA server.
B. Add ClearPass as a RADIUS authentication server.
C. Add ClearPass as a TACACS+ authentication server.
D. Add ClearPass as an HTTPS authentication server.

Correct Answer: B
Section:
Explanation:
5. Configuring the Aruba Controller
5.1 Add Clearpass as RADIUS Server
Navigate to Configuration > SECURITY > Authentication > Servers
Click on RADIUS Server and enter the Name of your Clearpass Server: myClearpass Click Add Click on myClearpass in the Server List Etc.
Reference: https://community.arubanetworks.com/t5/Security/Step-by-Step-Controller-CPPM-6-5-Captive-Portal-authentication/td-p/229740

QUESTION 88

A bank would like to deploy ClearPass Guest with web login authentication so that their customers can selfregister on the network to get network access when they have meetings with bank employees. However, they're concerned about security.

What is true? (Choose three.)

A. If HTTPS is used for the web login page, after authentication is completed guest Internet traffic willall be encrypted as well.

B. During web login authentication, if HTTPS is used for the web login page, guest credentials will beencrypted.

C. After authentication, an IPSEC VPN on the guest's client be used to encrypt Internet traffic.

D. HTTPS should never be used for Web Login Page authentication.

E. If HTTPS is used for the web login page, after authentication is completed some guest Internettraffic may be unencrypted.

Correct Answer: B, C, E

Section: