HPE6-A78최신인증시험자료시험준비에가장좋은최신공부자료

참고: PassTIP에서 Google Drive로 공유하는 무료 2025 HP HPE6-A78 시험 문제집이 있습니다: https://drive.google.com/open?id=1w4cwHU4K5XmgBouNCtl5xdAVmzHPuWhm

PassTIP의 HP인증 HPE6-A78시험덤프자료는 IT인사들의 많은 찬양을 받아왔습니다.이는PassTIP의 HP인증 HPE6-A78덤프가 신뢰성을 다시 한번 인증해주는것입니다. HP인증 HPE6-A78시험덤프의 인기는 이 시험과목이 얼마나 중요한지를 증명해줍니다. PassTIP의 HP인증 HPE6-A78덤프로 이 중요한 IT인증시험을 준비하시면 우수한 성적으로 시험을 통과하여 인정받는 IT전문가로 될것입니다.

HP HPE6-A78 시험을 준비하기 위해 응시자는 온라인 과정, 학습 가이드 및 실습 시험과 같은 다양한 학습 자료를 활용할 수 있습니다. 이러한 리소스는 응시자가 시험 주제에 대한 더 깊은 이해를 얻고 시험에 합격하는 데 필요한 기술을 개발할 수 있도록 도와줍니다.

>> HPE6-A78최신 인증시험자료 <<

시험패스 가능한 HPE6-A78최신 인증시험자료 덤프공부

HP HPE6-A78 시험탈락시HP HPE6-A78덤프비용전액을 환불해드릴만큼 저희 덤프자료에 자신이 있습니다. PassTIP에서는HP HPE6-A78덤프를 항상 최신버전이도록 보장해드리고 싶지만HP HPE6-A78시험문제변경시점을 예측할수 없어 시험에서 불합격받을수도 간혹 있습니다. 하지만 시험에서 떨어지면 덤프비용을 전액 환불해드려 고객님의 이익을 보장해드립니다.

HPE6-A78 시험은 Aruba 제품을 사용하여 네트워크 보안 솔루션을 설계, 구현 및 관리하는 개인을 대상으로합니다.

여기에는 네트워크 관리자, 보안 분석가 및 Aruba 제품 및 솔루션과 함께 일하는 기타 IT 전문가가 포함됩니다. 인증 시험은 Aruba의 보안 기능 및 모범 사례에 대한 후보자의 이해뿐만 아니라 Aruba Security Solutions를 구성하고 관리하는 능력을 검증하도록 설계되었습니다. HPE6-A78 시험의 성공적인 완료는 후보자가 Aruba 네트워크를 확보하고 위협으로부터 보호하는 데 필요한 지식과 기술을 가지고 있음을 보여줍니다.

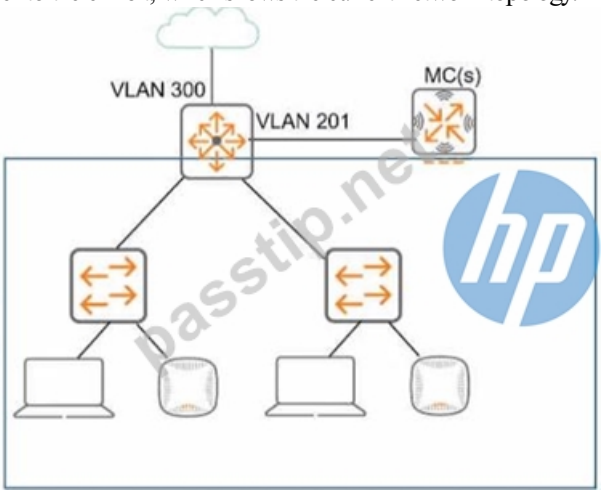
최신 Aruba ACNSA HPE6-A78 무료샘플문제 (Q108-Q113):

질문 # 108
You have deployed a new Aruba Mobility Controller (MC) and campus APs (CAPs). One of the WLANs enforces 802.IX authentication lo Aruba ClearPass Policy Manager {CPPM) When you test connecting the client to the WLAN. the test falls You check Aruba ClearPass Access Tracker and cannot find a record of the authentication attempt You ping from the MC to CPPM. and the ping is successful.
What is a good next step for troubleshooting?

- A. Renew CPPM's RADIUS/EAP certificate
- B. Check connectivity between CPPM and a backend directory server
- C. Reset the user credentials
- D. Check CPPM Event viewer.

정답：D

질문 # 109
Refer to the exhibit, which shows the current network topology.



You are deploying a new wireless solution with an Aruba Mobility Master (MM). Aruba Mobility Controllers (MCs). and campus APs (CAPs). The solution will Include a WLAN that uses Tunnel for the forwarding mode and Implements WPA3-Enterprise security What is a guideline for setting up the vlan for wireless devices connected to the WLAN?

- A. Assign the WLAN to a named VLAN which specified 100-150 as the range of IDs.
- B. Use wireless user roles to assign the devices to different VLANs in the 100-150 range
- C. Assign the WLAN to a single new VLAN which is dedicated to wireless users
- D. Use wireless user roles to assign the devices to a range of new vlan IDs.

정답：B

설명:
When setting up VLANs for a wireless solution with an Aruba Mobility Master (MM), Aruba Mobility Controllers (MCs), and campus APs (CAPs), it is recommended to use wireless user roles to assign devices to different VLANs. This allows for greater flexibility and control over network resources and policies applied to different user groups. Wireless user roles can dynamically assign devices to the appropriate VLAN based on a variety of criteria such as user identity, device type, location, and the resources they need to access. This approach aligns with the ArubaOS features that leverage user roles for network access control, as detailed in Aruba's configuration and administration guides.

질문 # 110

You have configured a WLAN to use Enterprise security with the WPA3 version.
How does the WLAN handle encryption?

- A. Traffic is encrypted with AES and keys derived from a PMK shared by all clients on the WLAN.
- B. Traffic is encrypted with AES and keys derived from a unique PMK per client.
- C. Traffic is encrypted with TKIP and keys derived from a unique PMK per client.
- D. Traffic is encrypted with TKIP and keys derived from a PMK shared by all clients on the WLAN.

정답：B

설명:
WPA3-Enterprise is a security protocol introduced to enhance the security of wireless networks, particularly in enterprise environments. It builds on the foundation of WPA2 but introduces stronger encryption and key management practices. In WPA3-Enterprise, authentication is typically performed using 802.1X, and encryption is handled using the Advanced Encryption Standard (AES).
WPA3-Enterprise Encryption: WPA3-Enterprise uses AES with the Galois/Counter Mode Protocol (GCMP) or Cipher Block Chaining Message Authentication Code Protocol (CCMP), both of which are AES-based encryption methods. WPA3 does not use TKIP (Temporal Key Integrity Protocol), which is a legacy encryption method used in WPA and early WPA2 deployments and is considered insecure.
Pairwise Master Key (PMK): In WPA3-Enterprise, the PMK is derived during the 802.1X authentication process (e.g., via EAP-TLS or EAP-TTLS). Each client authenticates individually with the authentication server (e.g., ClearPass), resulting in a unique PMK for each client. This PMK is then used to derive session keys (Pairwise Transient Keys, PTKs) for encrypting the client's traffic, ensuring that each client's traffic is encrypted with unique keys.
Option A, "Traffic is encrypted with TKIP and keys derived from a PMK shared by all clients on the WLAN," is incorrect because WPA3 does not use TKIP (it uses AES), and the PMK is not shared among clients in WPA3-Enterprise; each client has a unique PMK.
Option B, "Traffic is encrypted with TKIP and keys derived from a unique PMK per client," is incorrect because WPA3 does not use TKIP; it uses AES.
Option C, "Traffic is encrypted with AES and keys derived from a PMK shared by all clients on the WLAN," is incorrect because, in WPA3-Enterprise, the PMK is unique per client, not shared.
Option D, "Traffic is encrypted with AES and keys derived from a unique PMK per client," is correct. WPA3-Enterprise uses AES for encryption, and each client derives a unique PMK during 802.1X authentication, which is used to generate unique session keys for encryption.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"WPA3-Enterprise enhances security by using AES encryption with GCMP or CCMP. In WPA3-Enterprise mode, each client authenticates via 802.1X, resulting in a unique Pairwise Master Key (PMK) for each client. The PMK is used to derive session keys (Pairwise Transient Keys, PTKs) that encrypt the client's traffic with AES, ensuring that each client's traffic is protected with unique keys. WPA3 does not support TKIP, which is a legacy encryption method." (Page 285, WPA3-Enterprise Security Section)
Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"WPA3-Enterprise requires 802.1X authentication, which generates a unique PMK for each client. This PMK is used to derive AES-based session keys, providing individualized encryption for each client's traffic and eliminating the risks associated with shared keys." (Page 32, WPA3 Security Features Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, WPA3-Enterprise Security Section, Page 285.
HPE Aruba Networking Wireless Security Guide, WPA3 Security Features Section, Page 32.

질문 # 111
What purpose does an initialization vector (IV) serve for encryption?

- A. It enables the conversion of asymmetric keys into keys that are suitable for symmetric encryption.
- B. It helps parties to negotiate the keys and algorithms used to secure data before data transmission.
- C. It makes encryption algorithms more secure by ensuring that same plaintext and key can produce different ciphertext.
- D. It enables programs to convert easily-remembered passphrases to keys of a correct length.

정답：C

설명:
The primary purpose of an Initialization Vector (IV) in encryption is to ensure that the same plaintext encrypted with the same encryption key will produce different ciphertext each time it is encrypted. This variability is crucial for securing repetitive data patterns and preventing certain types of cryptographic attacks, such as replay or pattern analysis attacks. The IV adds randomness

to the encryption process, making it more secure by ensuring that encrypted messages are unique, even if the plaintext and key remain unchanged. This prevents attackers from deducing patterns or inferring any useful information from repeated ciphertext.

질문 # 112
Refer to the exhibits.
An admin has created a WLAN that uses the settings shown in the exhibits (and has not otherwise adjusted the settings in the AAA profile). A client connects to the WLAN. Under which circumstances will a client receive the default role assignment?

- A. The client has passed 802.1X authentication, and the value in the Aruba-User-Role VSA matches a role on the MC.
- B. The client has attempted 802.1X authentication, but failed to maintain a reliable connection, leading to a timeout error.
- C. The client has attempted 802.1X authentication, but the MC could not contact the authentication server.
- D. The client has passed 802.1X authentication, and the authentication server did not send an Aruba-User-Role VSA.

정답：D

설명:
The exhibit shows the configuration of a WLAN on an AOS-8 Mobility Controller (MC) with the following settings:
Key management: WPA3-Enterprise (indicating 802.1X authentication).
Use CNSA suite: Unchecked (using standard encryption, not the Commercial National Security Algorithm suite).
Key size: 128 bits (standard for AES-GCMP in WPA3).
Reauth interval: 1440 minutes (24 hours, the interval for re-authentication).
Machine authentication: Disabled (only user authentication is required).
Blacklisting: Disabled (clients are not blacklisted after failed attempts).
The question states that the AAA profile settings have not been adjusted, meaning the default roles (e.g., initial role, logon role, 802.1X default role) are not specified in the exhibit and are assumed to be the system defaults (e.g., "logon" for the initial and logon roles, and a default role like "guest" for the 802.1X default role). The question asks under which circumstances a client will receive the "default role assignment," which refers to the 802.1X default role configured in the AAA profile for the WLAN.
802.1X Authentication Process in AOS-8:
When a client connects to a WPA3-Enterprise WLAN, it starts in the initial role (typically "logon") to allow basic connectivity (e.g., DHCP, DNS).
During 802.1X authentication, the client is placed in the logon role to allow communication with the authentication server (e.g., ClearPass Policy Manager, CPPM).
If authentication succeeds, the client is assigned a role:
If the authentication server (e.g., CPPM) sends an Aruba-User-Role VSA with a role that exists on the MC, the client is assigned that role.
If no Aruba-User-Role VSA is sent, the client is assigned the 802.1X default role configured in the AAA profile for the WLAN.
If authentication fails or the server is unreachable, the client may be assigned a different role (e.g., a critical role, if configured) or denied access.
Option A, "The client has attempted 802.1X authentication, but the MC could not contact the authentication server," is incorrect. If the MC cannot contact the authentication server (e.g., due to a timeout), the client does not receive the 802.1X default role. Instead, the MC may apply a critical role (if configured) or deny access, depending on the configuration. The 802.1X default role is applied only after successful authentication.
Option B, "The client has passed 802.1X authentication, and the authentication server did not send an Aruba-User-Role VSA," is correct. If the client successfully authenticates via 802.1X and the authentication server (e.g., CPPM) does not send an Aruba-User-Role VSA, the MC assigns the client the 802.1X default role configured in the AAA profile for the WLAN. This is the "default role assignment" referred to in the question.
Option C, "The client has attempted 802.1X authentication, but failed to maintain a reliable connection, leading to a timeout error," is incorrect. A timeout error during authentication (e.g., the client fails to respond to EAP messages) typically results in an authentication failure, not a successful authentication. The client would not receive the 802.1X default role; it might be denied access or placed in a different role (e.g., a pre-authentication role).
Option D, "The client has passed 802.1X authentication, and the value in the Aruba-User-Role VSA matches a role on the MC," is incorrect. If the authentication server sends an Aruba-User-Role VSA with a role that exists on the MC, the client is assigned that specific role, not the 802.1X default role.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"After a client successfully authenticates via 802.1X, the Mobility Controller assigns a role to the client. If the authentication server (e.g., a RADIUS server) sends an Aruba-User-Role VSA with a role that exists on the controller, the client is assigned that role. If no Aruba-User-Role VSA is sent in the Access-Accept message, the client is assigned the 802.1X default role configured in the AAA profile for the WLAN. For example, if the AAA profile specifies 'guest' as the 802.1X default role, the client will be assigned the 'guest' role." (Page 305, Role Assignment Section) Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"In WPA3-Enterprise with 802.1X authentication, the default role assignment occurs when a client successfully authenticates but the

authentication server does not specify a role via the Aruba-User-Role VSA. In this case, the client receives the 802.1X default role defined in the AAA profile, such as 'guest' or another role configured by the administrator." (Page 42, 802.1X Role Assignment Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Role Assignment Section, Page 305.
HPE Aruba Networking Wireless Security Guide, 802.1X Role Assignment Section, Page 42.

질문 # 113
.....