PassQueen
a.k.a dumpsqueen.com

Aruba Certified ClearPass Professional (ACCP) 6.7

HP HPE6-A68

Version Demo

Total Demo Questions: 18

Total Premium Questions: 186

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, ClearPass Policy Manager	102
Topic 2, ClearPass Guest	37
Topic 3, ClearPass OnGuard	15
Topic 4, ClearPass Onboard	27
Topic 5, ClearPass Insight	3
Topic 6, Mix Questions	2
Total	186

QUESTION NO: 1

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: B D

Explanation:

ClearPass Policy Manager supports both LDAP server and Active Directory as external identity stores used in authentication and authorization workflows. An LDAP server can provide directory-based user or device records, including attributes such as group membership, organizational unit, or other directory fields. ClearPass can query those attributes and use them in role mapping and enforcement-policy decisions.

Active Directory is also a supported authentication source. ClearPass can join an Active Directory domain and use AD to validate credentials and retrieve authorization-relevant information, particularly user and computer group membership. This lets administrators apply differentiated network-access policies based on the directory identity and group assignments associated with a connecting user or endpoint.

In ClearPass terminology, these are configured under Authentication Sources and can supply the identity and attribute data required for policy evaluation. The resulting attributes may be mapped to ClearPass roles and then evaluated by enforcement policies to determine the access returned to the network device. Aruba's ClearPass Policy Manager documentation lists Active Directory and LDAP among the supported authentication-source types and describes their use in policy processing. See the ClearPass 6.7 Authentication Sources documentation and the Active Directory authentication-source documentation.

QUESTION NO: 2 - (SIMULATION)

Refer to the exhibit.

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

ANSWER: See the explanation for the answer

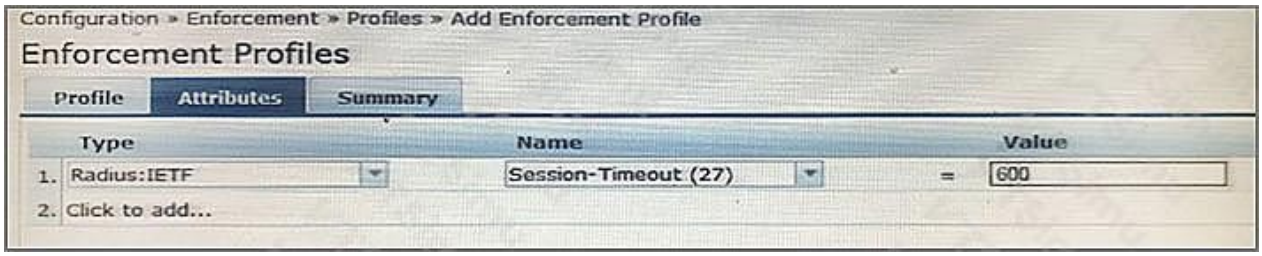
Explanation:

Cannot be determined from the supplied material. The question refers to a Policy Simulation exhibit, but no exhibit (and no answer choices) is included in the JSON. The simulation status must be read from the displayed authentication, role-mapping, and enforcement results—for example, whether each stage is marked successful or failed and which enforcement profile was selected.

Please provide the referenced screenshot/exhibit to identify the accurate status statement.

QUESTION NO: 3

Refer to the exhibit.



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

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

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

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

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

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

ANSWER: E

Explanation:

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. An Enforcement Profile that returns the standard RADIUS Session-Timeout attribute supplies a duration value, in seconds, as part of the authorization response. The Network Access Device, also called the NAS in RADIUS terminology, receives this attribute when it accepts the authentication request and is responsible for enforcing the resulting session limit. Therefore, a value of 600 instructs the NAD to limit the authorized connection to ten minutes.

This behavior follows the definition of Session-Timeout in RADIUS: it is included in an Access-Accept and specifies the maximum number of seconds that service may be provided to the user before termination. ClearPass acts as the RADIUS server and returns the configured enforcement attribute; it does not itself maintain a countdown for this attribute or need to issue a later change-of-authorization message to make the original timeout effective. See the IETF definition of Session-Timeout in RFC 2865 and Aruba's ClearPass Enforcement Profiles documentation.

QUESTION NO: 4

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

[Guest]

POII

Policy Name: Description: Default Eole:

Mapping Rules:

W EN role mapping

Rules Evaluation Algorithm: First applicable Conditions

1. (AutnoriZation:remotelad AD:Depanment EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)

Role Name Executive

z. (AuthoriZati0fl:tEndpoints Repository]:05 Family EQUALS IGNORE CASE Windows) Vendor

3. (AutJoriZatÍ0fl:tEndpoints Reoository]:Category CONTAINS SmanDevice) i0S Device AND (AuthoriZation:[Endg0l0tS R0Ç0Sitory]:05 Family EQUALS IGNORE CASE Apple)

4. (AutnoriZation:remotelab AD:Depanment EQUALS H R)

OR (Connection:NAD-IP-Address BELONGS TO GROUP Eq)

OR (Date:Day-of-week NOT BELONGS TO Saturday, Sunday)

s. (Hon:os/ype cox Aixs redoraj

OR (Host:0SType CONTAINS Redhat)

OR (Host:0SType CONTAINS Ubuntu)

6. (Connection:NAD-IP-Address BELONGS TO GROUP Remote NAD)

HR Local

Linux User

&9M0tP ÉM gl0ÿ9 9

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:

[Guest] is assigned because it is the Role Mapping policy's configured default role. ClearPass evaluates role-mapping rules using the configured *First applicable* algorithm, proceeding through the rules in order until it finds a rule whose conditions evaluate as true. For this authentication, the available facts are an Active Directory department value of *QA* and a macOS laptop. Those facts do not produce an applicable role-mapping result before the policy reaches its fallback behavior. ClearPass therefore assigns the default role, **[Guest]**.

Role mapping is the stage in ClearPass Policy Manager that converts authentication and authorization attributes—such as directory attributes, endpoint-profile data, connection data, and time-based data—into one or more local roles. The resulting role is then available to subsequent enforcement-policy evaluation. A default role is important because it provides a deterministic authorization outcome when no explicitly defined mapping rule matches the request, rather than leaving the session without a mapped role. Aruba's ClearPass documentation describes role mapping and the role-mapping policy workflow in the ClearPass Policy Manager Role Mapping documentation and the broader authorization flow in the ClearPass Services documentation.

QUESTION NO: 5

What is the certificate format PKCS #7, or .p7b, used for?

A. Certificate Signing Request

B. Binary encoded X.509 certificate

C. Binary encoded X.509 certificate with public key

D. Certificate with an encrypted private key

E. Certificate chain

ANSWER: E

Explanation:

PKCS #7 (.p7b or .p7c) is used to package and distribute certificates, most commonly an end-entity certificate together with one or more intermediate CA certificates that form its certification path. This makes “Certificate chain” the correct answer. The format is designed as a cryptographic message container and, in the certificate-distribution use case, carries X.509 certificates and certificate-revocation lists without including the certificate subject’s private key. A server or client can import the P7B bundle to obtain the certificates needed to establish trust through the issuing hierarchy. P7B files are commonly Base64-encoded, with PKCS7 BEGIN/END markers, although the underlying PKCS #7/CMS structure may also be encoded in binary DER. Aruba documentation specifically describes P7B as containing certificates and chain certificates, not a private key, and notes its support in environments such as Microsoft Windows and Java Tomcat. This is particularly useful when administrators need to import a signed certificate and its intermediate CA chain as one file, while retaining the private key separately in the system or keystore where the certificate request was generated. See Aruba’s Various Certificate Formats reference and the IETF’s PKCS #7 specification.

QUESTION NO: 6

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: A C

Explanation:

To use ClearPass as a TACACS+ authentication server, the network device must be configured to send its administrative-access TACACS+ requests to ClearPass. This includes defining ClearPass as the TACACS+ server on the device, using the appropriate ClearPass IP address, shared secret, and TACACS+ service settings. Without that device-side server configuration, the device has no TACACS+ path through which to submit administrator authentication and authorization requests to ClearPass.

ClearPass must also return the authorization attributes that establish the administrator’s permitted access after authentication. Configuring a TACACS Enforcement Profile for the desired privilege level supplies those TACACS+ authorization attributes, such as a privilege level or vendor-specific command/role attributes appropriate to the device platform. The enforcement profile is applied by an enforcement policy, commonly based on the authenticated user’s directory-group membership, so ClearPass can assign the intended administrative privilege level consistently. Aruba’s ClearPass documentation describes TACACS+ enforcement profiles as the mechanism for returning TACACS+ authorization information and documents configuration of network devices as TACACS+ clients. See the ClearPass Enforcement Profiles documentation and the ClearPass Network Devices documentation.

QUESTION NO: 7

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

A. Guest device fingerprinting

B. Guest endpoint health assessment

C. Sponsor based guest user access

D. Guest user self-registration for access

E. Guest personal device onboarding

ANSWER: C D

Explanation:

ClearPass Guest is the application module used to create and manage temporary guest identities and the workflows through which those identities obtain network access. Therefore, **Sponsor based guest user access** requires the ClearPass Guest application license because a sponsor uses the Guest interface and its role-based workflow to create, authorize, and manage a visitor account. The account can then be issued credentials and associated with an access duration, role, or other guest-access controls.

Guest user self-registration for access also requires the ClearPass Guest application license. This capability is delivered through Guest web-login and self-service workflows, where visitors register through a captive portal and ClearPass Guest handles account creation, validation, credential delivery, and lifecycle controls. These are core ClearPass Guest functions rather than merely standard RADIUS policy evaluation. Aruba's ClearPass documentation describes Guest as the component for sponsored and self-registered visitor access and documents the licensing of ClearPass application modules. See the Aruba ClearPass Guest overview and the ClearPass licensing documentation.

QUESTION NO: 8

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: A D

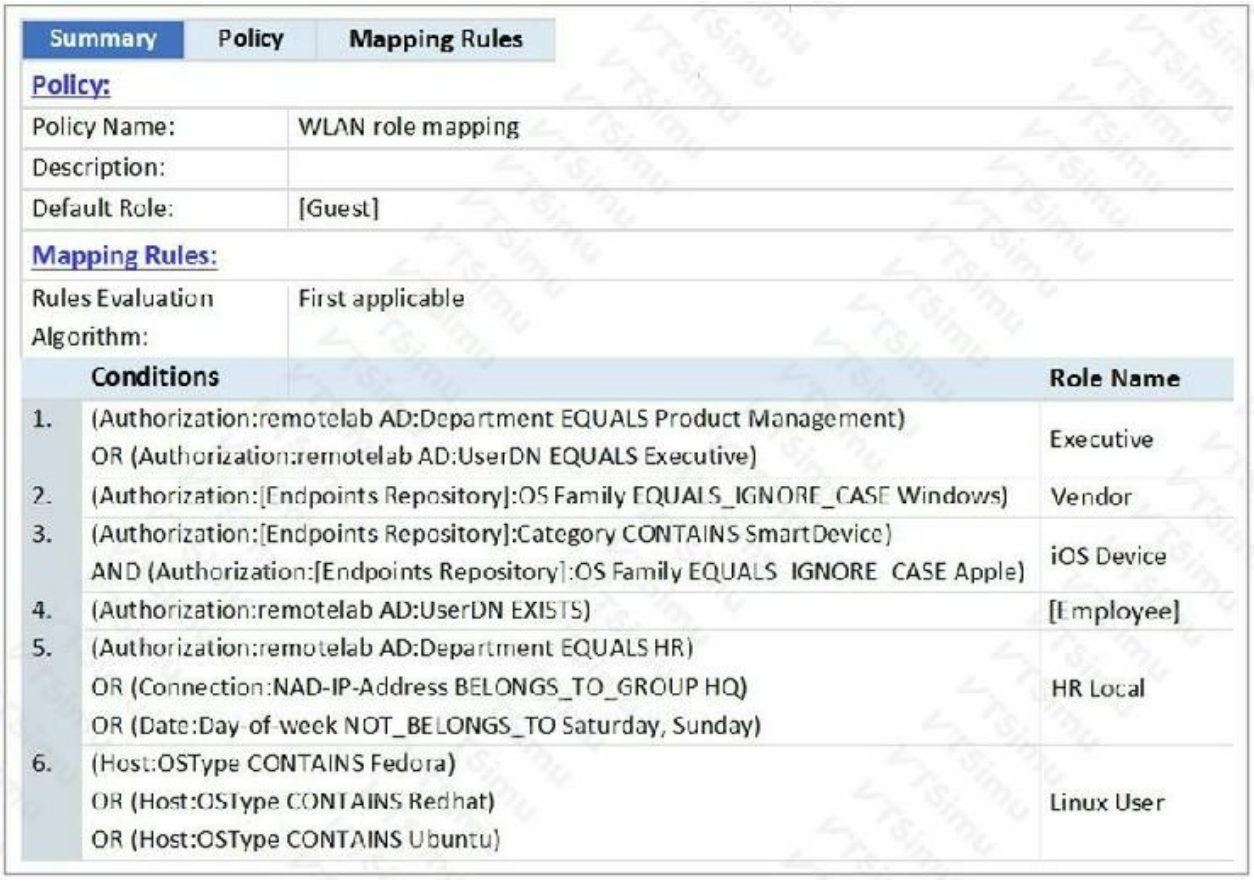
Explanation:

When counting policy manager licenses, include the additional 50 business partner devices. Policy Manager (Access) licensing is sized for endpoints that ClearPass authenticates for network access. The employee laptops using EAP-TLS and the partner devices using web-login authentication are both endpoints requesting access through ClearPass. Therefore, the deployment must be sized for the peak authentication population: the 100 corporate laptops plus the 50 partner devices present during the weekly meeting. License planning should account for this maximum concurrent operational requirement rather than only the normal daily employee population.

Purchase guest licenses. Web Login Guest Authentication uses the ClearPass Guest capability to create, manage, and authenticate guest users. Guest licensing is therefore required for the business-partner access workflow and should provide capacity for the expected partner population during the Friday meetings. EAP-TLS itself does not establish a requirement to purchase Onboard licenses; Onboard licensing applies when ClearPass Onboard is used to provision and manage endpoint certificates. Aruba describes ClearPass licensing and the available Guest capability in its ClearPass Policy Manager licensing documentation and its ClearPass product documentation.

QUESTION NO: 9

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 user is assigned the **Executive** role. ClearPass evaluates the configured role-mapping rules using attributes returned by the authentication source, such as the Active Directory *department* attribute, together with contextual attributes available during the request. In this case, the user's department value is *Product Management*, the NAD is a member of the *HQ*

device group, and the connection occurs on Monday. These values satisfy the conditions configured for the Executive role in the exhibit. Once a role-mapping condition evaluates as true, ClearPass adds its corresponding role to the request context. That role can then be used by the enforcement policy to select the appropriate enforcement profile, such as a VLAN, downloadable user role, or other network-access controls. Role mapping is therefore the policy stage that translates identity and connection context into the authorization role used for access decisions. Aruba's ClearPass Policy Manager documentation describes role mapping as the mechanism for assigning roles based on authentication-source attributes and request attributes; see the ClearPass Policy Manager documentation and Aruba's ClearPass technical documentation portal.

QUESTION NO: 10

A ClearPass Guest operator creates a visitor account with a duration of eight hours.

What occurs when the configured account duration expires?

A. The guest account can no longer be used for authentication.

B. The guest account is automatically converted to a local user account.

C. The account duration is automatically extended by another eight hours.

D. The guest is assigned the employee role.

E. The account is immediately removed from every ClearPass database.

ANSWER: A

Explanation:

The guest account can no longer be used for authentication. is correct. ClearPass Guest accounts can have a defined expiration or duration as part of their account lifecycle settings. Once the account reaches its expiration time, ClearPass treats the account as no longer valid for guest authentication.

The account record can remain available for reporting and administration until it is deleted according to the organization's operational or retention practices. Expiration does not convert the account into a local user account or automatically extend the account duration. ClearPass Guest supports account lifetime controls to limit guest access to the period authorized by the sponsor or registration workflow. See the ClearPass Guest account documentation.

QUESTION NO: 11

Refer to the exhibit.

An AD user's department attribute is configured as "HR". The user connects on Monday using an Android phone to an Aruba Controller that belongs to the Device Group Remote NAD.

Which roles are assigned to the user in ClearPass? (Select two.)

A. Executive

B. iOS Device

C. Vendor

D. Remote Employee

E. HR Local

ANSWER: D E

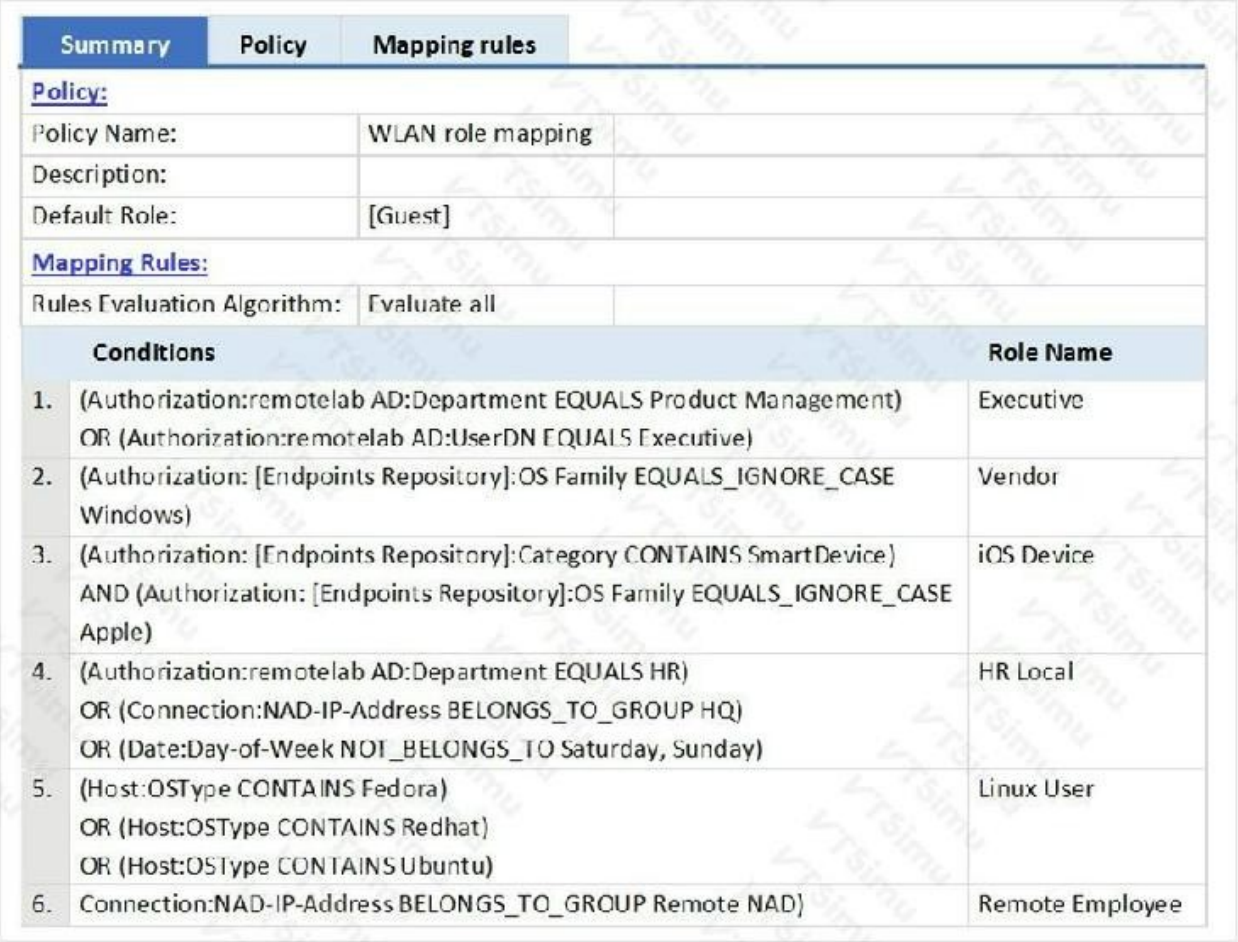
Explanation:

Remote Employee is assigned because the Aruba Controller used for the connection is a member of the *Remote NAD* device group. ClearPass role-mapping rules can evaluate connection attributes supplied by the network access device, including its configured device group, and assign a role when that rule's conditions match. This lets the same authentication service distinguish users connecting through remote infrastructure from users connecting through other NAD groups.

HR Local is also assigned because the authenticated user's Active Directory department attribute has the value *HR*. During authentication, ClearPass obtains authorization attributes from the configured AD source and evaluates them against the role-mapping policy. A matching department-based rule adds the associated ClearPass role. Roles are cumulative: every matching role-mapping rule contributes its role to the request, rather than ClearPass selecting only one matching role. The resulting roles can then be used by enforcement policy conditions to return the appropriate controller role, VLAN, downloadable role, or other authorization result. Aruba's ClearPass documentation describes role mapping as the mechanism that derives roles from authentication, authorization, endpoint, and connection-context attributes; see the ClearPass Role Mapping overview and the ClearPass documentation portal.

QUESTION NO: 12

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? (Select two.)

A. Executive

B. iOS Device

C. Vendor

D. Remote Employee

E. HR Local

ANSWER: D E

Explanation:

The assigned roles are **Remote Employee** and **HR Local**. ClearPass Role Mapping evaluates the attributes returned by authentication and endpoint/device context against the role-mapping rules shown in the exhibit. The controller's membership in the *Remote NAD* device group satisfies the location or NAD-based condition for the **Remote Employee** role. This role can then be used later by an enforcement policy to apply access appropriate for users connecting through remote network infrastructure.

The Active Directory department attribute is returned as `HR`, which satisfies the directory-attribute condition associated with **HR Local**. ClearPass can assign more than one role during the same authentication transaction; the roles are cumulative inputs for subsequent enforcement-policy matching rather than mutually exclusive user classifications. The weekday and Android endpoint details do not prevent the two matching role rules from being assigned under the displayed configuration.

For ClearPass role-mapping behavior and the use of authentication, authorization, and endpoint attributes in policy decisions, see the ClearPass Policy Manager Role Mapping documentation and the ClearPass Enforcement Policies documentation.

QUESTION NO: 13

Which attributes can a RADIUS enforcement profile return to an Aruba controller after successful authentication? (Select two.)

A. Aruba-User-Role

B. Tunnel-Private-Group-ID

C. RADIUS shared secret

D. EAP server certificate private key

E. Active Directory bind password

ANSWER: A B

Explanation:

Aruba-User-Role and **Tunnel-Private-Group-ID** can be returned by a RADIUS enforcement profile. Aruba-User-Role is an Aruba vendor-specific RADIUS attribute that instructs an Aruba controller to assign the authenticated client the specified user role. The role determines firewall policy, access rights, and other controller-based authorization behavior.

Tunnel-Private-Group-ID is part of the standard RADIUS tunnel attribute set and can be used for dynamic VLAN assignment when returned with the other required tunnel attributes. ClearPass enforcement profiles return these authorization values in an Access-Accept message. A shared secret and an EAP server certificate are configured as part of the RADIUS trust and authentication configuration; they are not values returned to the controller as an authorization result. See ClearPass Enforcement Profiles documentation and RFC 2868.

QUESTION NO: 14

Which attributes can be evaluated by a ClearPass Role Mapping policy to assign a role? (Select two.)

A. Attributes returned by an Active Directory authorization source

B. Attributes stored in the Endpoints repository

C. The text displayed in the Access Tracker Summary tab

D. The ClearPass application license serial number

E. The current CPU utilization of the Policy Manager server

ANSWER: A B

Explanation:

Role Mapping policies can evaluate attributes returned by authentication and authorization sources. For example, ClearPass can retrieve an Active Directory group-membership attribute and use it to assign an Employee or Contractor role.

Role Mapping policies can also evaluate endpoint attributes stored in the Endpoints repository. These attributes can include endpoint category, device name, ownership, profiling results, or attributes obtained through integrated systems such as an MDM server. The resulting ClearPass roles are available to the enforcement policy for the final authorization decision. See the ClearPass Role Mapping documentation.

QUESTION NO: 15

Refer to the exhibit.

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

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

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

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

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

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

ANSWER: D

Explanation:

If the user is not found in the local user repository and remotelab AD, a reject message is sent back to the NAD. ClearPass Policy Manager evaluates the authentication sources configured for the service to locate the connecting user or device and authenticate that entity. When multiple authentication sources are configured, the request can be evaluated against each applicable configured source. A user absent from one source is therefore not immediately rejected if another configured authentication source can locate that user. However, if ClearPass cannot find the identity in any configured authentication source—in this case, neither the local user repository nor the remotelab Active Directory source—it cannot perform authentication for the request. Policy Manager then rejects the authentication request and returns an Access-Reject response to the network access device (NAD). This behavior prevents an unknown identity from proceeding to later policy stages, such as authorization and role mapping, because those stages depend on a successfully identified and authenticated entity. Aruba documents this authentication-source lookup and rejection behavior in the ClearPass Policy Manager User Guide. Additional ClearPass documentation is available from the ClearPass Authentication documentation.

QUESTION NO: 16

Refer to the exhibit.

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

Explanation:

It will be visible in the Endpoints table with Known Status. ClearPass Guest MAC caching associates the authenticated guest session with the client device's MAC address and records that device in the Policy Manager Endpoint Repository. Following successful authentication through the guest.php web login page, the MAC Caching service updates or creates the endpoint record so that ClearPass can recognize the device on later connections and apply the intended cached-access behavior without requiring the same full guest-login workflow during the configured cache period. The endpoint is marked *Known* because ClearPass has learned the device identity through a successful authentication event and has an associated, trusted endpoint record for policy evaluation. This endpoint information is distinct from the guest account data used to authenticate the visitor; MAC caching is specifically a device-recognition mechanism implemented through endpoint records. Aruba's ClearPass Policy Manager documentation describes the Endpoint Repository as the store used for endpoint attributes and identity information, while the Guest configuration documentation covers MAC-caching behavior for guest access. See the Aruba ClearPass Policy Manager 6.7 documentation and the Endpoint Repository documentation.

QUESTION NO: 17

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

Explanation:

ClearPass Onboard is used to securely provision personally owned and other unmanaged endpoint devices for network access. Rather than relying on a shared pre-shared key or an insecure enrollment process, Onboard guides users through device enrollment and installs a unique client certificate and the appropriate wireless or wired network profile. The device can then authenticate using certificate-based 802.1X, commonly through EAP-TLS, which provides strong, individual device identity and enables credentials to be revoked when needed. Onboard supports self-service onboarding workflows, reducing the operational burden on IT while allowing an organization to apply its access policies to user-owned devices. It is therefore designed specifically for securely connecting personal devices to the enterprise network. Aruba describes Onboard as a ClearPass service for provisioning devices with certificates and configuring them for secure network access. See the ClearPass Onboard Overview and the ClearPass Onboard documentation.

QUESTION NO: 18

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

A. to force the client to re-authenticate upon roaming to a new Controller

B. to apply firewall policies based on authentication credentials

C. to validate a host MAC address against a whitelist or a blacklist

D. to authenticate users or devices before granting them access to a network

E. to transmit messages to the NAD/NAS to modify a user's session status

ANSWER: E

Explanation:

RADIUS Change of Authorization (CoA) is used to send an authorization change to a network access device (NAD), also called a NAS, for a session that is already active. A RADIUS server can initiate a CoA-Request when a user's role, policy, endpoint posture, bandwidth entitlement, VLAN assignment, access-control list, or other session authorization attributes need to be updated without waiting for the session to end and start again. The NAD identifies the applicable active session using attributes such as the User-Name, NAS IP address, Acct-Session-Id, or Calling-Station-Id, then applies the requested change and returns a CoA acknowledgement or failure response. This enables ClearPass and similar policy servers to dynamically enforce changed access decisions after authentication. RFC 3576 defines these dynamic authorization extensions, including both CoA messages for modifying an existing session's authorization and Disconnect messages for terminating an active session. Therefore, the purpose is accurately described as transmitting messages to the NAD/NAS to modify a user's session status. See RFC 3576: Dynamic Authorization Extensions to RADIUS and Aruba ClearPass Change of Authorization documentation.