PassQueen
a.k.a dumpsqueen.com

Aruba Certified ClearPass Associate Exam

HP HPE6-A82

Version Demo

Total Demo Questions: 13

Total Premium Questions: 130

Buy Premium PDF

https://passqueen.com

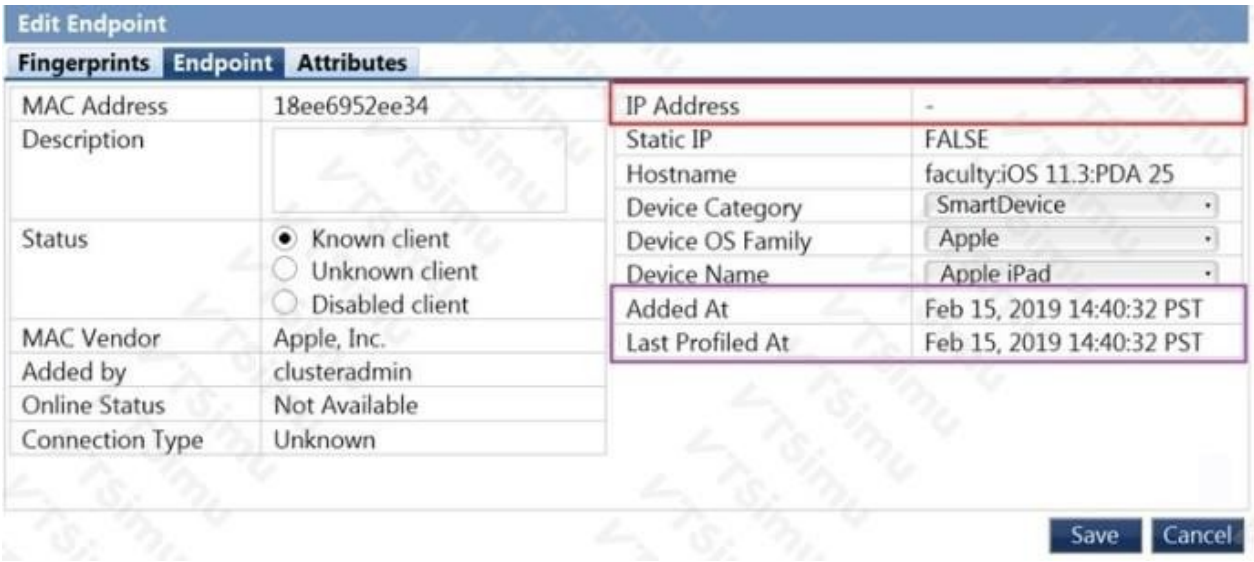
support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Identify the functions and features of Aruba products and solutions	123
Topic 2, Given a scenario, recommend Aruba solutions	7
Total	130

QUESTION NO: 1

Refer to the Endpoint in the screenshot.



What are possible ways that it was profiled? (Choose two.)

A. Exchange Plugging agent

B. NAD ARP listening handler

C. 3rd part MDM

D. DNS fingerprinting

E. Cisco Device Sensor

ANSWER: B C

Explanation:

The endpoint can be profiled through the NAD ARP listening handler and through a 3rd party MDM integration. ClearPass gathers endpoint intelligence from multiple sources and associates the resulting attributes with the endpoint record. The NAD ARP listening handler passively learns ARP information observed by a network access device, allowing ClearPass to correlate IP and MAC address data and use that information as part of endpoint discovery and classification. This is particularly useful for endpoints that are visible on the network even when they are not supplying a rich authentication exchange.

A 3rd party MDM can also supply device inventory, ownership, operating-system, compliance, and management-state information to ClearPass. ClearPass can use these externally supplied attributes in endpoint records and in policy decisions, making MDM-based information a valid profiling source for managed mobile devices. In practice, combining network-observed attributes with MDM context gives ClearPass a more complete device profile and supports more precise access-control enforcement. Aruba documents endpoint profiling and the available data-collection mechanisms in the ClearPass Policy Manager documentation; Aruba's ClearPass product overview also describes its use of endpoint context and third-party integrations for policy enforcement.

QUESTION NO: 2

What needs to be configured for ClearPass use an enforcement rule base on client Data Cap?

A. Enable Logging of Accounting Start-Stop packets.

B. Interim Accounting on the Network Access Device (NAD).

C. Make sure the Endpoint Profiling is configured.

D. Enable Active Sessions in ClearPass Guest

ANSWER: B

Explanation:

Interim Accounting on the Network Access Device (NAD). is required because a data-cap decision depends on ClearPass receiving timely RADIUS accounting updates that report the client's accumulated traffic consumption during an active session. The NAD, such as a controller, switch, or wireless gateway, is the device that measures session traffic and sends RADIUS accounting records to ClearPass. Configuring interim accounting causes it to transmit periodic Accounting-Interim-Update messages rather than reporting usage only when the session ends.

These periodic updates allow ClearPass to maintain a current usage value for the client and evaluate a data-cap-based enforcement condition while the session is still in progress. When the defined cap is reached, ClearPass has the information needed to apply the configured enforcement outcome at the appropriate policy reevaluation or session-control point. The RADIUS Accounting specification defines the Acct-Interim-Interval mechanism used to request and send these periodic usage updates: RFC 2869, RADIUS Extensions. Aruba ClearPass is designed to consume RADIUS accounting information from network access devices as part of its policy and access-control workflow: Aruba ClearPass product documentation and overview.

QUESTION NO: 3

What is a good collector type used for ClearPass to discover devices with static IP addresses?

A. DHCP Collectors

B. ClearPass Air Monitors

C. Active Collectors

D. Network Functions

ANSWER: C

Explanation:

Active Collectors are the appropriate ClearPass collector type for discovering devices that use static IP addresses. Unlike endpoints that obtain addressing information dynamically, static-addressed devices may not generate a lease event that can be consumed by a DHCP-based discovery process. An Active Collector instead performs scheduled discovery against configured network ranges, actively probing addresses to identify reachable endpoints and collect endpoint attributes for use in ClearPass profiling and policy decisions.

This makes Active Collectors especially useful for infrastructure and embedded devices—such as printers, cameras, badge readers, and similar equipment—that are commonly configured with fixed addresses. The collector can be scoped to the relevant subnets and run on an appropriate schedule, allowing ClearPass to build and refresh endpoint visibility even when the devices do not appear in DHCP records. Aruba's ClearPass documentation describes Active Collectors as a mechanism for discovering endpoints through active scanning of specified IP ranges. See the ClearPass Policy Manager Collectors documentation and the Active Collector configuration documentation.

QUESTION NO: 4

An organization wants employees to enroll personally owned devices and then connect to the secure WLAN using certificate-based 802.1X authentication.

Which ClearPass feature is designed to provision the required client certificate?

A. ClearPass Onboard

B. ClearPass Insight

C. ClearPass Guest

D. ClearPass Profiler

ANSWER: A

Explanation:

ClearPass Onboard is designed to provision client certificates for managed or personally owned devices. Onboard can guide users through an enrollment workflow, authenticate the user, create or obtain a certificate, and install the required network profile on supported devices.

After enrollment, the device can use the installed certificate for EAP-TLS authentication to the secure WLAN. This removes the need for users to repeatedly enter directory credentials and provides stronger identity assurance than password-based wireless authentication. ClearPass Onboard also supports certificate lifecycle management, including revocation when access should be removed.

See the HPE Aruba Networking ClearPass Onboard documentation.

QUESTION NO: 5

When using Guest Authentication with MAC Caching service template, which statements are true? (Choose two.)

A. The guest authentication is provided better security than without using MAC caching.

B. The endpoint status of the client will be treated as "known" the first time the client associates to the network.

C. Which wireless SSID and wireless controller must be indicated when configuring the template.

D. The client will be required to re-enter their credentials even if still within the MAC-Auth Expiry term.

ANSWER: A C

Explanation:

The guest authentication is provided better security than without using MAC caching. MAC caching records the endpoint MAC address after the guest completes the initial authentication and uses that recognized endpoint identity during the configured cache period. This allows ClearPass to make a policy decision for a returning guest device based on the previously authenticated device record, rather than relying only on a transient captive-portal browser interaction. The cache lifetime remains an important control because it limits how long the remembered authorization can be used before a new guest authentication is needed.

Which wireless SSID and wireless controller must be indicated when configuring the template. The Guest Authentication with MAC Caching template must be scoped to the wireless context in which it will operate. Identifying the applicable controller and SSID provides the information ClearPass needs to match the authentication request to the intended guest service and apply the appropriate guest workflow and enforcement policy. This configuration also ensures that MAC-cached guest access is associated with the correct wireless network rather than being applied indiscriminately. Aruba describes ClearPass as using contextual identity and policy information for secure access control; see HPE Aruba Networking ClearPass and the HPE Aruba Networking Support Portal for ClearPass documentation.

QUESTION NO: 6 - (SIMULATION)

Match the correct Profiling Collector with the Collector Type. Collector Types may be used more than once **.**

ANSWER: See the explanation for the answer

Explanation:

Match the profiling collectors as follows:

NMAP and SNMP are active methods because ClearPass actively queries/scans endpoints. TCP fingerprinting relies on observed packet traffic, while DHCP, Controller IF-MAP, and Cisco Device Sensor obtain endpoint information through network-function integrations.

QUESTION NO: 7

A customer plans to use ClearPass OnGuard to restrict access for unhealthy employee laptops.

Which actions can ClearPass policy take when an endpoint does not meet posture requirements? (Choose two.)

A. Assign a restricted or quarantine access role.

B. Send a Change of Authorization to apply an updated access policy.

C. Remove malware directly from the endpoint without endpoint security software.

D. Convert the endpoint MAC address into a client certificate.

E. Grant unrestricted access regardless of the posture result.

ANSWER: A B

Explanation:

Assign a restricted or quarantine access role is correct. ClearPass can use the posture result supplied by OnGuard as a policy condition and return an enforcement result that limits the endpoint to remediation resources or other restricted network services.

Send a Change of Authorization to apply an updated access policy is also correct when the Network Access Device supports dynamic authorization. A CoA allows ClearPass to update the authorization treatment for an active session after the endpoint posture state changes, without necessarily waiting for a manual reconnect.

OnGuard evaluates endpoint compliance; it does not itself replace anti-malware software or automatically grant unrestricted access to all clients. See the ClearPass OnGuard documentation and RFC 5176.

QUESTION NO: 8

ClearPass receives fingerprinting profile data for a client device that is based on MAC OUI, NMAP, DHCP, and OnGuard.

Which fingerprint or fingerprints are used?

A. NMAP because it is actively obtained

B. The last fingerprint gathered

C. OnGuard because it is application based

D. All fingerprints are applied

ANSWER: A

Explanation:

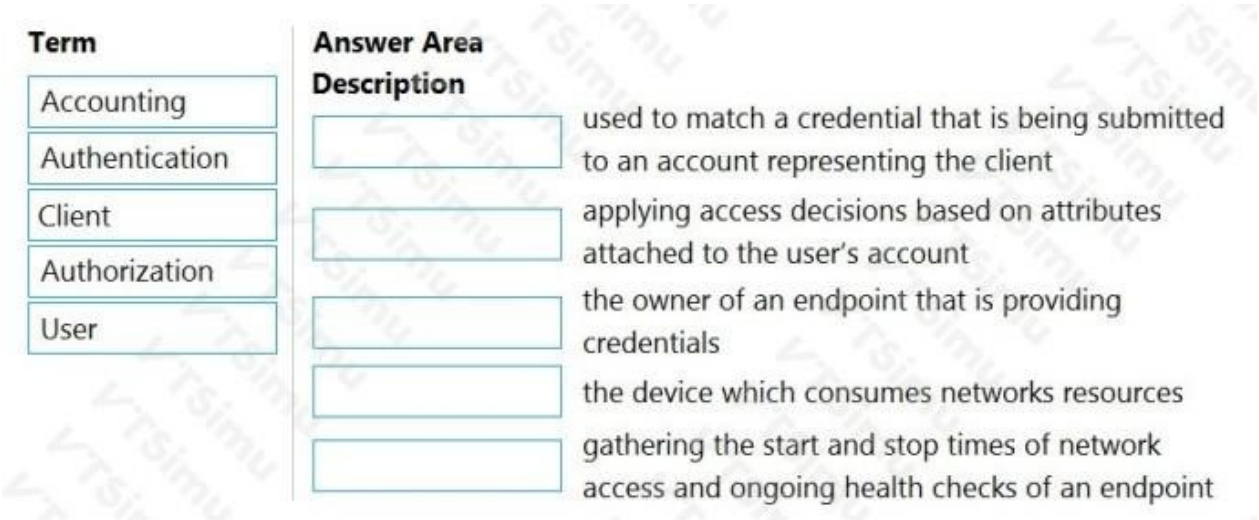
NMAP because it is actively obtained is correct. ClearPass Policy Manager can collect endpoint-profile attributes through several mechanisms, including passive observations such as DHCP and MAC organizationally unique identifier information, plus information supplied by OnGuard. When ClearPass has multiple profiling results for the same endpoint, an active NMAP-derived fingerprint takes precedence. NMAP actively probes the endpoint and evaluates the resulting network-service and operating-system characteristics, so its result is treated as the authoritative fingerprint when it is available. This precedence allows endpoint classification to be based on directly observed behavior rather than solely on attributes that are advertised, inferred, or reported by another software component. The selected fingerprint is then available for role mapping, enforcement-policy decisions, endpoint visibility, and related access-control workflows. ClearPass administrators should ensure that NMAP scanning is appropriately enabled and permitted for the relevant network segments, since successful active collection is what provides this preferred fingerprinting outcome. Aruba's ClearPass documentation describes endpoint profiling and fingerprint collection as part of Policy Manager endpoint classification and policy enforcement. See the Aruba ClearPass Policy Manager documentation and the Aruba Support Portal downloads and documentation.

QUESTION NO: 9 - (DRAG DROP)

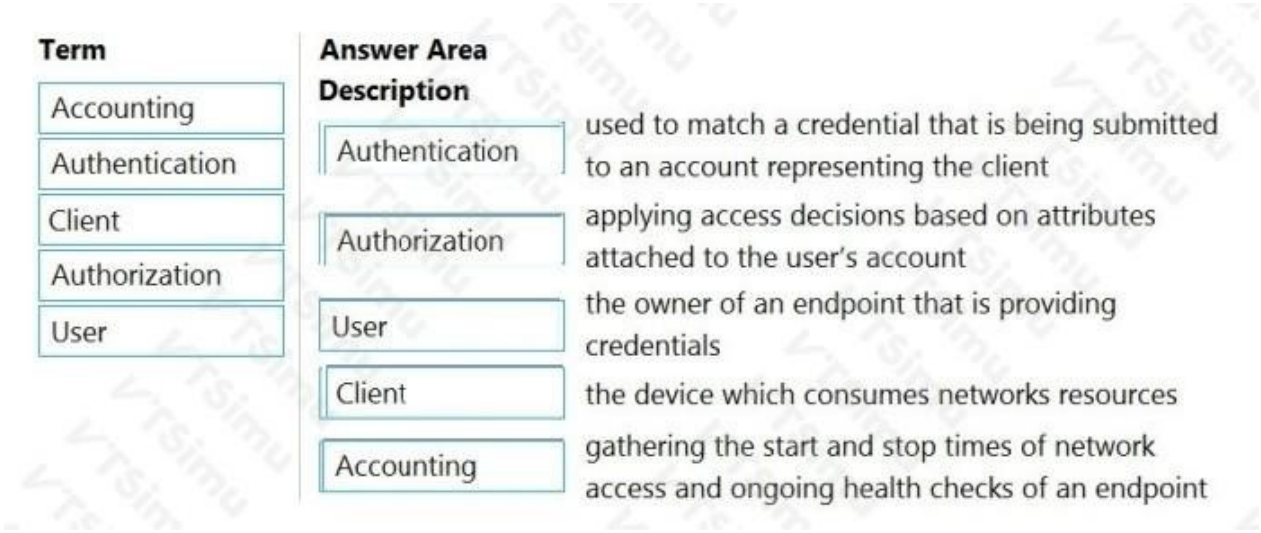
DRAG DROP

Match the security description to the term that best fits. Options are used only once.

Select and Place:



ANSWER:



Explanation:

The correct mapping follows the standard access-control model used for enterprise network access. Authentication is the process that validates a presented identity by matching submitted credentials, such as a username and password or certificate, to the account associated with the connecting endpoint or user. This establishes that the identity claiming access is valid before access is granted.

Authorization follows identity validation and determines what the authenticated identity is permitted to do. In Aruba environments, authorization decisions can use account attributes, roles, device posture, group membership, and policy information to assign the appropriate network permissions. The user is the person who owns or operates the endpoint and supplies the credentials used during the access request. The client is the endpoint itself, such as a laptop, phone, or other device, that connects to and consumes network resources.

Accounting records details of the network-access session. These records commonly include when access begins and ends, session duration, usage information, and status or health-related updates received while the endpoint remains connected. This information supports auditing, reporting, troubleshooting, and operational visibility. Aruba describes these access-control functions and policy-driven access concepts in its ClearPass Policy Manager documentation, while the IETF defines remote authentication, authorization, and accounting protocol behavior in RFC 2865 and accounting behavior in RFC 2866.

QUESTION NO: 10

When should a role mapping policy be used in an 802.1x service with Active Directory as the authentication source?

A. When you want to match Active Directory attributes directly to an enforcement policy.

B. When you want to enable attributes as roles directly without combining multiple attributes

C. When you want to translate and combine Active Directory attributes into ClearPass roles.

D. When you want to match Active Directory attributes to a Aruba firewall role on a Aruba Network Access Device.

ANSWER: C

Explanation:

When you want to translate and combine Active Directory attributes into ClearPass roles is correct because a ClearPass role mapping policy evaluates the attributes returned by the authentication source and assigns one or more internal ClearPass roles based on defined conditions. For an Active Directory authentication source, these conditions can use information such as group membership, usernames, machine names, organizational details, and other returned authorization attributes. This creates a meaningful authorization classification—for example, identifying a user as an employee, contractor, or privileged administrator—before enforcement decisions are made.

Role mapping is especially appropriate when authorization requires logic that translates directory data into roles that are consistent across services and policy decisions, or when multiple directory attributes must be evaluated together. The resulting ClearPass roles are then available to the enforcement policy, which can use them to select the appropriate access

controls, such as a downloadable role, VLAN assignment, or Aruba user role. This separation of attribute evaluation from enforcement makes policies easier to maintain and lets the organization use directory data without requiring enforcement rules to directly interpret every raw Active Directory attribute. Aruba documents role mapping as the mechanism for mapping authorization-source attributes to ClearPass roles in its ClearPass Role Mapping Policies documentation and describes its role in service authorization in the ClearPass Services documentation.

QUESTION NO: 11

Which fingerprint collectors can help to distinguish between an iPhone and an iPad? (Select two.)

A. IF-MAP

B. MAC OUI

C. HTTP

D. TCP header capture

E. SNMP

ANSWER: A C

Explanation:

HTTP and **IF-MAP** are the applicable selections because distinguishing closely related Apple device types requires information beyond a DHCP fingerprint. Apple iPhones and iPads can present DHCP characteristics that are not sufficiently unique to identify the precise device class. HTTP user-agent information adds the browser and operating-system details needed by ClearPass profiling to refine that classification. An HTTP user-agent string can indicate whether the device is presenting itself as an iPhone or an iPad, allowing ClearPass to apply a more specific endpoint profile and the related access policy.

IF-MAP supports this process when an Aruba controller is the source of the relevant metadata. The controller can provide HTTP user-agent details to ClearPass through the Interface for Metadata Access Points integration. ClearPass can use those received attributes as part of its profiling evidence, supplementing information learned from other network observations. Aruba documents HTTP User-Agent fingerprinting as a method for improving endpoint identification, including collection through ClearPass components and Aruba controllers via IF-MAP. See the Aruba ClearPass documentation for HTTP User-Agent Fingerprinting and the ClearPass device profiling overview.

QUESTION NO: 12

What is the benefit to installing a wild card certificate for captive portal authentication?

A. Guests no longer are required to validate certificates during captive portal.

B. Allows different certificates for each controller for increased security

C. Wild card certificates are provide greater security than normal certificates

D. Allows the single wild card certificate to be installed on all controllers in the environment

ANSWER: D

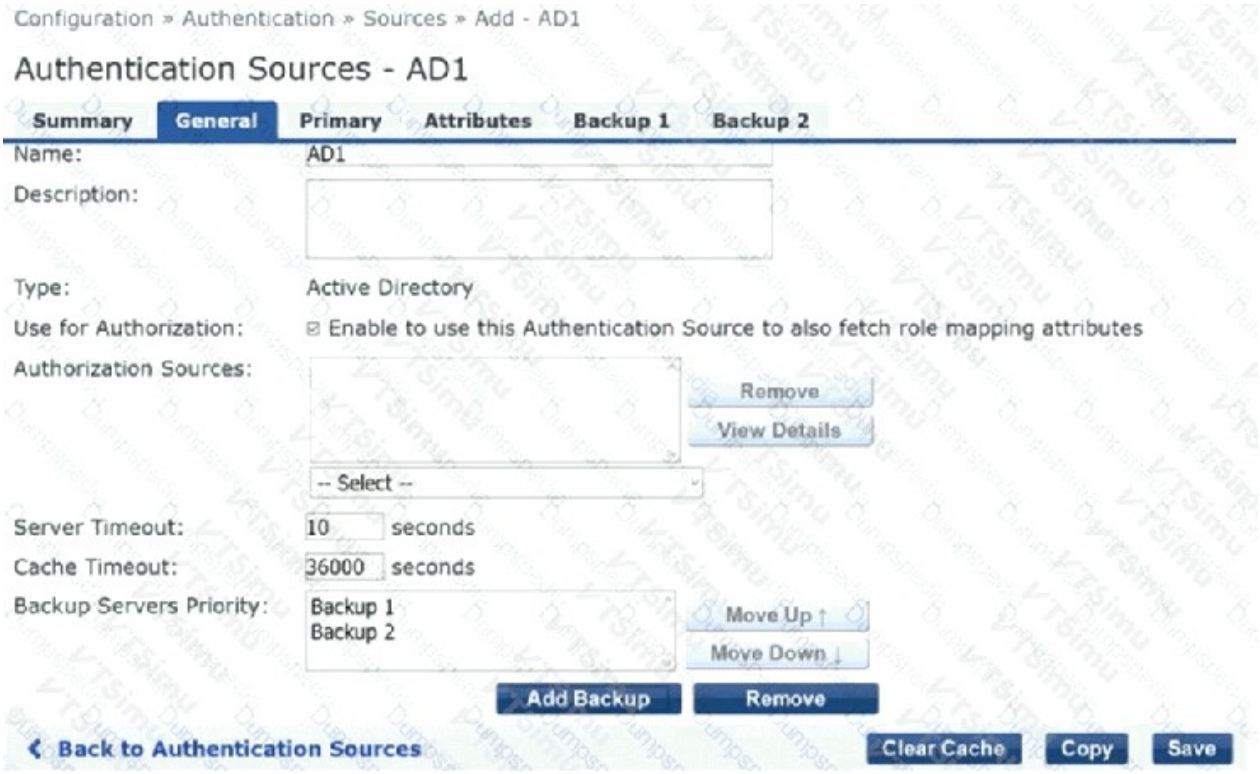
Explanation:

Allows the single wild card certificate to be installed on all controllers in the environment is correct because a wildcard certificate covers multiple hostnames within the same DNS domain. For example, a certificate issued for `*.example.com` can be deployed to controllers using names such as `controller1.example.com` and `controller2.example.com`. In a captive-portal deployment, this enables the organization to use one appropriately issued and trusted server certificate across multiple controllers rather than obtaining, installing, and tracking a separate certificate for every controller hostname. This reduces certificate-management effort and helps provide a consistent HTTPS identity to guest devices when they are

redirected to the portal. The controller hostnames must still fall within the wildcard's covered domain, and the certificate must be issued by a certificate authority trusted by the client devices to avoid browser trust warnings. Aruba's captive portal documentation describes configuring a server certificate for secure captive-portal access, while the TLS specification defines the hostname-matching behavior that permits wildcard DNS identities. See ArubaOS captive portal certificate documentation and RFC 6125: Service Identity and Wildcard Certificate Matching.

QUESTION NO: 13

Refer to the exhibit.



What are two consequences of the Cache Timeout being set to 36000 seconds? (Select two.)

A. ClearPass will cache all user and machine attributes from AD every 10 hours in anticipation of one of those users or machines attempting to authenticate.

B. Less traffic is required between ClearPass and the AD server when re-authenticating within a 10 hourperiod.

C. The Cache Timeout is designed to reduce the amount of traffic between ClearPass and the AD server by caching user credentials for a 10 hour period.

D. A user changing departments may not see their Department attribute change in AD reflected whileauthenticating until the Cache Timeout period has ended.

E. On a failed authentication attempt, ClearPass will consider any subsequent attempts within 10 hours as total failed attempts before blacklisting the client.

ANSWER: B D

Explanation:

36000 seconds equals 10 hours. ClearPass uses the Active Directory authentication-source cache to retain previously retrieved directory information for the configured timeout. Therefore, when the same user or machine authenticates again during that 10-hour interval, ClearPass can use the cached directory lookup result rather than issuing another AD query. This reduces the AD-query traffic generated by repeated authentications and can also reduce the dependency on an immediate directory lookup for those cached entries.

The cached result includes directory attributes that policy evaluation may use, such as a user's department, group membership, or other mapped AD attributes. Consequently, an AD change made after the entry has been cached is not necessarily reflected in authentication-policy processing until the cached entry expires and ClearPass obtains current information from AD. A department change is a representative example: the user can continue to authenticate with the previously cached Department value during the remaining cache lifetime. This behavior is important when selecting a cache duration, because it balances reduced AD traffic against how quickly authorization decisions must reflect directory updates. Aruba's ClearPass documentation describes Active Directory authentication-source configuration and cache behavior in the ClearPass Policy Manager User Guide, and Aruba documentation resources are available through the Aruba TechDocs portal.