

Exam Questions HPE6-A68

Aruba Certified Clearpass Professional 6.7

<https://www.2passeasy.com/dumps/HPE6-A68/>



NEW QUESTION 1

Refer to the exhibit.

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

Services - MAC Caching - Guest Access With MAC Caching

Summary Service Authentication Authorization Roles **Enforcement**

Use Cached Results: Use 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 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 Caching - 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.

Answer: D

NEW QUESTION 2

Refer to the exhibit.

Search

Search Type: ☒ Search All Records ☐ Search Reports ☐ Search Alerts

Select Template: **RADIUS Failed Authentications** [Create Report](#)

Rules: ☒ AND ☐ OR

Type	Name	Operator	Value	+/-
Auth	Protocol	EQUALS	RADIUS	
Auth	Error Code	NOT_EQUALS	0	<input type="button" value="-"/> <input type="button" value="0"/> <input type="button" value="+"/>

Select date range: From : 2013-05-20 18:38:52 To : 2013-05-29 18:38:51 [Search](#)

Show 10 entries

Auth.Username	Auth.Host MAC Address	Auth.Network Device	Auth.Service	CppmIrrorCode.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.

Answer: E

NEW QUESTION 3

Refer to the exhibit.

4 **MatchAdmin** *memberOf contains CN=Administrators*

Edit Delete Duplicate Disable Move Up Move Down

Edit Translation Rule

*Name:
Enter a name for this translation rule.

Enabled: ☒ Use this rule when processing reply attributes

Attribute Name:
Enter the name of the attribute (e.g. memberOf). Use * for all attributes.

Matching Rule:
Select the matching rule to apply to the value of the attribute.

Value:
Enter the value to match the attribute against.

On Match:
Select what happens when this translation rule matches an attribute.

Operator Profile:
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 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.

Answer: A

NEW QUESTION 4

Refer to the exhibit.

Administration » Dictionaries » TACACS+ Services

TACACS+ Services Dictionaries

TACACS+ Service Dictionary Attributes

#	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

Close

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

Answer: C

NEW QUESTION 5

Refer to the exhibit.

Summary	Input	Output
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.

Answer: B

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.

References: CLEARPASS ONGUARD CONFIGURATION GUIDE (July 2015), page 13

[https://community.arubanetworks.com/aruba/attachments/aruba/aaa-nac-guest-access-byod/21122/1/OnGuard%](https://community.arubanetworks.com/aruba/attachments/aruba/aaa-nac-guest-access-byod/21122/1/OnGuard%20Configuration%20Guide.pdf)

NEW QUESTION 6

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.

Answer: C

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 wired switch, a separate 802.1x authentication must be used prior to the OnGuard posture check. In this example, an 802.1x PEAP-EAP-MSCHAPv2 authentication is completed first. A separate WebAuth service must be setup with posture checks to use the OnGuard agent.

References: MAC Authentication and OnGuard Posture Enforcement using Dell WSeries ClearPass and Dell Networking Switches (August 2013), page 21

NEW QUESTION 7

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?

Configuration » Enforcement » Policies » Edit - Vlan enforcement

Enforcement Policies - Vlan enforcement

Summary	Enforcement	Rules
Enforcement:		
Name:	Vlan enforcement	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	Internet VLAN	
Rules:		
Rules Evaluation Algorithm: First applicable		
Conditions	Actions	
(Tips:Role EQUALS Engineer)		
1. AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday)	Full Access VLAN	
AND (Connection:Protocol EQUALS RADIUS)		
(Tips:Role EQUALS Manager)		
2. AND (Connection:Protocol BELONGS_TO RADIUS, TACACS, WEBAUTH, Application)	Full Access VLAN	
(Tips:Role EQUALS Engineer)		
3. AND (Connection:Protocol BELONGS_TO WEBAUTH)	Employee Vlan	

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

Answer: B

NEW QUESTION 8

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.

Answer: BD

NEW QUESTION 9

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.

Answer: B

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.

References:

<https://community.arubanetworks.com/t5/Security/Step-by-Step-Controller-CPPM-6-5-Captive-Portal-authentic>

NEW QUESTION 10

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

Answer: D

NEW QUESTION 10

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

Answer: BD

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

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 114

[https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%](https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%206.5%20User%20Guide%20October%202015.pdf)

NEW QUESTION 14

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="Guest Network"/> Enter a name for this web login page.
Page Name:	<input type="text" value="Aruba_login"/> Enter a page name for this web login. The web login be accessible from <code>"/guest/page_name.php"</code> .
Description:	<div></div> Comments or descriptive text about the web login.
* Vendor Settings:	<div><input type="text" value="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><input type="text" value="Use vendor default"/></div> Select a security option to apply to the web login process.
Dynamic Address:	<div><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 addresses. The address above will be used whenever the parameter is not available or fails.</div>

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.

Answer: C

NEW QUESTION 19

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: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. Executive
- E. IOS Device

Answer: C

Explanation:

None of the Listed Role Name conditions are met.

NEW QUESTION 21

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

Filter: ▼ contains

#	<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

- A. We can't know this from the screenshot above.
- B. mike
- C. Employee
- D. john

Answer: A

NEW QUESTION 23

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

Answer: D

NEW QUESTION 27

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.

Answer: AC

NEW QUESTION 29

Refer to the exhibit.

Captive Portal Authentication Profile > default **Show Reference** **Save As** **Reset**

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

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

Answer: E

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.

References:

http://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Captive_Portal/C

NEW QUESTION 30

What does Authorization allow users 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 sored in internal databases for Enforcement, but not external databases.

Answer: A

NEW QUESTION 31

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.

Answer: B

NEW QUESTION 34

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

Answer: ACE

NEW QUESTION 35

Refer to the exhibit.

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

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

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

Answer: BD

NEW QUESTION 40

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

Answer: A

NEW QUESTION 43

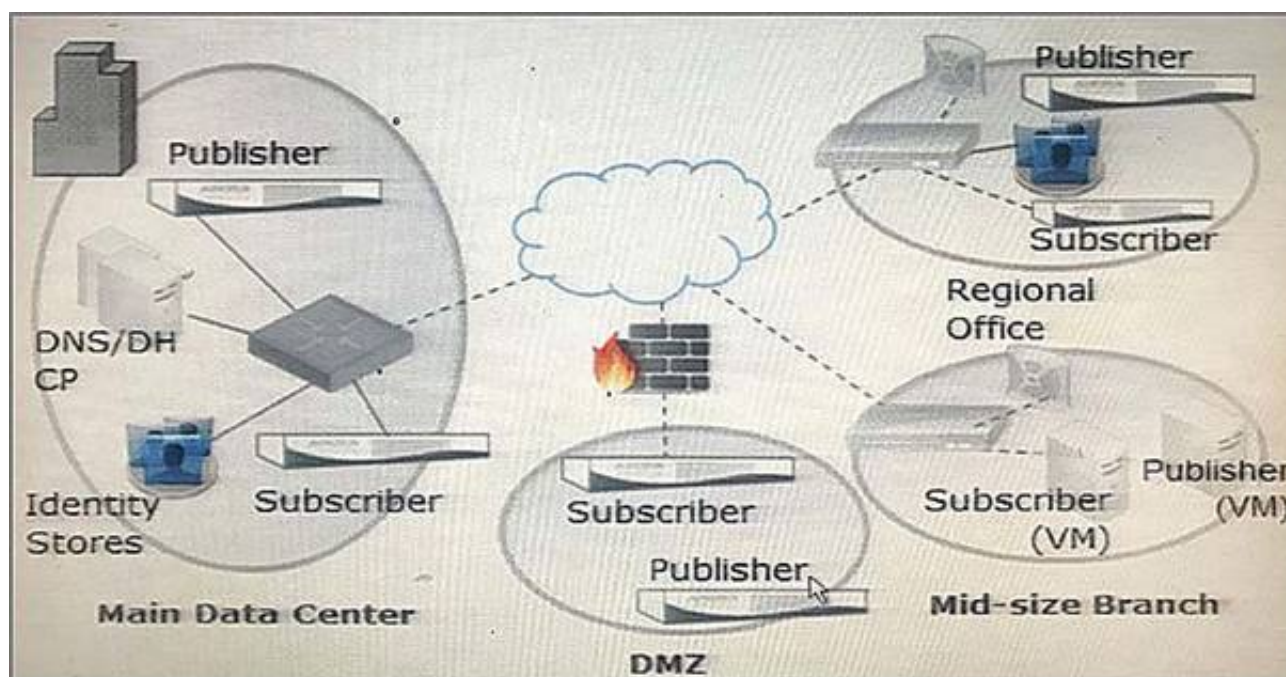
Which statement is true? (Choose two.)

- 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.

Answer: BE

NEW QUESTION 48

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

Answer: A

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.

References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster%20Deploy

NEW QUESTION 53

Refer to the exhibit.

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

<div> <div>Quick Help</div> <div>Preview Form</div> </div>				
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
<div> <div>Edit</div> <div>Edit base field</div> <div>Remove</div> <div>Insert before</div> <div>Insert After</div> <div>Enable Field</div> </div>				
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.

Answer: A

Explanation:

References:

<https://community.arubanetworks.com/t5/AAA-NAC-Guest-Access-BYOD/expire-timezone-field-is-not-showin>

NEW QUESTION 55

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

Answer: AE

NEW QUESTION 57

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

Answer: A

NEW QUESTION 60

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

Answer: B

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)

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 564

<https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%>

NEW QUESTION 65

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

Answer: CD

NEW QUESTION 67

Refer to the exhibit.

* Key Type:	1024-bit RSA - created by device Select the type of private key to use for TLS certificates.
* Unique Device Credentials:	<input checked="" type="checkbox"/> Include the username in unique device credentials 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 ne
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 to devices.
* Maximum Devices:	3 The maximum number of devices that a user may provision. Use 0 for unlimit

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

- A. The user cannot Onboard any devices.
- B. It limits the total number of devices that can be provisioned by ClearPass.
- C. It limits the total number of Onboarded devices connected to the network.

- D. It limits the number of devices that a single user can Onboard.
E. It limits the number of devices that a single user can connect to the network.

Answer: D

NEW QUESTION 71

Refer to the exhibit.

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.

Answer: DE

NEW QUESTION 73

Refer to the exhibit.

Summary	Enforcement	Rules
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	
(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

Answer: E

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

References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Rules

NEW QUESTION 77

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

Answer: E

NEW QUESTION 82

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.

Answer: A

NEW QUESTION 86

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

Answer: A

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.

References: ClearPass Profiling TechNote (2014), page 23

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

NEW QUESTION 87

Use the arrows to sort the steps to request a Policy Service on the left into the order they are performed on the right.

Steps to Request a Policy Service Order Performed

ClearPass tests the request against Service Rules to select a Policy Service.

ClearPass applies the Enforcement Policy

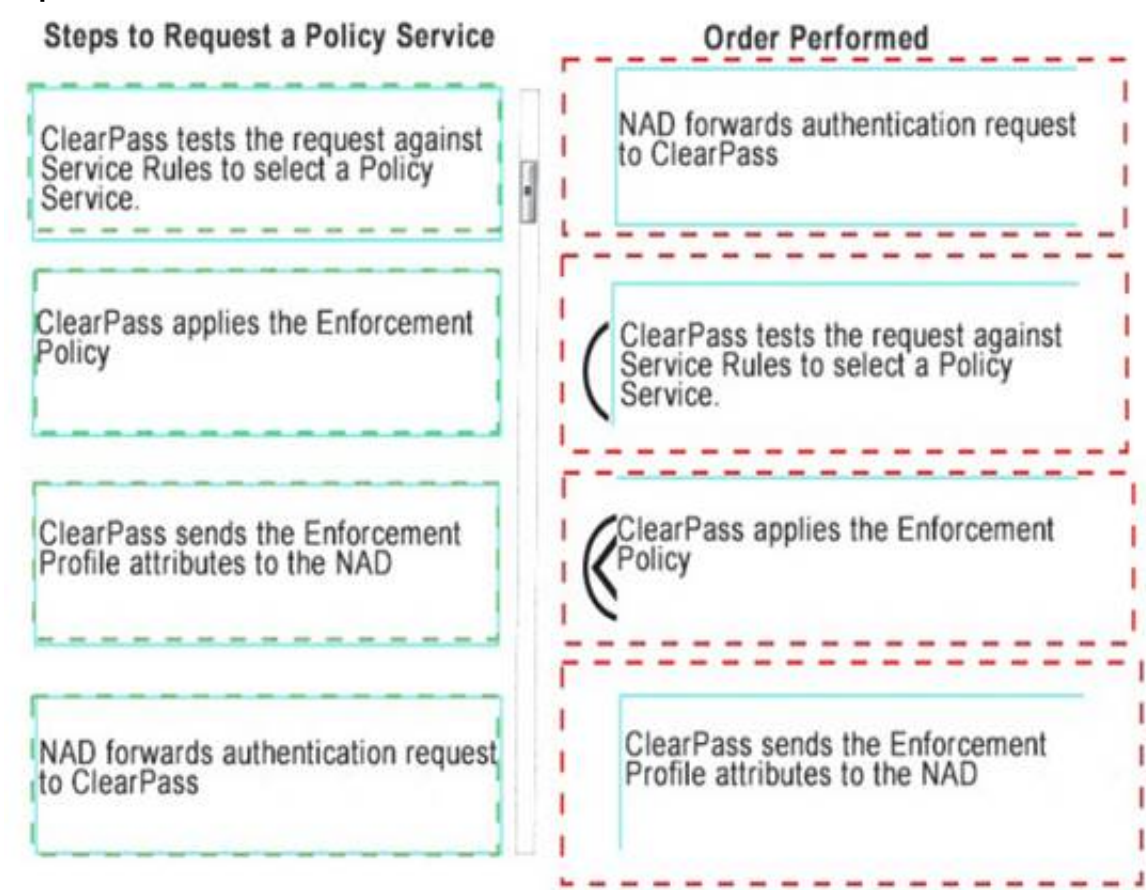
ClearPass sends the Enforcement Profile attributes to the NAD

NAD forwards authentication request to ClearPass

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 89

Refer to the exhibit.

Certificate Issuing These options control how certificates are issued by this certificate authority.	
* Authority Info Access:	<div>Include OCSP Responder URL</div> <div>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 in order to determine if the certificate is still valid.</div>
OCSP URL:	<div>http://cp62-server1/guest/mdps_ocsp.php/4</div> <div>The OCSP URL to be included in certificates.</div>
* Validity Period:	<div>365 days</div> <div>Maximum validity period for client certificates (in days).</div>
* Clock Skew Allowance:	<div>15</div> <div>Amount to pre/post date certificate validity period (in minutes).</div>
Subject Alternative Name:	<div><input checked="" type="checkbox"/> Include device information in TLS client certificates</div> <div>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.</div>

What is the purpose of the 'Clock Skew Allowance' setting? (Select two.)

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

Answer: D

Explanation:

Clock Skew Allowance adds a small amount of time to the start and end of the client certificate's, not the server certificate's, validity period. This permits a newly issued certificate to be recognized as valid in a network where not all devices are perfectly synchronized.

References:

<http://www.arubanetworks.com/techdocs/ClearPass/6.6/Guest/Content/Onboard/EditingCASettings.htm>

NEW QUESTION 92

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

Answer: C

NEW QUESTION 97

Refer to the exhibit.

Configuration » Enforcement » Policies » Edit - Onboard Provisioning - Aruba

Enforcement Policies - Onboard Provisioning - Aruba

Summary	Enforcement	Rules
Enforcement:		
Name:	Onboard Provisioning - Aruba	
Description:	Enforcement policy controlling network access for device provisioning	
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
Rules:		
Rules Evaluation Algorithm: First applicable		
Conditions	Actions	
1. (Authentication:OuterMethod EQUALS EAP-TLS)	[Allow Access Profile], Onboard Post-Provisioning - Aruba	
2. (Authentication:Source EQUALS [Onboard Devices Repository])	[Allow Access Profile], Onboard Post-Provisioning - Aruba	
3. (Authentication:Source NOT_EQUALS [Onboard Devices Repository])	[Allow Access Profile], Onboard Pre-Provisioning - Aruba	

Based on the Enforcement Policy configuration shown, which Enforcement Profile will an employee receive when connecting an IOS device to the network or the first time using EAP-PEAP?

- A. Deny Access Profile
- B. Onboard Device Repository
- C. Cannot be determined
- D. Onboard Post-Provisioning – Aruba
- E. Onboard Pre-Provisioning – Aruba

Answer: E

NEW QUESTION 101

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.

Answer: D

NEW QUESTION 106

Refer to the exhibit.

Summary	Policy	Mapping rules
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

Answer: C

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.

References: CLEARPASS ONGUARD CONFIGURATION GUIDE (July 2015), page 27

NEW QUESTION 108

Refer to the exhibit.

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

Role Mappings - [Guest Roles]

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

Buttons: Add Rule, Move Up, Move Down

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

Answer: C

NEW QUESTION 109

Refer to the exhibit.

Configuration » Services » Edit - CompanyX Onboard Authorization

Services - CompanyX Onboard Authorization

Summary Service Authentication Roles Enforcement

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

1. (Date:Day-of-Week EQUALS 1)

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Enforcement Profiles

[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 EAP-TLS 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.

Answer: B

NEW QUESTION 114

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

Answer: DE

Explanation:

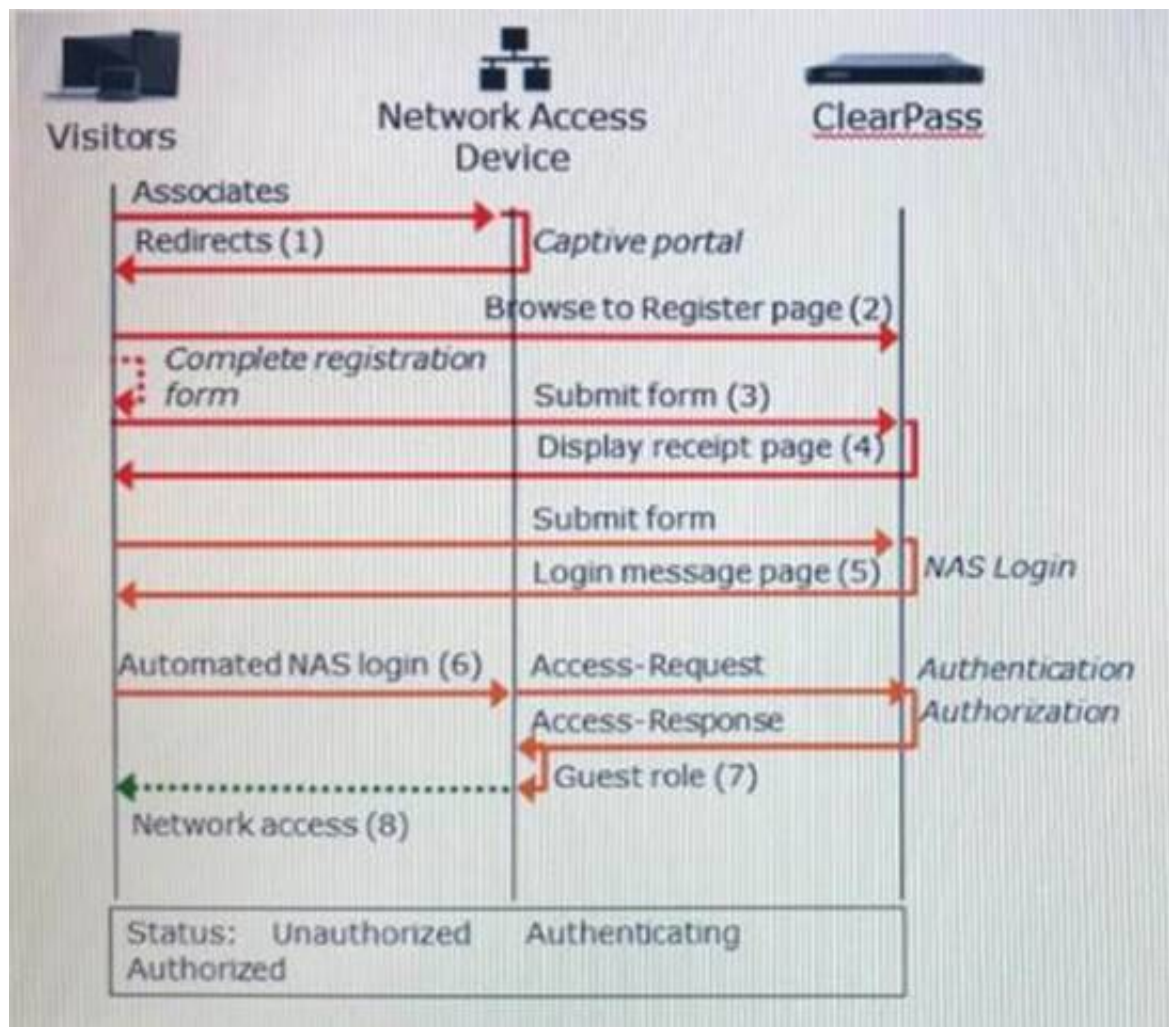
When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other. Certificates must meet specific requirements both on the server and on the client for successful authentication.

References:

<https://support.microsoft.com/en-us/help/814394/certificate-requirements-when-you-use-eap-tls-or-peap-with-ea>

NEW QUESTION 119

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

Answer: E

NEW QUESTION 121

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

Answer: C

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.

NEW QUESTION 122

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			
		[Endpoints Repository] [Local SQL DB]		Remove	
		[Time Source] [Local SQL DB]		View Details	
				Modify	
		-- Select to Add --			

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

Answer: D

NEW QUESTION 127

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.

The screenshot shows a configuration form for the RADIUS Web Login Guest Network. The 'Pre-Auth Check' section is highlighted, showing a dropdown menu set to 'RADIUS - check using a RADIUS request'. Other sections include 'Authentication' with a dropdown for 'Credentials - Require a username and password', 'Custom Form' with a checkbox for 'Provide a custom login form', 'Custom Labels' with a checkbox for 'Override the default labels and error messages', and 'Terms' with a checkbox for 'Require a Terms and Conditions confirmation'.

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 ClearPass
- 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

Answer: B

NEW QUESTION 128

What does the Posture Token QUARANTINE imply?

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

Answer: E

NEW QUESTION 129

Which device type supports Exchange ActiveSync configuration with Onboard?

- A. Linux laptop
- B. Mac OS X device
- C. Apple iOS device
- D. Windows laptop
- E. Android device

Answer: C

Explanation:

Exchange ActiveSync configurations you define can be used in configuration profiles to automatically configure an email account on an iOS device.

References:

<http://www.arubanetworks.com/techdocs/ClearPass/6.6/Guest/Content/Onboard/CreateEditActiveSync.htm>

NEW QUESTION 130

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.

Answer: E

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.

References:

http://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Enfor

NEW QUESTION 131

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?

Configuration » Enforcement » Policies » Edit - Vlan enforcement

Enforcement Policies - Vlan enforcement

Summary

Enforcement

Rules

Enforcement:

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

Rules:

Rules Evaluation Algorithm: First applicable

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

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

Answer: B

NEW QUESTION 132

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

Answer: E

Explanation:

The conditions of the Executive Role is met.

NEW QUESTION 134

Refer to the exhibit.

Refer to the exhibit.

Configuration > Services > Add

Services

Service

Authentication

Roles

Enforcement

Summary

Type: 802.1X Wireless

Name: Test device group

Description: 802.1X Wireless Access Service

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Connection	NAD-IP-Address	BELONGS_TO_GROUP	HQ
4. Click to add...			

Under which circumstances will ClearPass select the Policy Service named 'Test device group'?

- A. when the NAD belongs to an Airware device group HQ
- B. when the ClearPass IP address is part of the device group HQ
- C. when the Aruba access point that the client is associated to is part of the device group HQ
- D. when an end user IP address is part of the device group HQ
- E. when the IP address of the NAD is part of the device group HQ

Answer: E

NEW QUESTION 137

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.

Answer: AC

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.

NEW QUESTION 138

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual HPE6-A68 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the HPE6-A68 Product From:

<https://www.2passeasy.com/dumps/HPE6-A68/>

Money Back Guarantee

HPE6-A68 Practice Exam Features:

- * HPE6-A68 Questions and Answers Updated Frequently
- * HPE6-A68 Practice Questions Verified by Expert Senior Certified Staff
- * HPE6-A68 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * HPE6-A68 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year