PassQueen
a.k.a dumpsqueen.com

HPE Aruba Networking ClearPass Exam

HP HPE6-A88

Version Demo

Total Demo Questions: 11

Total Premium Questions: 111

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

A client connects to a network and initially has the attribute 'IsProfiled=false'. The client is placed in a 'Limited Access to the Profiler' role. What sequence of events will occur next to ensure the client gains full access to the network?

A. ClearPass immediately profiles the client upon connection, and the client is granted full access without any further steps.

B. The client sends a DHCP request, ClearPass profiles the client, sends a terminate session instruction, and the client re-authenticates with full access.

C. The client sends a DHCP request, ClearPass profiles the client and grants full access without terminating the session.

ANSWER: B

Explanation:

The correct sequence is: “The client sends a DHCP request, ClearPass profiles the client, sends a terminate session instruction, and the client re-authenticates with full access.” This is the ClearPass Profile and Bounce workflow. Initially, the endpoint has not yet been identified, so policy uses the `IsProfiled=false` attribute to assign restricted access. That restricted role must still permit the endpoint to perform the traffic needed for profiling, commonly DHCP. ClearPass Profiler examines DHCP information such as the DHCP fingerprint and other observed endpoint attributes, then updates the endpoint record with the identified profile.

The original RADIUS session was authorized using the endpoint’s prior, unprofiled state. Therefore, ClearPass sends a RADIUS Change of Authorization request that terminates the active session at the network access device. The endpoint reconnects or reauthenticates, causing a new RADIUS request. On this new authorization evaluation, ClearPass sees the updated profiled state and can match the full-access enforcement policy. This process ensures the access change is applied immediately rather than waiting for the existing session to expire. Aruba ClearPass documentation describes endpoint profiling and policy use in the ClearPass Policy Manager documentation; the RADIUS CoA mechanism is standardized in RFC 5176.

QUESTION NO: 2

A company uses ClearPass to manage network access and has integrated it with an external server that supports HTTP API access. A new policy requires that any device managed by the EMM server must receive a specific configuration update upon network authentication. How can ClearPass facilitate this requirement?

A. ClearPass can directly update the device configuration without involving the EMM server.

B. ClearPass can only notify the network administrator to manually update the device configuration.

C. ClearPass can send an HTTP message to the EMM server, triggering the server to push the required configuration update to the device.

ANSWER: C

Explanation:

ClearPass can send an HTTP message to the EMM server, triggering the server to push the required configuration update to the device. This is accomplished with a ClearPass Context Server Action, which enables Policy Manager to communicate with an external HTTP/REST API as part of policy processing. The authentication or authorization event supplies the context for the action, such as the authenticated user, device identity, endpoint attributes, or session details. ClearPass can then make an outbound API request to the EMM platform according to the configured URL, method, headers, authentication method, and message body. The EMM platform remains responsible for managing the enrolled device and delivering the required profile, policy, application, or other configuration payload. This approach lets the organization connect successful network-access decisions to an automated endpoint-management workflow, rather than treating network authentication and device configuration as unrelated processes. In practice, the Context Server Action is associated with the relevant enforcement policy so that it runs when the device meets the policy conditions for the update. Aruba documents Context

Server Actions as an integration mechanism for invoking external RESTful services from ClearPass Policy Manager. See the ClearPass Policy Manager Context Server Actions documentation and Aruba's enforcement policy documentation.

QUESTION NO: 3

An IT professional is setting up a Pre-Authentication Check using RADIUS. They need to ensure that the same service will authenticate the user to the Network Access Device (NAD). What is a crucial step they must take to configure this correctly?

A. Set up a separate RADIUS server to handle the Pre-Authentication Check.

B. Configure the RADIUS server to process the Pre-Authentication Check and the NAD authentication request.

C. Use a different authentication protocol for the NAD.

ANSWER: B

Explanation:

Configure the RADIUS server to process the Pre-Authentication Check and the NAD authentication request. In ClearPass, a RADIUS pre-authentication exchange is an initial credential-validation request that occurs before the NAD submits the authentication request used to authorize network access. The ClearPass service logic must therefore be able to match and process both request stages consistently. This includes ensuring that the applicable service selection criteria recognize the relevant requests and that the same authentication, authorization, and enforcement policy flow is available when the NAD sends its RADIUS Access-Request. Doing so maintains a consistent identity and policy decision from the pre-authentication check through the actual access decision, including any role or enforcement attributes returned to the NAD. ClearPass services are the policy-processing components that classify incoming requests and apply configured authentication, role-mapping, and enforcement logic. The NAD must also be configured as a valid ClearPass network device/client so its RADIUS requests can be received and processed by that policy workflow. See the Aruba documentation on ClearPass services and network devices and RADIUS clients.

QUESTION NO: 4

An IT administrator is managing a network with ClearPass and notices that one of the devices is sending multiple health checks throughout the day via different networks (wired, wireless, and VPN). How does OnGuard handle the license usage for this device?

A. OnGuard debits one license per day for the device regardless of the number of health checks or networks used.

B. OnGuard debits a license for each network the device connects to throughout the day.

C. OnGuard debits a separate license for each health check sent by the device.

ANSWER: A

Explanation:

OnGuard debits one license per day for the device regardless of the number of health checks or networks used. ClearPass OnGuard licensing is designed around the endpoint being assessed during a licensing day, rather than around every individual posture transaction, connection type, or access network. Consequently, a managed endpoint can submit its posture state when it connects through wired access, wireless access, or a VPN without repeatedly consuming additional OnGuard licenses merely because it changes connectivity methods or performs multiple health checks.

This approach is important for roaming users, whose devices commonly move between office Ethernet, corporate Wi-Fi, home VPN, and other access methods within the same day. The health-validation workflow continues to provide posture information to ClearPass for policy enforcement, while license accounting remains predictable at the device level for that daily period. Administrators should therefore size the OnGuard license pool based on the number of distinct endpoints expected to use OnGuard, rather than multiplying that count by the number of networks or posture reports each endpoint generates. Aruba describes ClearPass OnGuard as its endpoint posture and health-validation capability; product and documentation resources are available at Aruba ClearPass and ClearPass documentation.

QUESTION NO: 5

A network engineer is installing a new HTTPS certificate on a ClearPass server to replace the built-in self-signed certificate. They want to ensure the certificate is trusted and properly installed. What critical step must they remember to avoid installation issues?

A. Install the certificate without specifying the subject alternative names

B. Include the entire certificate bundle with root CA and intermediate CA trusts

C. Only install the certificate for the publisher

ANSWER: B

Explanation:

Include the entire certificate bundle with root CA and intermediate CA trusts. A publicly or privately issued HTTPS server certificate is trusted only when ClearPass and connecting clients can build a complete, verifiable chain from the server identity certificate through any issuing intermediate certificate authorities to a trusted root certificate authority. During the ClearPass certificate replacement process, the server certificate must be associated with its private key, and the relevant issuing certificates must be available in the ClearPass trust configuration. Supplying the full chain prevents incomplete-chain errors and allows browsers, API clients, and other HTTPS consumers to validate the certificate presented by the ClearPass management interface. This is particularly important when the issuing authority uses one or more intermediate certificates, because clients may not be able to retrieve missing intermediates automatically. The certificate identity should also match the ClearPass hostname used by administrators, but maintaining the complete issuing chain is the essential installation step for establishing trust. Aruba documents certificate administration and trusted-certificate handling in its ClearPass Server Certificates documentation; see also the ClearPass Trust List documentation.

QUESTION NO: 6

In an enterprise environment, a network administrator is tasked with configuring ClearPass to interact with various network access devices (NADs). After navigating to the 'Devices' section under the 'Network' menu, what critical step must the administrator take to add a new NAD to ClearPass properly?

A. Set up a VPN tunnel between the NAD and ClearPass.

B. Configure the device's MAC address in the Add Device window.

C. Enter a source IP address or address range for the device.

ANSWER: C

Explanation:

Enter a source IP address or address range for the device. ClearPass Policy Manager identifies a Network Access Device from the source IP address of the RADIUS request it receives. Therefore, when defining a NAD under *Configuration* > *Network* > *Devices*, the administrator must specify the individual IP address or an IP address range/subnet from which that device, or group of devices, will send RADIUS traffic. This device definition establishes the basis for ClearPass to recognize the RADIUS client and apply the appropriate device configuration, including its shared secret and vendor-specific settings. A single address is appropriate for one switch, controller, firewall, or access point; a CIDR range can be used when multiple NADs are managed as a group. The address entered must match the actual source address used by the NAD's RADIUS packets, which may be a management interface, loopback interface, or another configured source interface. Correct source-IP definition is essential before ClearPass can reliably accept and process authentication and accounting requests from the NAD. Aruba's ClearPass documentation describes adding network devices and defining their IP address or subnet in the Network Devices configuration: ClearPass Policy Manager Network Devices overview and Add a Network Device.

QUESTION NO: 7

A network engineer is tasked with creating enforcement profiles for a multi-vendor environment and wants to minimize the number of enforcement profiles they need to write. Which approach should the engineer take?

A. Enable SNMP services on all network devices.

B. Utilize IETF attributes instead of vendor-specific attributes.

C. Write separate enforcement profiles for each device vendor type.

ANSWER: B

Explanation:

Utilize IETF attributes instead of vendor-specific attributes is correct because IETF RADIUS attributes are standardized and therefore provide the best basis for enforcement that must operate consistently across equipment from multiple vendors. ClearPass Enforcement Profiles can return standard RADIUS attributes such as Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID. When supported and configured by the network access devices, these attributes can be used for common outcomes such as assigning a client to a VLAN without tying the profile to a particular vendor's proprietary RADIUS dictionary or command syntax. This lets an engineer design a smaller, reusable set of profiles around common access-control requirements, rather than duplicating equivalent logic for each switch, controller, or wireless platform. The approach is especially useful where the desired enforcement action has a well-defined RADIUS standard representation. ClearPass documentation describes Enforcement Profiles as the mechanism for returning RADIUS attributes to network devices, while the IETF RADIUS tunnel attributes define standardized values used for tunnel and VLAN-related assignments. Device configuration must still be validated to ensure the relevant standard attributes are accepted for the intended enforcement behavior. See RFC 2865: Remote Authentication Dial In User Service (RADIUS) and RFC 3580: IEEE 802.1X RADIUS Usage Guidelines.

QUESTION NO: 8

A network engineer needs to ensure secure and reliable communication between network devices and the RADIUS server over an unsecured network. Which configuration should they implement?

A. Implement RadSec because it encrypts all RADIUS communication and uses TCP for reliable packet delivery.

B. Use UDP for faster message transport and rely on internal network security.

C. Implement RADIUS with PSK because it is simpler to configure and only encrypts passwords.

ANSWER: A

Explanation:

Implement RadSec because it encrypts all RADIUS communication and uses TCP for reliable packet delivery. RadSec is RADIUS transported over TLS, normally using TCP as its transport protocol. The TLS session provides confidentiality and integrity protection for RADIUS traffic in transit, which is essential when the communication path crosses an untrusted or publicly reachable network. This protection is broader than the limited protection traditionally associated with RADIUS shared-secret handling, because TLS protects the RADIUS exchange while it is carried between the network access device and the RADIUS server.

TCP also provides an established, connection-oriented transport with ordered delivery and retransmission capabilities. This is useful for a deployment where dependable communication is required over links that may be less predictable than a private local network. RadSec is specifically standardized to allow RADIUS clients and servers to exchange RADIUS messages securely using TLS, including the use of mutual certificate-based authentication where configured. In a ClearPass deployment, using RadSec aligns the RADIUS transport with a secure, standards-based method for connecting devices and policy infrastructure across untrusted network segments. The RadSec protocol specification is available in RFC 6614; the related RADIUS-over-TLS operational guidance is available in RFC 7585.

QUESTION NO: 9

An IT administrator notices that a client endpoint has failed a health check and wants to send a notification that will not only inform the user but also force the client to re-authenticate. Which action should the administrator take?

A. Send a message to disable the network interface.

B. Send a notification to disable the network interface.

C. Send a notification with an action to restart the session.

ANSWER: C

Explanation:

Send a notification with an action to restart the session. is the appropriate ClearPass OnGuard post-authentication action when an endpoint's health status changes and the administrator needs both user communication and immediate policy reevaluation. The notification presents the compliance-related information to the user, while restarting the session causes ClearPass to initiate a Change of Authorization workflow toward the applicable network-access device. The endpoint then performs authentication again, allowing ClearPass to evaluate the newly reported unhealthy posture result during the fresh authorization request. The resulting enforcement policy can apply the organization's defined restricted-access, remediation, or quarantine role until the device returns to compliance. This is useful because posture changes can occur after a user has already connected; restarting the session ensures that access is updated promptly rather than waiting for a later reconnect or session timeout. Aruba documents OnGuard posture assessment and post-authentication behavior in the ClearPass Policy Manager documentation. The session restart mechanism relies on RADIUS Change of Authorization, standardized by the IETF in RFC 5176.

QUESTION NO: 10

How does ClearPass Guest utilize the information sent by the client's browser to profile the device and update its database?

A. ClearPass Guest reads the HTTP User Agent information sent with the page request to profile the device automatically.

B. ClearPass Guest requires a separate plugin to read and profile the device.

C. ClearPass Guest relies on the DHCP options to profile the device.

ANSWER: A

Explanation:

ClearPass Guest reads the HTTP User Agent information sent with the page request to profile the device automatically. When a client reaches a guest captive portal, its browser includes an HTTP *User-Agent* header in the request for the portal page. This header commonly identifies characteristics such as the browser family, browser version, operating system, and device type. ClearPass Guest can use that browser-supplied information for device detection, allowing it to recognize and classify the endpoint without requiring the guest to manually provide those technical details. The detected information is retained with the device record in the Guest database and can provide useful context for guest access operations, endpoint visibility, and downstream policy decisions. This is particularly useful in captive-portal workflows because the browser request is available as soon as the endpoint is redirected to the portal, enabling automatic identification during the guest-registration or login experience. Aruba's ClearPass Guest documentation describes device detection as using information supplied by the client browser, including the User-Agent value. See the ClearPass Guest device-detection reference and the ClearPass Guest documentation overview.

QUESTION NO: 11

What is the most critical step the administrator should take to integrate ClearPass with Microsoft Active Directory for user management?

A. Configure ClearPass to interact with Microsoft Active Directory and validate user credentials.

B. Set up ClearPass to log all user activities for auditing purposes.

C. Ensure that ClearPass can enforce network policies based on user roles.

ANSWER: A

Explanation:

Configure ClearPass to interact with Microsoft Active Directory and validate user credentials. This is the essential integration step because ClearPass must have an Active Directory authentication source that enables it to communicate with the domain environment, authenticate users, and retrieve directory attributes. In a typical domain-joined deployment, ClearPass is joined to the AD domain and uses the machine account and Kerberos/LDAP mechanisms to query domain controllers. Alternatively, an AD/LDAP authentication source can be configured with appropriate secure connectivity and credentials. Once this connection is established, ClearPass can validate a user's supplied credentials against Active Directory and use returned attributes—such as username, group membership, department, or organizational unit—in service rules, role mapping, and enforcement decisions. This provides the identity data on which the remainder of ClearPass access-control processing depends. Aruba's ClearPass documentation describes configuring authentication sources and joining ClearPass to an Active Directory domain as part of integrating directory-based identity services. See the ClearPass Active Directory authentication source documentation and the ClearPass Active Directory domain-join guidance.