DUMPSARENA

Aruba Certified Network Security Associate Exam

HP HPE6-A78

Version Demo

Total Demo Questions: 20

Total Premium Questions: 201

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Network Security Fundamentals	30
Topic 2, Security Technologies	109
Topic 3, Security Architecture	5
Topic 4, Security Management	57
Total	201

QUESTION NO: 1

What is one of the policies that a company should define for digital forensics?

A. which data should be routinely logged, where logs should be forwarded, and which logs should be archived

B. what are the first steps that a company can take to implement micro-segmentation in their environment

C. to which resources should various users be allowed access, based on their identity and the identity of their clients

D. which type of EAP method is most secure for authenticating wired and wireless users with 802.1

ANSWER: A

Explanation:

The policy defining which data should be routinely logged, where logs should be forwarded, and which logs should be archived is a core digital-forensics policy. Digital investigations depend on reliable, relevant, and available evidence. A logging policy establishes the events and systems that must generate records, while centralized log forwarding helps protect evidence from loss on an individual endpoint or network device and makes correlation during an investigation practical. Archive and retention requirements also ensure that evidence remains available for an appropriate period, including when an incident is detected long after the relevant event occurred. The policy should be supported by secure time synchronization, controls that protect log integrity, and documented retention procedures so investigators can establish an accurate event timeline and handle collected data consistently. These practices align with the NIST guidance that organizations maintain and preserve log data to support incident response and forensic analysis. See NIST SP 800-92, Guide to Computer Security Log Management and NIST Cybersecurity Framework resources.

QUESTION NO: 2

A company wants to improve the security of EAP-TLS authentication for its Aruba wired and wireless networks. Which two practices are recommended? (Select two)

A. Configure clients to validate the authentication server certificate.

B. Revoke certificates assigned to departed users or lost devices.

C. Install the same client certificate and private key on every endpoint.

D. Disable server certificate validation to avoid connection failures.

E. Use a self-signed client certificate without configuring any certificate trust.

ANSWER: A B

Explanation:

Clients should validate the authentication server certificate, including trusting the issuing CA and verifying the expected server identity. This reduces the risk that a client accepts an attacker-controlled authentication server. The organization should also revoke certificates that are no longer authorized, such as certificates assigned to departed employees or lost devices, so they cannot continue to authenticate successfully.

Using the same client certificate on all endpoints weakens accountability and increases the impact of compromise. Disabling certificate validation makes clients vulnerable to rogue authentication servers. EAP-TLS mutual certificate authentication is described in RFC 5216; Aruba ClearPass certificate and authentication guidance is available through the ClearPass TechDocs portal.

QUESTION NO: 3

A company has an Aruba solution with a Mobility Master (MM) Mobility Controllers (MCs) and campus Aps. What is one benefit of adding Aruba Airwave from the perspective of forensics?

A. Airwave can provide more advanced authentication and access control services for the AmbaOS solution

B. Airwave retains information about the network for much longer periods than ArubaOS solution

C. Airwave is required to activate Wireless Intrusion Prevention (WIP) services on the ArubaOS solution

D. AirWave enables low level debugging on the devices across the ArubaOS solution

ANSWER: B

Explanation:

Airwave retains information about the network for much longer periods than ArubaOS solution. This is valuable for forensics because investigations frequently begin well after an event has occurred. AirWave acts as a centralized management, monitoring, reporting, and historical-data platform for the Aruba wireless environment. It collects device and client information, alerts, event records, performance statistics, configuration-related data, and other operational details over time. An administrator can therefore use its historical reports and monitoring data to establish a timeline, identify affected devices or clients, correlate unusual activity with network conditions, and review evidence that may no longer be present in the controllers' more limited operational logs. Long-term visibility is especially important when investigating intermittent incidents, policy violations, unauthorized access, or events discovered only during a later audit. Aruba describes AirWave as a management platform that provides monitoring, reporting, and troubleshooting capabilities across the network, making it well suited to preserving and reviewing historical operational context. See the Aruba AirWave Management Platform overview and the AirWave documentation portal.

QUESTION NO: 4

You have detected a Rogue AP using the Security Dashboard Which two actions should you take in responding to this event? (Select two)

A. There is no need to locale the AP If you manually contain It.

B. This is a serious security event, so you should always contain the AP immediately regardless of your company's specific policies.

C. You should receive permission before containing an AP. as this action could have legal Implications.

D. For forensic purposes, you should copy out logs with relevant information, such as the time mat the AP was detected and the AP's MAC address.

E. There is no need to locate the AP If the Aruba solution is properly configured to automatically contain it.

ANSWER: C D

Explanation:

"You should receive permission before containing an AP. as this action could have legal Implications." is correct because wireless containment actively disrupts communications between an access point and its clients. Although containment can be an important response for a confirmed threat, it must be performed according to the organization's incident-response process and with appropriate authorization. The AP may belong to a neighboring organization or another legitimate party, and transmitting deauthentication frames or otherwise interfering with its wireless service can create legal, regulatory, and operational consequences. Aruba's wireless intrusion protection capabilities should therefore be applied under defined security policies and authorized procedures.

"For forensic purposes, you should copy out logs with relevant information, such as the time mat the AP was detected and the AP's MAC address." is also correct. Preserving the Security Dashboard event details establishes an evidence trail before the rogue device changes location, stops transmitting, or ages out of monitoring records. Detection time, radio/BSSID MAC address, SSID, channel, signal information, and observing AP details support investigation, correlation with other security events, physical location efforts, escalation, and any required incident documentation. Aruba documents rogue-AP detection and classification as part of its wireless IDS capabilities; evidence collection is a sound operational response before and during authorized remediation. See ArubaOS Wireless IDS overview and CISA incident-response guidance.

QUESTION NO: 5

Which two statements are correct about a WPA3-Enterprise WLAN? (Select two)

A. It uses 802.1X authentication with an authentication server.

B. It requires Protected Management Frames.

C. It uses Simultaneous Authentication of Equals as its authentication method.

D. It requires all users to share one pre-shared key.

E. It prevents the need to validate the RADIUS server certificate.

ANSWER: A B

Explanation:

WPA3-Enterprise uses 802.1X authentication with a backend authentication server, such as ClearPass Policy Manager. It also requires Protected Management Frames (PMF), which protects robust management frames such as deauthentication and disassociation frames against spoofing after security has been established.

WPA3-Personal, not WPA3-Enterprise, uses Simultaneous Authentication of Equals (SAE) for password-based authentication. WPA3-Enterprise does not require every deployment to use a common pre-shared key. See the Wi-Fi Alliance security overview and Aruba's WPA3 security overview.

QUESTION NO: 6

A company has AOS-CX switches deployed in a two-tier topology that uses OSPF routing at the core.

You need to prevent ARP poisoning attacks. To meet this need, what is one technology that you could apply to user VLANs on access layer switches? (Select two.)

A. ARP inspection

B. OSPF passive interface

C. BPDU guard (protection)

D. DHCPv4 snooping

E. BPDU filtering

ANSWER: A D

Explanation:

ARP inspection and **DHCPv4 snooping** should be applied together on access-switch user VLANs to mitigate ARP poisoning. DHCPv4 snooping monitors DHCP exchanges and creates a trusted binding database associating client IP addresses, MAC addresses, VLANs, and switch ports. This database establishes the valid client identity information needed for subsequent Layer 2 validation. Aruba AOS-CX ARP inspection uses those trusted DHCP snooping bindings when it examines ARP traffic on protected VLANs. When an ARP packet claims an IP-to-MAC mapping that does not match a valid binding, ARP inspection can discard it rather than allowing a forged mapping to reach other hosts. This prevents an attacker connected to a user port from advertising itself as the default gateway or another endpoint through fraudulent ARP replies. Applying the controls at the access layer is appropriate because it validates client-originated ARP traffic close to where untrusted devices attach. In practice, DHCPv4 snooping is enabled for the relevant user VLANs before enabling ARP inspection, so the switch can learn and maintain the bindings on which ARP validation relies. Aruba's AOS-CX security documentation describes both the DHCP snooping binding table and its use by ARP inspection: AOS-CX Dynamic ARP Inspection documentation.

QUESTION NO: 7

A security administrator suspects that an attacker is sending forged deauthentication frames to disrupt a company WLAN. Which two actions help reduce the impact of this attack? (Select two)

A. Enable Protected Management Frames for the WLAN.

B. Use WPA3 security for clients that support it.

C. Increase the DHCP lease time for wireless clients.

D. Increase AP transmit power on all radios.

E. Configure a longer RADIUS shared secret.

ANSWER: A B

Explanation:

Protected Management Frames (PMF) protects robust management frames from forgery and tampering after the client and AP establish security. This helps prevent a nearby attacker from causing a client to disconnect merely by transmitting a spoofed deauthentication frame. WPA3 requires PMF, so migrating compatible clients and WLANs to WPA3 also ensures that PMF is used.

Changing the DHCP scope or increasing the transmit power does not validate management frames and does not address forged deauthentication traffic. Aruba documents PMF in the ArubaOS Management Frame Protection documentation.

QUESTION NO: 8

A company uses ClearPass Policy Manager (CPPM) and ArubaOS-CX switches for wired 802.1X access control. Which two benefits can result from returning authorization attributes in a RADIUS Access-Accept? (Select two)

A. Apply a port-access role to the authenticated client.

B. Assign the client to an authorized VLAN.

C. Encrypt all client traffic between the switch and the default gateway.

D. Set the physical speed and duplex of the client interface.

E. Establish the EAPOL exchange before the client authenticates.

ANSWER: A B

Explanation:

A RADIUS Access-Accept can include authorization attributes that instruct the authenticator how to provide network access after successful authentication. For an ArubaOS-CX switch, these attributes can be used to apply an appropriate access role and to assign the endpoint to a VLAN. This enables ClearPass to make centralized, identity-aware authorization decisions while the switch enforces those decisions at the access port.

The RADIUS Access-Accept does not itself encrypt client traffic or establish the physical Ethernet link. It provides the authorization result and associated attributes after authentication. RADIUS support for authorization attributes is defined in RFC 2865, and ArubaOS-CX port-access concepts are documented in the ArubaOS-CX Port Access overview.

QUESTION NO: 9

A security administrator is collecting evidence after discovering suspicious activity from a wireless client. Which two practices help preserve the value of the evidence? (Select two)

A. Export relevant logs and packet captures before their retention period expires.

B. Document the collector, collection time, and handling of the evidence.

C. Clear the client session and delete its authentication records immediately.

D. Change the timestamps in exported logs to match the investigator's local time.

E. Disable NTP on infrastructure devices during the investigation.

ANSWER: A B

Explanation:

Exporting the relevant logs and captures preserves the original event information before short-term buffers roll over or operational data changes. Recording who collected the evidence, when it was collected, and how it was handled establishes chain-of-custody information that supports later investigation and demonstrates that the evidence was controlled.

Investigators should avoid changing or deleting the original information while gathering evidence. Reliable timestamps and documented handling are important for correlating authentication records, controller logs, packet captures, and other sources. See NIST SP 800-86 and NIST SP 800-92.

QUESTION NO: 10

You are hardening management access to Aruba network infrastructure. Which two practices reduce the risk of unauthorized management access? (Select two)

A. Restrict management services to a dedicated management network.

B. Use TACACS+ with individual administrator accounts.

C. Enable Telnet as a fallback for administrators who cannot use SSH.

D. Use one shared administrator account for all network engineers.

E. Allow HTTPS management access from any client subnet.

ANSWER: A B

Explanation:

Restricting management services to a dedicated management network reduces the systems and users that can reach administrative interfaces. Using TACACS+ with individual administrator accounts supports centralized authentication, authorization, and accounting for device administration, allowing organizations to apply role- or command-based controls and retain accountability for administrative activity.

Telnet should not be used for administrative access because it transmits session data in clear text. Shared administrative accounts also reduce accountability because activity cannot be reliably associated with an individual administrator. Aruba documentation provides secure management guidance through the Aruba Networking TechDocs portal; TACACS+ protocol behavior is described in the IETF TACACS+ specification.

QUESTION NO: 11

Which scenario requires the Aruba Mobility Controller to use a Server Certificate?

A. Obtain downloadable user roles (DURs) from ClearPass.

B. Synchronize its clock with an NTP server that requires authentication.

C. Use RadSec for enforcing 802.1X authentication to ClearPass.

D. Use RADIUS for enforcing 802.1X authentication to ClearPass.

ANSWER: C

Explanation:

Use RadSec for enforcing 802.1X authentication to ClearPass. RadSec (RADIUS over TLS) protects RADIUS authentication, authorization, and accounting exchanges by placing them inside a TLS connection rather than sending conventional RADIUS traffic over its usual UDP transport. TLS requires certificate-based authentication of the secure endpoint, including presentation and validation of a server certificate as the protected connection is established. In an Aruba deployment using a Mobility Controller and ClearPass, the controller's RadSec configuration must therefore be able to validate the certificate identity presented for the RadSec service and establish the TLS trust relationship before it sends 802.1X RADIUS requests. Certificate trust, appropriate certificate names, and the certificate authority chain are consequently essential parts of deploying RadSec securely. This certificate requirement is intrinsic to the TLS transport that RadSec uses, not merely an optional RADIUS tuning setting. The RadSec protocol requirements are defined in RFC 6614: Transport Layer Security for RADIUS. Aruba's documentation portal also provides ArubaOS and ClearPass deployment documentation, including RADIUS and certificate configuration guidance, at Aruba Technical Documentation.

QUESTION NO: 12

You have been asked to send RADIUS debug messages from an ArubaOS-CX switch to a central SIEM server at 10.5.15.6. The server is already defined on the switch with this command: logging 10.5.6.12

You enter this command: debug radius all

What is the correct debug destination?

A. console

B. file

C. syslog

D. buffer

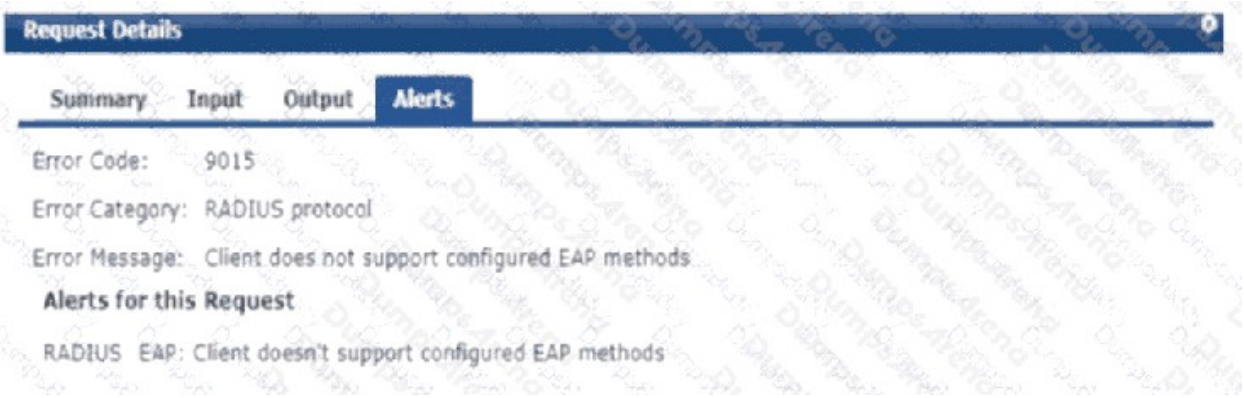
ANSWER: C

Explanation:

syslog is the correct debug destination because it sends the output generated by `debug radius all` through the switch's syslog logging mechanism. This is the appropriate mechanism for exporting RADIUS diagnostic activity to a centralized SIEM or log collector rather than viewing it only in an interactive management session. On ArubaOS-CX, the debug destination controls where enabled debug output is emitted, and selecting syslog integrates that output with the configured remote logging infrastructure. The remote syslog host must also be configured with the intended SIEM address and with a logging severity/filter configuration that permits debug-level messages to be forwarded. The question contains an address discrepancy: the stated intended SIEM is `10.5.15.6`, while the displayed logging command configures `10.5.6.12`. Therefore, the remote logging configuration should be corrected or supplemented to use `10.5.15.6` if that is the actual SIEM destination. The destination type remains syslog; the IP address is configured separately in the logging configuration. Aruba's AOS-CX documentation describes debug controls and output destinations in its Debugging guide and documents remote event logging under Logging.

QUESTION NO: 13

Refer to the exhibit.



A company has an HPE Aruba Networking Instant AP cluster. A Windows 10 client is attempting to connect to a WLAN that enforces WPA3-Enterprise with authentication to HPE Aruba Networking ClearPass Policy Manager (CPPM). CPPM is configured to require EAP-TLS. The client authentication fails. In the record for this client's authentication attempt on CPPM, you see this alert.

What is one thing that you check to resolve this issue?

A. Whether EAP-TLS is enabled in the AAA Profile settings for the WLAN on the IAP cluster

B. Whether the client has a valid certificate installed on it to let it support EAP-TLS

C. Whether EAP-TLS is enabled in the SSID Profile settings for the WLAN on the IAP cluster

D. Whether the client has a third-party 802.1X supplicant, as Windows 10 does not support EAP-TLS

ANSWER: B

Explanation:

Whether the client has a valid certificate installed on it to let it support EAP-TLS is the appropriate item to check. EAP-TLS is a mutual certificate-based authentication method: ClearPass presents its server certificate and the Windows client must select and present a usable client-authentication certificate. In this situation, the ClearPass alert indicates that the authentication attempt did not offer a method compatible with the EAP-TLS method required by the service. A missing, expired, unusable, or improperly enrolled client certificate can prevent the Windows native supplicant from selecting EAP-TLS and supplying credentials for it.

Confirm that the client certificate exists in the user or computer personal certificate store selected by the WLAN profile, is within its validity period, includes the Client Authentication enhanced key usage, and has an accessible private key. Also confirm that the certificate chain is trusted by ClearPass and that the Windows client trusts the certification authority that issued the ClearPass server certificate. Windows supports EAP-TLS natively when an appropriate certificate is available. Microsoft's configuration guidance describes EAP-TLS as certificate-based authentication and details the client certificate requirements: Microsoft wireless 802.1X deployment guidance. Aruba's ClearPass documentation also covers EAP-TLS configuration and certificate validation: ClearPass EAP-TLS documentation.

QUESTION NO: 14

Why might devices use a Diffie-Hellman exchange?

A. to agree on a shared secret in a secure manner over an insecure network

B. to obtain a digital certificate signed by a trusted Certification Authority

C. to prove knowledge of a passphrase without transmitting the passphrase

D. to signal that they want to use asymmetric encryption for future communications

ANSWER: A

Explanation:

Devices use a Diffie-Hellman exchange “to agree on a shared secret in a secure manner over an insecure network.” Diffie-Hellman is a key-establishment mechanism: each device creates a private value, exchanges a corresponding public value with its peer, and then independently calculates the same shared secret. An observer can see the public exchange but, assuming the underlying mathematical problem is computationally difficult, cannot feasibly derive the resulting secret. The devices can feed that shared secret into a key-derivation function and use the derived symmetric keys to protect later traffic with encryption and integrity algorithms.

This function is particularly useful when the peers do not already possess a common symmetric key. Modern protocols commonly use ephemeral Diffie-Hellman values, which can provide forward secrecy: compromise of a long-term authentication credential later does not by itself reveal session keys from previously recorded sessions. Diffie-Hellman establishes keying material, while authentication mechanisms in the surrounding protocol bind the exchange to the intended peer and protect against active interception. RFC 2631 describes Diffie-Hellman key agreement and its purpose of allowing two parties to establish a shared secret over an insecure channel: RFC 2631. NIST also specifies approved key-establishment schemes based on discrete-logarithm cryptography in NIST SP 800-56A Rev. 3.

QUESTION NO: 15

A company with 465 employees wants to deploy an open WLAN for guests. The company wants the experience to be as follows:

Guests select the WLAN and connect without having to enter a password.

Guests are redirected to a welcome web page and log in.The company also wants to provide encryption for the network for devices that are capable. Which security options should you implement for the WLAN?

A. Opportunistic Wireless Encryption (OWE) and WPA3-Personal

B. Captive portal and WPA3-Personal

C. WPA3-Personal and MAC-Auth

D. Captive portal and Opportunistic Wireless Encryption (OWE) in transition mode

ANSWER: D

Explanation:

Captive portal and Opportunistic Wireless Encryption (OWE) in transition mode meets each part of the requested guest experience. A captive portal allows a client to associate to the guest WLAN first and then intercepts web access to present a splash, welcome, or login page. This provides the required web-based guest sign-in without requiring a wireless password during initial connection. OWE is the Wi-Fi security mechanism intended for open networks: it establishes individualized encryption for clients without using a shared passphrase. Therefore, capable client devices gain over-the-air privacy while retaining the simple, password-free onboarding expected for public or guest access. Transition mode is appropriate where guest client capabilities vary, because it preserves access for legacy clients that do not support OWE while allowing compatible clients to use enhanced open encryption. Aruba documents OWE as an Enhanced Open security method for WLANs and identifies transition mode as the interoperability approach for supporting both OWE and open clients. Aruba also documents captive portal as the mechanism used to require guest acceptance or authentication after association. See Aruba's OWE configuration documentation and captive portal documentation.

QUESTION NO: 16

What distinguishes a Distributed Denial of Service (DDoS) attack from a traditional Denial of Service (DoS) attack?

A. A DDoS attack originates from external devices, while a DoS attack originates from internal devices.

B. A DoS attack targets one server; a DDoS attack targets all the clients that use a server.

C. A DDoS attack targets multiple devices, while a DoS is designed to incapacitate only one device.

D. A DDoS attack is launched from multiple devices, while a DoS attack is launched from a single device.

ANSWER: D

Explanation:

A DDoS attack is launched from multiple devices, while a DoS attack is launched from a single device. The defining characteristic is the distribution of the attacking traffic sources, rather than whether the sources are internal or external, or how many targets are affected. In a conventional DoS event, one host or one network source attempts to exhaust a target's bandwidth, processing capacity, connection table, or another finite resource. A DDoS event coordinates traffic from numerous independent systems, commonly devices that have been compromised and enrolled in a botnet. The target receives harmful traffic from many source addresses and networks at the same time. This distributed nature can substantially increase traffic volume and complicate mitigation, because blocking one source does not stop the overall attack and indiscriminate filtering can affect legitimate users. Aruba network-security operations therefore need visibility into traffic patterns and source distribution when detecting and responding to availability attacks. This definition is consistent with the U.S. Cybersecurity and Infrastructure Security Agency's explanation that DDoS attacks use multiple compromised systems to attack a target, and with NIST's description of distributed denial-of-service attacks as originating from multiple hosts. See CISA: Understanding Denial-of-Service Attacks and NIST: Distributed Denial of Service.

QUESTION NO: 17

You have been instructed to look in an AOS Security Dashboard's client list. Your goal is to find clients that belong to the company and have connected to devices that might belong to hackers.

Which client fits this description?

A. MAC address: d8:50:e6:f3:6d:a4; Client Classification: Authorized; AP Classification: Suspected Rogue

B. MAC address: d8:50:e6:f3:6e:c5; Client Classification: Interfering; AP Classification: Neighbor

C. MAC address: d8:50:e6:f3:6e:60; Client Classification: Interfering; AP Classification: Interfering

D. MAC address: d8:50:e6:f3:70:ab; Client Classification: Interfering; AP Classification: Suspected Rogue

ANSWER: A

Explanation:

MAC address: d8:50:e6:f3:6d:a4; Client Classification: Authorized; AP Classification: Suspected Rogue is the client that meets both conditions in the task. Its *Authorized* client classification identifies it as a client recognized as belonging to, or permitted on, the organization's network. The associated AP classification is *Suspected Rogue*, meaning the AP has been detected and classified as a potential unauthorized threat that warrants investigation. Viewing these two classifications together is important in the Security Dashboard because an organization-associated device communicating through a suspected rogue AP can indicate an unsafe association, such as an evil-twin or other unauthorized wireless device attempting to attract legitimate users. The client MAC address provides the specific endpoint that the administrator should investigate, while the AP classification identifies the potentially malicious infrastructure involved. ArubaOS provides monitoring and wireless intrusion-protection information to help administrators identify and investigate these kinds of wireless security events. See the ArubaOS documentation resources at ArubaOS Monitoring documentation and the Aruba Security Dashboard documentation.

QUESTION NO: 18

You are deploying EAP-TLS authentication for managed wireless clients. Which two client-side requirements are necessary for a successful and secure deployment? (Select two)

A. A valid client certificate with its associated private key.

B. Trust for the CA that issued the ClearPass RADIUS server certificate.

C. A copy of the ClearPass RADIUS server private key.

D. A shared WPA2-Personal passphrase for the WLAN.

E. A local administrator account on the Mobility Controller.

ANSWER: A B

Explanation:

Each supplicant needs a valid client certificate and access to its associated private key so it can prove possession of the certificate during the TLS exchange. The supplicant must also trust the CA that issued the ClearPass RADIUS server certificate and validate that certificate. This allows the client to authenticate the server before presenting its own credential.

The RADIUS server private key must remain protected on the server and must never be distributed to clients. Aruba documents EAP-TLS configuration and certificate requirements in the ClearPass EAP-TLS documentation.

QUESTION NO: 19

You configure an ArubaOS-Switch to enforce 802.1X authentication with ClearPass Policy Manager (CPPM) denned as the RADIUS server Clients cannot authenticate You check Aruba ClearPass Access Tracker and cannot find a record of the authentication attempt.

What are two possible problems that have this symptom? (Select two)

A. users are logging in with the wrong usernames and passwords or invalid certificates.

B. Clients are configured to use a mismatched EAP method from the one In the CPPM service.

C. The RADIUS shared secret does not match between the switch and CPPM.

D. CPPM does not have a network device defined for the switch's IP address.

E. Clients are not configured to trust the root CA certificate for CPPM's RADIUS/EAP certificate.

ANSWER: C D

Explanation:

The RADIUS shared secret does not match between the switch and CPPM, and CPPM does not have a network device defined for the switch's IP address, are both problems that can prevent ClearPass from creating a normal Access Tracker transaction. ClearPass first has to recognize and validate the RADIUS client that sent the packet. The network-device definition associates the switch's RADIUS source IP address with its device configuration and shared secret. If the switch source address is not defined as a network device, ClearPass cannot identify the sender as an authorized RADIUS client. If the shared secret differs, the RADIUS packet authenticator cannot be validated. In either case, packet validation fails before ClearPass can process the request through a service, perform EAP authentication, and generate the usual Access Tracker entry. The correct troubleshooting workflow is therefore to verify the switch's actual RADIUS source IP address, confirm that this exact address is configured as a ClearPass network device, and ensure that the shared secret is identical on both the switch and ClearPass. RADIUS shared-secret validation is defined in RFC 2865, section 3; Aruba's ClearPass documentation also describes network-device configuration and monitoring through ClearPass Policy Manager documentation.

QUESTION NO: 20

A company has an ArubaOS controller-based solution with a WPA3-Enterprise WLAN. which authenticates wireless clients to Aruba ClearPass Policy Manager (CPPM). The company has decided to use digital certificates for authentication A user's Windows domain computer has had certificates installed on it However, the Networks and Connections window shows that authentication has tailed for the user. The Mobility Controllers (MC's) RADIUS events show that it is receiving Access-Rejects for the authentication attempt.

What is one place that you can you look for deeper insight into why this authentication attempt is failing?

A. the reports generated by Aruba ClearPass Insight

B. the RADIUS events within the CPPM Event Viewer

C. the Alerts tab in the authentication record in CPPM Access Tracker

D. the packets captured on the MC control plane destined to UDP 1812

ANSWER: C

Explanation:

The Alerts tab in the authentication record in CPPM Access Tracker is the best place to investigate this certificate-based authentication failure. Access Tracker records the complete processing path for an individual authentication request, allowing an administrator to locate the specific rejected attempt and inspect the messages generated while ClearPass evaluated it. For an enterprise wireless connection using certificates, the alerts can expose meaningful authentication diagnostics, such as certificate-chain validation problems, an untrusted issuing authority, an expired certificate, a certificate identity mismatch, or an issue encountered during the EAP-TLS exchange. This is especially useful when the controller has already confirmed only the final RADIUS result—Access-Reject—because the controller does not necessarily show the detailed reason ClearPass arrived at that decision. The administrator can correlate the failed Windows client attempt by time, username, endpoint details, or request attributes, then open its Access Tracker record and review the Alerts information alongside the request-processing details. This provides the actionable ClearPass-side evidence needed to correct the certificate, trust configuration, or authentication policy. Aruba documents Access Tracker as the interface for viewing and troubleshooting individual authentication requests in the ClearPass Policy Manager Access Tracker documentation. Additional ClearPass administration resources are available from the Aruba ClearPass documentation portal.