PrepAwayPDF

ONLINE TEST ENGINE

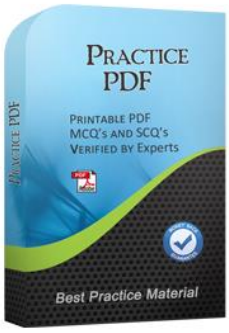
- Online Tool, Convenient, easy to study.
- Practice Online Anytime
- Instant Online Access
- Test History and Performance Review
- Supports All Web Browsers
- Supports Windows / Mac / Android / iOS, etc.

Online Test Engine

DESKTOP TEST ENGINE

- Installable Software Application
- Supports MS Operating System
- Simulates Real Exam Environment
- Two Modes For Practice
- Builds Exam Confidence
- Practice Offline Anytime

Desktop Test Engine



PDF PRACTICE Q&A'S

- Printable PDF Format
- Study Anywhere, Anytime
- Prepared by IT Experts
- 365 Days Free Updates
- Instant Access to Download
- Free PDF Demo Available

PDF Practice Q&A's

60920	59520	59062	59146
Demo Downloads	Successfull Cases	Satisfied Clients	The number of consulting

http://www.prepawaypdf.com/

Best Professional Test Guide Help You Pass and Provide Safe Shopping

Exam : **HPE6-A88**

Title : HPE Aruba Networking ClearPass Exam

Vendor : HP

Version : DEMO

NO.1 A company has recently shifted to a zero-trust model and is facing challenges with its legacy network infrastructure, which was not designed for such a model. The company is particularly concerned about the security of its network as it accommodates a growing number of remote users and IoT devices. What solution could help them create role-based access policies and ensure continuous, closed-loop security across their network?

A. Implementing ClearPass to enable role-based access policies and device profiling.

B. Adding more traditional firewalls to strengthen the network perimeter.

C. Deploying additional VPNs for remote user access.

Answer: A

Explanation:

The Zero Trust framework dictates that "trust" is never granted implicitly but is instead based on identity and context. ClearPass provides this by moving security away from static IP/VLAN-based rules to Dynamic Role- Based Access Control (RBAC) . By integrating profiling (to identify what the device is) with authentication (to identify who the user is), ClearPass assigns a "Role." This role stays with the user/device regardless of where or how they connect, ensuring a consistent security posture across legacy and modern infrastructure.

NO.2 A network administrator notices that a client device leaves the network and returns after ten minutes. Upon reconnecting, the device's posture token is unknown. What is the most likely reason for this behavior?

A. The agent failed to send any updates to ClearPass during the ten-minute period.

B. The posture token expired due to inactivity beyond the five-minute threshold.

C. The endpoint profile information was permanently deleted from ClearPass.

Answer: B

Explanation:

Posture tokens are temporary and have a configurable expiry timer (often defaulted to 5 minutes). If a device disconnects and remains inactive for longer than this threshold, ClearPass clears the token to ensure it doesn't grant access based on potentially stale health data. When the device returns after 10 minutes, it must perform a new health check to regain its "Healthy" status.

NO.3 In a corporate network secured with 802.1X authentication, a client device initially receives a quarantine role due to an unknown posture token. After the client completes a health check using the dissolvable OnGuard agent, the health information is processed by the WEBAUTH service. How does ClearPass utilize this information during the client's second authentication attempt?

A. ClearPass requires the client to complete another health check before allowing network access.

B. ClearPass automatically assigns the client to a guest VLAN without further validation.

C. ClearPass references the cached posture token to determine the appropriate enforcement policy.

Answer: C

NO.4 A web developer is tasked with creating a series of web pages with a unified look and feel using ClearPass Guest. The pages must mirror the company's internal website. Which type of skin should they use?

A. Built-in Custom Skins allow for customization but do not change the overall look and feel.

B. Fully Custom or Personalized Skins are fee-paid services that can be downloaded as plug-ins.

C. Default Skins, as they provide an out-of-the-box look and feel.
Answer: B

NO.5 A network administrator is troubleshooting an issue where endpoints are not receiving updated enforcement decisions after a second authentication. What is the most likely configuration change needed?
A. Increase the frequency of the posture checks.
B. Disable the "Use Cached Results" on enforcement tab.
C. Disable endpoint re-authentication.
Answer: B

NO.6 A company is setting up a RADIUS server for their wireless network authentication. They want to use a certificate with a generic CN for all their ClearPass RADIUS servers. What must they ensure for the certificate to be valid for the clients managed by an Active Directory domain?
A. The domain component of the CN must be a domain that the client can verify.
B. The SAN must include the IP addresses of all RADIUS servers.
C. The CN must match the exact hostname of each RADIUS server.
Answer: A
Explanation:
When Active Directory-joined clients perform 802.1X authentication (such as EAP-PEAP or EAP-TLS), they validate the server's certificate against their trusted root CAs and their domain configuration. For a certificate with a generic Common Name (CN) to be trusted, its domain component must align with a domain the client recognizes and can verify. If the domain in the certificate's CN is completely foreign to the client's trusted environment, the supplicant will likely trigger a certificate warning or fail the connection entirely.

NO.7 While configuring ClearPass for a new network setup, an administrator needs to ensure that a service for a specific wireless SSID at a corporate office is correctly prioritized. They notice that a generic service that processes requests from any wireless SSID is placed above the specific service in the list. What is the likely outcome of this configuration?
A. The specific service for the corporate office SSID will never be used.
B. The generic service will be ignored in favor of the specific service.
C. The specific service for the corporate office SSID will be processed first.
Answer: A
Explanation:
ClearPass evaluates services using a top-down matching logic. When an authentication request arrives, ClearPass compares it against the "Service Rules" of the first service in the list. If the request matches those rules, ClearPass processes the request using that service and stops looking further down the list. If a "Generic Wireless" service with broad rules (e.g., Type = Wireless) is placed at the top, it will intercept all wireless requests-even those intended for a specific SSID service placed lower in the list. Best practice is to place the most specific services at the top and the most generic at the bottom.

NO.8 A web developer is tasked with creating a series of web pages with a unified look and feel using ClearPass Guest. The pages must mirror the company's internal website. Which type of skin

should they use?

A. Default Skins, as they provide an out-of-the-box look and feel.

B. Fully Custom or Personalized Skins are fee-paid services that can be downloaded as plug-ins.

C. Built-in Custom Skins allow for customization but do not change the overall look and feel.

Answer: B

Explanation:

While ClearPass provides built-in skins that allow for basic logo and color changes, achieving a pixel-perfect mirror of an existing corporate website usually requires a Fully Custom Skin . These skins allow developers to upload custom CSS, HTML headers/footers, and JavaScript to match the exact "look and feel" of the brand's main site. These are often provided as specialized plugins or professional service packages to ensure compatibility across different browser types.

NO.9 An IT administrator is tasked with creating a self-service portal for guest users to request and maintain their own user identities. Which type of web page should they create using ClearPass Guest's Web Content Manager?

A. Web Logins

B. Self-Registrations

C. Web Pages

Answer: B

Explanation:

ClearPass Guest distinguishes between simple login pages and complex registration workflows. A Self- Registration page is the correct choice for this requirement because it includes the logic for the guest to enter their information, select a sponsor, receive credentials, and manage their own account details (like password changes or extending their stay).

NO.10 A network administrator wants to ensure that users see their company's logo when accessing the guest network. They have already uploaded the logo as a JPEG file into the Content Manager. What is the next step they should take to display this logo on the custom web pages?

A. Enable public access for the uploaded logo file.

B. Apply a skin that includes the uploaded logo to the web pages.

C. Edit the ClearPass Guest configuration to include the logo in the default template.

Answer: B

Explanation:

Visual branding in ClearPass Guest is handled through Skins . While the Content Manager stores the physical file (the logo), the Skin defines where and how that logo appears on the page. After uploading the logo, the administrator must configure or edit a skin to reference that specific JPEG, and then apply that skin to the desired guest registration or login pages.

NO.11 In a scenario where ClearPass is configured to poll an EMM server, what advantage does ClearPass gain by ingesting device context from the EMM server?

A. ClearPass can encrypt all data transmissions from managed devices.

B. ClearPass can disable unauthorized devices before they connect to the network.

C. ClearPass identifies managed devices attempting to authenticate and access the network in advance.

Answer: C

Explanation:

By polling an EMM/MDM server, ClearPass pre-synchronizes its endpoint database with managed device information. This "Advanced Context" means that when a device eventually connects for the first time, ClearPass already knows its serial number, compliance status, and owner. This eliminates the need for manual profiling or initial "limited access" phases, allowing the system to grant appropriate access levels immediately upon the first authentication attempt.