

HPE6-A68.VCEplus.premium.exam.58q

Number: HPE6-A68
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

HPE6-A68

Aruba Certified ClearPass Professional (ACCP) V6.7



Version 1.0

Exam A

QUESTION 1

Refer to the exhibit.

Administration » Server Manager » Server Configuration

Server Configuration

Cluster-Wide Parameters

General
Cleanup Intervals
Notifications
Standby Publisher
Virtual IP Configuration

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

Restore Defaults
Save
Cancel

Which statement accurately describes the cp82 ClearPass node? (Choose two.)

- A. It stays as a Subscriber when the Publisher fails.
- B. It becomes the Publisher when the primary Publisher fails.
- C. It operates as a Publisher in a separate cluster when the Publisher is active.
- D. It operates as a Publisher in the same cluster as the primary Publisher when the primary is active.
- E. It operates as a Subscriber when the Publisher is active.



Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2 A customer with an Aruba Controller wants to set it up to work with ClearPass Guest.

Hoe should they configure ClearPass as an authentication server in the controller so that guests are able to authenticate successfully?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Refer to the exhibit.

RADIUS Attributes				
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
			Disable	Export Close



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: (none)

Explanation

Explanation/Reference:

QUESTION 4

A bank would like to deploy ClearPass Guest with web login authentication so that their customers can self-register 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 will all be encrypted as well.
- B. During web login authentication, if HTTPS is used for the web login page, guest credentials will be encrypted.
- 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 Internet traffic may be unencrypted.

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5 A customer wants to make enforcement decisions during 802.1x authentication based on a client's Onguard posture token.

What enforcement profile should be used in the health check service?

- A. Quarantine VLAN
- B. RADIUS CoA
- C. RADIUS Accept
- D. RADIUS RejectE. Full Access VLAN.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6 Which authorization servers are supported by ClearPass?
(Choose two.)

- A. Active Directory
- B. Cisco Controller
- C. Aruba Controller
- D. LDAP server
- E. Aruba Mobility Access Switch



Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

Refer to the exhibit.

Summary	Policy	Mapping rules
<u>Profile:</u>		
Name:	Agent Unhealthy Profile	
Description:		
Type:	Agent	
Action:	Accept	
Device Group List:	-	
<u>Attributes:</u>		
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. A message is sent to the Onguard Agent on the client device.
- C. An unhealthy role value is sent to the Network Access 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: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Refer to the exhibit.

Summary	Policy	Mapping rules
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? (Choose two.)

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

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Refer to the exhibit.

Summary	Enforcement	Rules
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))	[RADIUS] WIRELESS_GUEST_NETWORK	
4. (Tips:Role EQUALS [Guest]) AND (Connection:SSID CONTAINS guest)	RestrictedACL	
5. (Tips:Role EQUALS Remote Worker) AND (Tips:Posture NOT_EQUALS Healthy (0))		

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10 What does Authorization allow us to do in a Policy Service?

- A. To use attributes in databases in role mapping and Enforcement.
- B. To use attributes stored in databases in Enforcement only, but not role mapping.
- C. To use attributes stored in external databases for Enforcement, but not internal databases.
- D. To use attributes stored in databases in role mapping only, but not Enforcement.
- E. To use attributes stored in internal databases for Enforcement, but not external databases.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Refer to the exhibit.

Summary	Enforcement	Rules
Enforcement:		
Name:	Handled_Wireless_Access_Policy	
Description:	Enforcement policy for handled 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_HANDLED_NETWORK	
(Tips: Role MATCHES_ANY conferencelaptop developer	WIRELESS_EMPLOYEE_NETWORK	
3. senior_mgmt		
testqa		
Role_Engineer)		

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. WIRELESS_EMPLOYEE_NETWORK

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12 Which statement is true about the

databases in ClearPass? A. Entries in the guest user database do not expire.

B. A Static host list can only contain a list of IP addresses.

- C. Entries in the guest user database can be deleted.
- D. Entries in the local user database cannot be modified.
- E. The endpoints database can only be populated by manually adding MAC addresses to the table.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

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:	<input type="text" value="GuestNetwork"/> Enter a name for this web login page.
Page Name:	<input type="text" value="Aruba_login"/> Enter a name for this web login page. The web login will be accessible from "/guest/page_name.php".
Description:	<input type="text"/> Comments or descriptive text about the web login.
* Vendor Settings:	<div>Aruba Networks ▼</div> Select a predefined group of settings suitable for standard network configurations.
Address:	<input type="text" value="securelogin.arubanetworks.com"/> Enter the IP address or hostname of the vendor's product here.
Secure Login:	<div>Use Vendor default ▼</div> Select a security option to apply to the web login process.
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different add The address above will be used whenever the parameter is not available or fails the r

When configuring a Web Login Page in Clear Pass Guest, the information shown is displayed.

What is the page name field used for?

- A. For Administrators to access the PHP page, but not guests.
- B. For forming the Web Login Page URL.
- C. For forming the Web Login Page URL where Administrators add guest users.
- D. For Administrators to reference the page only.
- E. For forming the Web Login Page URL and the page name that guests must configure on their laptop wireless supplicant.

Correct Answer: B








Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

Refer to the exhibit.

Device Provisioning Settings	
<div>  General  Web Login  iOS iOS & OS X  Legacy OS X  Windows  Android  Onboard Client </div>	
*Name:	<input type="text" value="Local Device Provisioning"/> <p>Enter a name for this configuration set.</p>
Description:	<input type="text" value="This is the default configuration set for device provisioning."/> <p>Enter a description for the configuration set.</p>
*Organization:	<input type="text" value="Example Organization"/> <p>Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.</p>
Identity <p>These options control the generation of device credentials</p>	
* Certificate Authority:	<input type="text" value="Local Certificate Authority"/> <p>Select the certificate authority that will be used to sign profiles and messages.</p>
* Signer:	<input type="text" value="Onboard Certificate Authority"/> <p>Select the source that will be use to sign TLS client certificates.</p>
* Key Type:	<input type="text" value="1024-bit RSA - created by device"/> <p>Select the type of private key to use for TLS certificates.</p>
* Unique Device Credentials:	<input checked="" type="checkbox"/> <input type="text" value="Include the username in unique device credentials"/> <p>When checked, the username is prefixed to the device's PEAP credentials. This unique set of credentials is used to identify the user and device on the network.</p>

Based on the configuration for the client's certificate private key as shown, which statements accurately describe the settings? (Choose two.)

- A. More bits in the private key will increase security.
- B. The private key for TLS client certificates is not created.
- C. The private key is stored in the ClearPass server.
- D. More bits in the private key will reduce security.
- E. The private key is stored in the user device.

Correct Answer: AE

Section: (none)


Explanation

Explanation/Reference:

QUESTION 15

Refer to the exhibit.







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 does 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: (none)

Explanation

Explanation/Reference:

QUESTION 16

A University wants to deploy ClearPass with the Guest module. They have two types of users that need to use web login authentication. The first type of users are students whose accounts are in Active Directory server. The second type of user are friends of students who need to self-register to access the network.

How should the service be setup in the Policy Manager for this Network?

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

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Refer to the exhibit.



Authentication Sources - remotelab AD

Summary	General	Primary	Attributes
Name:	retemotelab AD		
Description:			
Type:	Active Directory		
User for Authorization:	<input checked="" type="checkbox"/> Enable to use this authentication source to		
Authorization Sources:	<div> <div></div> <div>-- Select --</div> <div></div> </div>		
Server Timeout:	10	seconds	
Cache Timeout:	36000	seconds	
Backup Servers Priority:			



What does the Cache Timeout Value refer to?

- A. The amount of time the Policy Manager caches the user credentials stored in the Active Directory.
- B. The amount of time the Policy Manager waits for a response from the Active Directory before checking the backup authentication source.
- C. The amount of time the Policy Manager caches the user attributes fetched from Active Directory.
- D. The amount of time the Policy Manager waits for response from the Active Directory before sending a timeout message to the Network Access Device.
- E. The amount of time the Policy Manager caches the user's client certificate.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

Which components of a ClearPass is mandatory?

- A. Authorization Source
- B. Enforcement
- C. Profiler
- D. Role Mapping Policy
- E. Posture

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19 Which is a valid policy simulation types in ClearPass?
(Choose three.)

- A. Enforcement Policy
- B. Posture token derivation
- C. Role Mapping
- D. Endpoint Profiler
- E. Chained simulation

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:



QUESTION 20 Which needs to be validated for a successful EAP-TLS authentication? (Choose two.)

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21 What does a client need for it to perform EAP-PEAP successfully, if 'Validate server Certificate' is not enabled?

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

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

Refer to the exhibit.

Configuration » Authentication » Sources » Add - remotelab AD

Authentication Sources - remotelab AD

Summary	General	Primary	Attributes
Specify filter queries used to fetch authentication and authorization attributes.			
Filter Name	Attribute Name	Alias Name	Enabled as
1. Authentication	dn	UserDN	-
	department	Department	Role, Attribute
	title	Title	Attribute
	company	company	-
	memberOf	memberOf	Role, Attribute
	telephoneNumber	Phone	Attribute
	mail	Email	Attribute

Based on the Attribute configuration shown, which statement accurately describes the status of attribute values?

- A. The attribute values of department, title, memberOf, telephoneNumber, mail are directly applied as ClearPass roles.
- B. The attribute values of department and memberOf are directly applied as ClearPass roles.
- C. Only the attribute value of company can be used in role mapping policies, not other attributes.
- D. Only the attribute value of department and memberOf can be used in role mapping policies.
- E. Only the attribute value of title, memberOf, telephoneNumber can be used in role mapping policies.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23 Which components can use Active Directory authorization attributes for the decision-making process? (Choose two.)

- A. Posture policy
- B. Role Mapping policy
- C. Certificate validation policy

- D. Profiling policy
- E. Enforcement policy

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Refer to the exhibit.



Configuration » Enforcement » Policies » Edit - Vlan enforcement

Enforcement Policies - Vlan enforcement

Summary	Enforcement	Rules
<u>Enforcement:</u>		
Name:	Vlan enforcement	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	Internet VLAN	
<u>Rules:</u>		
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 a ClearPass role Engineer authenticates to the network successfully on Saturday using connection protocol WEBAUTH?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

What is RADIUS CoA (RFC 3576) used for?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27 What types of files are stored in the Local Shared Folders database in ClearPass? (Choose two.)

- A. Backup Files
- B. Posture dictionaries
- C. Software image
- D. Device fingerprint dictionaries
- E. Log files

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

Refer to the exhibit.



Summary	Service	Authentication	Authorization	Roles	Enforcement
Used Cached Results:	<input type="checkbox"/> Used cached Roles and Posture attributes from previous sessions				
Enforcement Policy:	Mac Caching - Guest Access With MAC Caching ▼ Modify Add new Enforcement Policy				
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 CREATER_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 Caching Limit, MAC Caching - Guest MAC Caching [Update Endpoint Known] MAC Caching - Guest Do Expire, MAC Caching - Guest Expire Post Login		

A guest 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 guest's MAC address is accurate?

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

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29 Why can't the Onguard posture check be done during 802.1x authentication?

- A. Onguard uses TACACS so an additional service must be created.
- B. 802.1x is already secure so Onguard is not needed.
- C. Health Checks can't be used with 802.1x.
- D. Onguard uses RADIUS so an additional service must be created.
- E. Onguard uses HTTPS so an additional service must be created.

Correct Answer: E

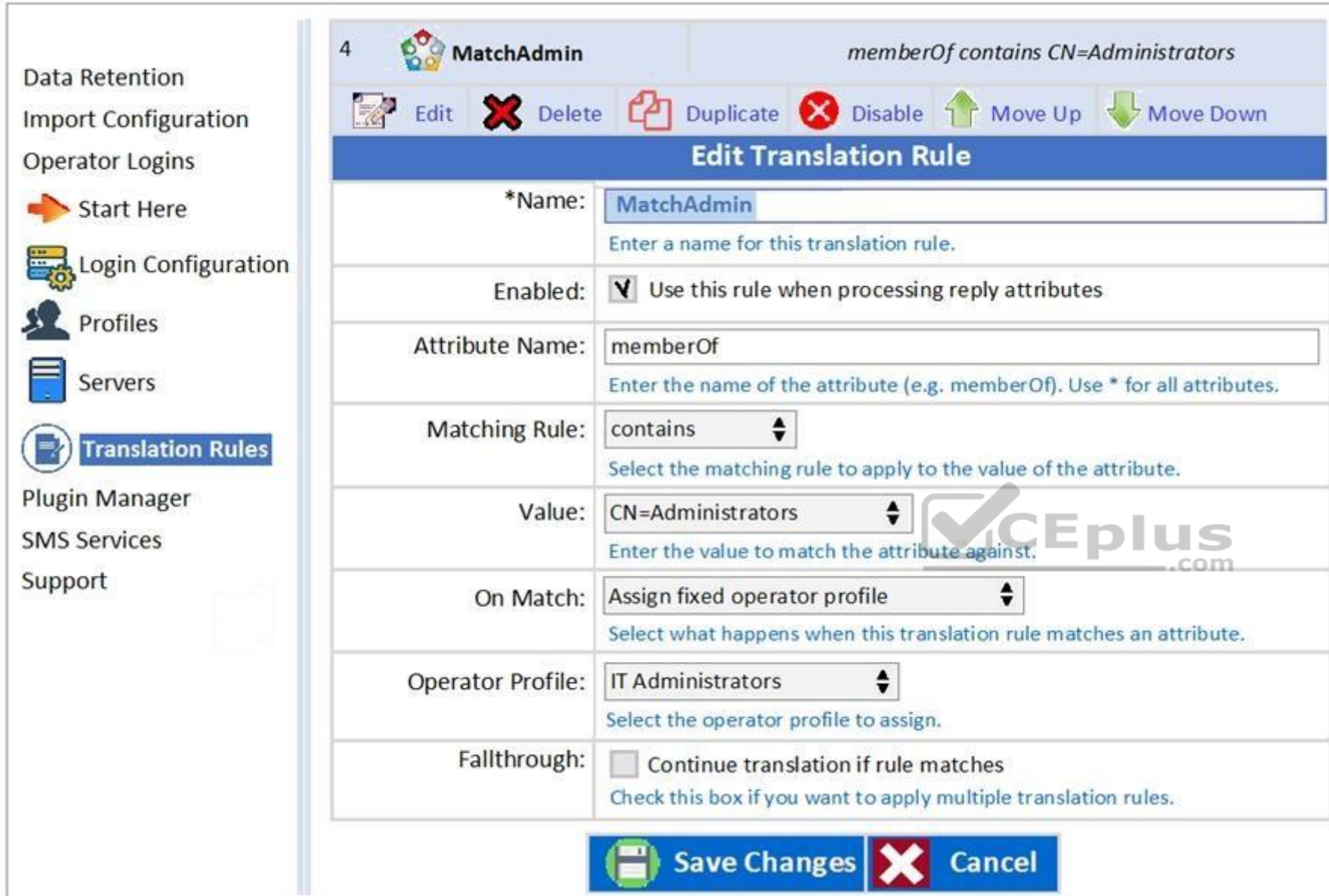
Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

Refer to the exhibit.



4 MatchAdmin *memberOf contains CN=Administrators*

Edit Delete Duplicate Disable Move Up Move Down

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.

Save Changes Cancel

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31 Which checks are made with Onguard posture evaluation in ClearPass?
(Choose three.)

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

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

Refer to the exhibit.

Summary	Service	Authentication	Authorization	Roles	Enforcement
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 <div> <div> [Endpoints Repository] [Local SQL DB] [Time Source] [Local SQL DB] </div> <div> Remove View Details Modify </div> </div> <div>-- Select to Add --</div>			

Based on the information, 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

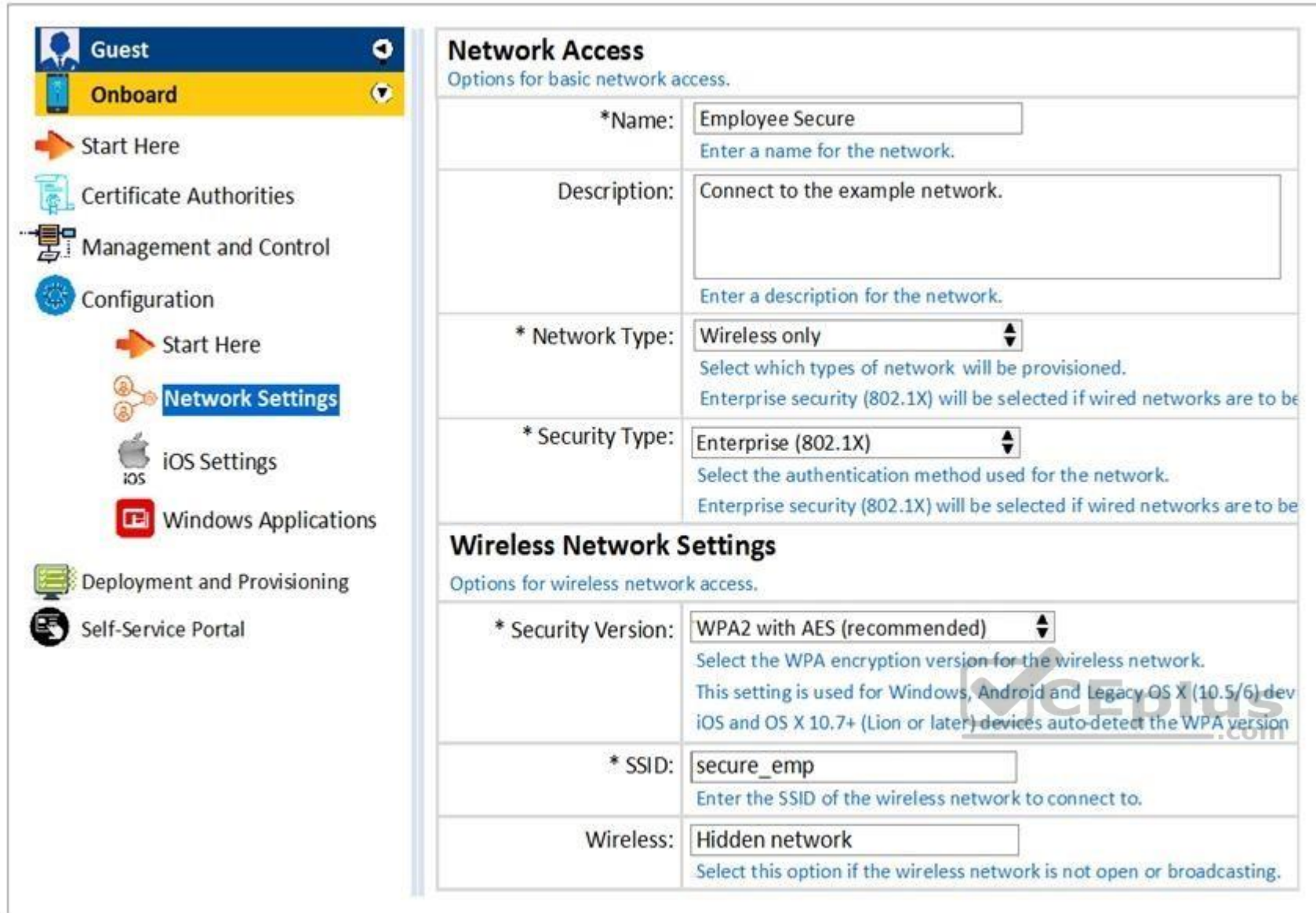
Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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

* 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

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) dev
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? (Choose two.)

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

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34 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 statement is true? (Choose two.)

- A. Both the primary and secondary nodes will respond to authentication requests sent to the Virtual IP address when the primary node is active.
- B. The primary node will respond to authentication requests sent to the Virtual IP address when the primary node is active.

- C. The NAD should be configured with the primary node IP address for RADIUS authentications on the 802.1x network.
- D. A new Virtual IP address should be created for each NAD.
- E. The NAD should be configured with the virtual IP address for RADIUS authentications on the 802.1x network.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

An SNMP probe is sent from ClearPass to a network access device but ClearPass is unable to get profiling information.

What could be a valid cause? (Choose three.)

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

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

Refer to the exhibit.



Summary	Policy	Mapping Rules
<u>Policy:</u>		
Policy Name:	WLAN role mapping	
Description:		
Default Role:	[Guest]	
<u>Mapping Rules:</u>		
Rules Evaluation Algorithm:	First applicable	
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 value is configured as "QA". The user authenticates from a laptop running MAC OS X.

Which role is assigned to the user in ClearPass?

- A. HR Local
- B. Remote Employee
- C. [Guest]
- D. iOS Device
- E. Executive

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37 What can ClearPass use to assign roles to the client during policy service processing? (Choose two.)

- A. Through a role mapping policy.
- B. From the attributes configured in a Network Access Device.

- C. From the server derivation rule in the Aruba Controller server group for the client.
- D. From the attributes configured in Active Directory.
- E. Roles can be derived from the Aruba Network Access Device.

Correct Answer: AD

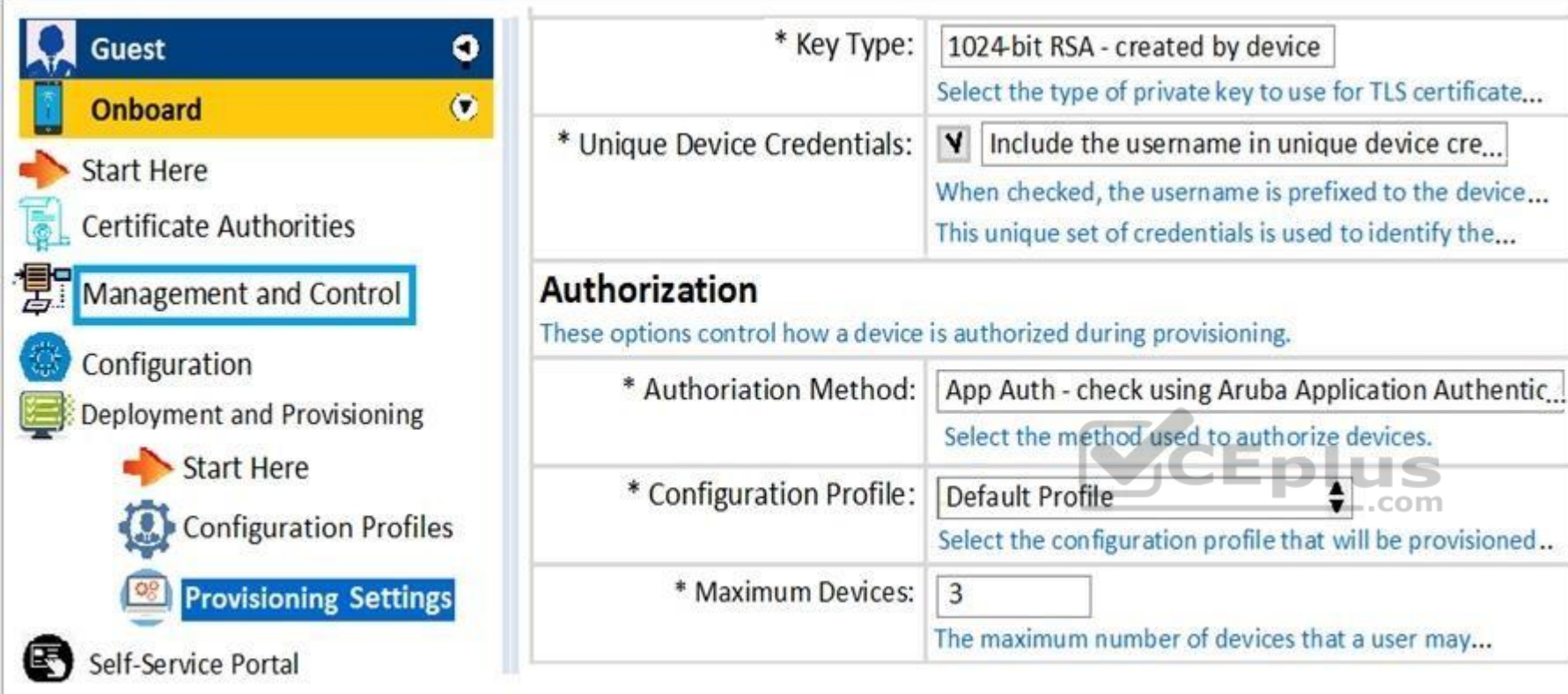
Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

Refer on the exhibit.



* Key Type:	1024-bit RSA - created by device
Select the type of private key to use for TLS certificate...	
* Unique Device Credentials:	<input checked="" type="checkbox"/> Include the username in unique device credentials
When checked, the username is prefixed to the device... This unique set of credentials is used to identify the...	
Authorization These options control how a device is authorized during provisioning.	
* Authorization Method:	App Auth - check using Aruba Application Authentication
Select the method used to authorize devices.	
* Configuration Profile:	Default Profile
Select the configuration profile that will be provisioned...	
* Maximum Devices:	3
The maximum number of devices that a user may...	

Based on the configuration for 'maximum devices' shown, which statement accurately describes its settings?

- A. It limits the number of devices that a single user can connect to the network.
- B. It limits the number of devices that a single user can Onboard.
- C. It limits the total number of Onboarded devices connected to the network.
- D. It limits the total number of devices that can be provisioned by ClearPass.
- E. With this setting, the user cannot Onboard any devices.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39 An Android device goes through the single-SSID Onboarding process and successfully connects using EAP-TLS to the secure network.

What is the order in which services are triggered?

- A. Onboard Provisioning, Onboard Authorization, Onboard Pre-Auth
- B. Onboard Authorization, Onboard Provisioning, Onboard Authorization
- C. Onboard Provisioning, Onboard Pre-Auth, Onboard Authorization
- D. Onboard Provisioning, Onboard Authorization, Onboard Provisioning
- E. Onboard Provisioning, Onboard Pre-Auth, Onboard Authorization, Onboard Provisioning

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

What does the Posture Token QUARANTINE imply?

- A. The client is compliant. However, there is an update available to remediate the client to HEALTHY state.
- B. The posture of the client is unknown.
- C. The client is infected and is a threat to other systems in the network.
- D. The client is out of compliance, but has HEALTHY state.
- E. The client is out of compliance.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41 Which step is required to use ClearPass as a TACACS+ Authentication server for a network device? (Choose two.)

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42 What must be configured to enable RADIUS authentication with ClearPass on a network access device (NAD)? (Choose 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 on the NAD.
- E. A bind username and bind password must be provided.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

Refer to the exhibit.

Certificate Issuing	
These options control how certificates are issued by this certificate authority.	
* Authority Info Access:	<input type="text" value="Include OCSP Responder URL"/> <p>Select the information about the certificate authority to include in the client certificate. Note that when an OCSP URL is provided, clients may need to access this URL to determine if the certifi...</p>
* OCSP URL:	<input type="text" value="http://cp62-server1/guest/mdps_ocsp.php/4"/> <p>The OCSP URL to be included in certificates.</p>
* Validity Period:	<input type="text" value="365"/> days <p>Maximum validity period for client certificates (in days).</p>
* Clock Skew Allowance:	<input type="text" value="15"/> days <p>Amount to pre/post date certificate validity period (in minutes).</p>
Subject Alternative Name:	<input type="text" value="Include Device information in TLS client certificates"/> <p>Store information about the device in the subjectAltName extension of the certificate. Note: Aruba OS version 6.1 or later is required to enable this feature.</p>
Retention Policy	
These options control how long to retain certificates after revocation or expiry.	
Minimum Period:	<input type="text" value="12"/> weeks <p>The minimum delay required before an expired certificate (or a rejected request) can be deleted. Leave blank to allow certificates and requests to be deleted at any time, including before expiration.</p>
Maximum Period:	<input type="text" value="52"/> weeks <p>The period after which an expired certificate (or a rejected request) will be automatically deleted. Leave blank to disable automatic deletion.</p>

What is the purpose of the 'Clock Skew Allowance' setting? (Choose tow.)

- A. to ensure server certificate validation does not fail due to client clock sync issues
- B. to set expiry time in client certificate to a few minutes longer than the default setting
- C. to adjust clock time on client device to a few minutes before current time
- D. to ensure client certificate validation does not fail due to client clock sync issues
- E. to set start time in client certificate to a few minutes before current time

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:




QUESTION 44

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.

 Quick Help
  Create
  More Options

Filter:

Username	Role	State	Activation	Expiration
 12063775	[Guest]	Expired	2015-08-27 00:19	Expired
 128962798	[Guest]	Expired	2015-08-27 00:19	Expired
 def@mycomany.com	[Guest]	Disabled	2015-08-22 20:51	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 not be able to access the Web Login page.
- B. The user will be able to login and authenticate successfully but they will be immediately disconnected after.
- C. The user will not be able to login and authenticate.
- D. The user will be able to login for the next 4.9 days, but after this they will not be able to login anymore.
- E. The user will be able to login and authenticate successfully, but get a quarantine role after logging in.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

Refer to the exhibit.

Profile	Attributes	Summary
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: (none)

Explanation

Explanation/Reference:

QUESTION 46

Refer to the exhibit.



Home » Configuration » Web Logins

RADIUS Web Login

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

Login Form
Options for specifying the behavior 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 Code and Anonymous require the account to have the Username Authentic...
Custom Form:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header of Footer HT...
Custom Labels:	<input type="checkbox"/> 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:	<input type="checkbox"/> RADIUS - check using a RADIUS request Select how username and password should be checked before processing to...
Terms:	<input type="checkbox"/> 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 ClearPass Guest as shown.

What is the purpose of the Pre-Auth Check?

- A. To -re-authenticate users when they're roaming from one NAD to another.
- B. To authenticate users before they launch the Web Login Page.
- C. To replace the need for the NAD to send an authentication request to ClearPass.
- D. To authenticate users after the NAD sends an authentication request to ClearPass.
- E. To authenticate users before the client sends the credentials to the NAD.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47 Which statement is true? (Choose two.)

- A. Mobile device Management is the result of Onboarding.
- B. Third party Mobile Device Management solutions can be integrated with ClearPass.
- C. Mobile Device Management is the authentication that happens before Onboarding.
- D. Mobile Device Management is an application container that is used to provision work applications.
- E. Mobile Device Management is used to control device functions post-Onboarding.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48 During a web login authentication, what is expected to happen as part of the Automated NAS login?

- A. NAD sends TACACS+ request to ClearPass. B. ClearPass sends TACACS+ request to NAD.
- C. Client device sends RADIUS request to NAD.
- D. NAD sends RADIUS request to ClearPass.E. ClearPass sends RADIUS request to NAD.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49 What is the purpose of the Audit Viewer in the Monitoring section of ClearPass Policy Manager?

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



Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

Refer to the exhibit.

Summary	Policy	Mapping Rules
Policy:		
Policy Name:	WLAN role mapping	
Description:		
Default Role:	[Guest]	
Mapping Rules:		
Rules Evaluation Algorithm:	First applicable	
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:UserDN EXISTS)	[Employee]	
5. (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	
6. (Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User	

An AD user's department attribute value is configured as "Product Management". The user connects on Monday to a NAD that belongs to the Device Group HQ.

Which role is assigned to the user in ClearPass?

- A. Linux User
- B. Executive
- C. [Employee]
- D. [Guest]
- E. HR Local

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51 What are Operator Profiles used for?

- A. To map AD attributes to admin privilege levels in ClearPass Guest.

- B. To enforce role based access control for ClearPass Guest Admin users.
- C. To enforce role based access control for Aruba Controllers.
- D. To assign ClearPass roles to guest users.
- E. To enforce role based access control for ClearPass Policy Manager users.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

Refer to the exhibit.

Summary	Service	Authentication	Authorization	Roles	Enforcement
<div> <div>Authorization Methods:</div> <div> <div>[EAP PEAP]</div> <div>[EAP TLS]</div> <div>[EAP MSCHAPv2]</div> </div> <div> <div>Move up</div> <div>Move down</div> <div>Remove</div> <div>View details</div> <div>Modify</div> </div> </div>					
<div> <div>-- Select to Add --</div> </div>					
<div> <div>Authentication Sources:</div> <div> <div>[Local User Repository] [Local SQL DB]</div> <div>remotelab AD [Active Directory]</div> </div> <div> <div>Move up</div> <div>Move down</div> <div>Remove</div> <div>View details</div> <div>Modify</div> </div> </div>					

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 local user repository and remotelab AD, 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 remotelab AD but is present in the local user repository, a reject message is sent back to the NAD.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

An organization has decided to implement dual SSID Onboarding. An administrator has used the Onboard service template to create services for dual SSID Onboarding.

Which statement is true?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

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: (none)

Explanation

Explanation/Reference:



QUESTION 55

Which statement is true about the configuration of a generic LDAP server as an External Authentication server in ClearPass? (Choose three.)

- A. Generic LDAP Browser can be used to search the Base DN.
- B. An administrator can customize the selection of attributes fetched from an LDAP server.
- C. The bind DN can be in the administrator@domain format.
- D. A maximum of one generic LDAP server can be configured in ClearPass.
- E. A LDAP Browser can be used to search the Base DN.

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

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:	<input type="text" value="GuestNetwork"/> Enter a name for this web login page.
Page Name:	<input type="text" value="Aruba_login"/> Enter a name for this web login page. The web login will be accessible from "/guest/page_name.php".
Description:	<input type="text"/> Comments or descriptive text about the web login.
* Vendor Settings:	<div>Aruba Networks ▼</div> Select a predefined group of settings suitable for standard network configurations.
Address:	<input type="text" value="securelogin.arubanetworks.com"/> Enter the IP address or hostname of the vendor's product here.
Secure Login:	<div>Use Vendor default ▼</div> Select a security option to apply to the web login process.
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different add The address above will be used whenever the parameter is not available or fails the r

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 the client to POST the user credentials to the NAD.
- B. For ClearPass to send a RADIUS request to the NAD.
- C. For ClearPass to send a TACACS+ request to the NAD.
- D. For appending to the Web Login URL, after the page name.
- E. For appending to the Web Login URL, before the page name.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

Refer to the exhibit.

Summary	Policy	Posture Plugins	Rules
Policy Name:	Employee Posture Policy		
Description:			
Posture Agent:	<input type="radio"/> NAP Agent <input checked="" type="radio"/> OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	<input checked="" type="radio"/> Windows <input type="radio"/> Linux <input type="radio"/> Mac OS X		

Based on the Posture Policy configuration shown, above, which statement is true?

- A. This Posture Policy can only be applied to an 802.1x wired service not 802.1x wireless.
- B. This Posture Policy checks the health status of devices running Windows, Linux and Mac OS X.
- C. This Posture Policy can use either the persistent or dissolvable Onguard agent to obtain the statement of health.
- D. This Posture Policy checks for presence of a firewall application in Windows devices.
- E. This Posture Policy checks with a Windows NPS server for posture tokens.



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

Filter: Role ▼ contains employee + Go Clear Filter

#	<input type="checkbox"/>	User ID ▲	Name	Role
1.	<input type="checkbox"/>	john	john	[Employee]
2.	<input type="checkbox"/>	mike	mike	[Employee]
3.	<input type="checkbox"/>	neil	neil	[Employee]

Showing 1-3 of 3

Based on the Local User repository in ClearPass shown, which Aruba firewall role will be assigned to “mike” when this user authenticates Aruba Controller?

- A. We can't know this from the screenshot above.
- B. mike

C. Employee
D. john

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

