[UPDATED 2024 Free HP HPE6-A78 Exam Questions Self-Assess Preparation [Q29-Q52

[UPDATED 2024] Free HP HPE6-A78 Exam Questions Self-Assess Preparation
HPE6-A78 Free Sample Questions to Practice One Year Update

HPE6-A78 exam is a challenging exam that requires a comprehensive understanding of network security concepts and technologies. HPE6-A78 exam consists of 60 multiple-choice questions, and the candidate must complete the exam within 90 minutes. To pass the exam, the candidate must score at least 70% or higher. HPE6-A78 exam is available in multiple languages, including English, Japanese, French, Spanish, Portuguese, and more. HPE6-A78 exam can be taken online or at a testing center, and the certification is valid for three years.

QUESTION 29

What is one way that WPA3-PerSonal enhances security when compared to WPA2-Personal?
* WPA3-Perscn3i is more secure against password leaking Because all users nave their own username and password
* WPA3-Personai prevents eavesdropping on other users&#8217; wireless traffic by a user who knows the passphrase for the WLAN.

* WPA3-Personai is more resistant to passphrase cracking Because it requires passphrases to be at least 12 characters
* WPA3-Personal is more complicated to deploy because it requires a backend authentication server

QUESTION 30

You are troubleshooting an authentication issue for Aruba switches that enforce 802 IX10 a cluster of Aruba ClearPass Policy Manager (CPPMs) You know that CPPM Is receiving and processing the authentication requests because the Aruba switches are showing Access-Rejects in their statistics However, you cannot find the record tor the Access-Rejects in CPPM Access Tracker What is something you can do to look for the records?
* Make sure that CPPM cluster settings are configured to show Access-Rejects
* Verify that you are logged in to the CPPM Ul with read-write, not read-only, access
* Click Edit in Access viewer and make sure that the correct servers are selected.
* Go to the CPPM Event Viewer, because this is where RADIUS Access Rejects are stored.

QUESTION 31

What is one difference between EAP-Tunneled Layer security (EAP-TLS) and Protected EAP (PEAP)?
* EAP-TLS creates a TLS tunnel for transmitting user credentials, while PEAP authenticates the server and supplicant during a TLS handshake.
* EAP-TLS requires the supplicant to authenticate with a certificate, hut PEAP allows the supplicant to use a username and password.
* EAP-TLS begins with the establishment of a TLS tunnel, but PEAP does not use a TLS tunnel as part of Its process
* EAP-TLS creates a TLS tunnel for transmitting user credentials securely while PEAP protects user credentials with TKIP encryption.

QUESTION 32

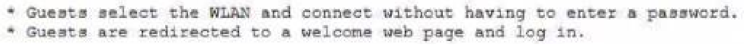
What is a vulnerability of an unauthenticated Dime-Heliman exchange?
* A hacker can replace the public values exchanged by the legitimate peers and launch an MITM attack.
* A brute force attack can relatively quickly derive Diffie-Hellman private values if they are able to obtain public values
* Diffie-Hellman with elliptic curve values is no longer considered secure in modem networks, based on NIST recommendations.
* Participants must agree on a passphrase in advance, which can limit the usefulness of Diffie- Hell man in practical contexts.

QUESTION 33

What is a guideline for creating certificate signing requests (CSRs) and deploying server Certificates on ArubaOS Mobility Controllers (MCs)?
* Create the CSR online using the MC Web Ul if your company requires you to archive the private key.
* if you create the CSR and public/private Keypair offline, create a matching private key online on the MC.
* Create the CSR and public/private keypair offline If you want to install the same certificate on multiple MCs.
* Generate the private key online, but the public key and CSR offline, to install the same certificate on multiple MCs.

QUESTION 34

A company with 382 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 mat are capable, you implement Tor the WLAN?

Which security options should
* WPA3-Personal and MAC-Auth
* Captive portal and WPA3-Personai
* Captive portal and Opportunistic Wireless Encryption (OWE) in transition mode
* Opportunistic Wireless Encryption (OWE) and WPA3-Personal

QUESTION 35

How does the ArubaOS firewall determine which rules to apply to a specific client&#8217;s traffic?
* The firewall applies every rule that includes the dent&#8217;s IP address as the source.
* The firewall applies the rules in policies associated with the client&#8217;s wlan
* The firewall applies thee rules in policies associated with the client&#8217;s user role.
* The firewall applies every rule that includes the client&#8217;s IP address as the source or destination.

QUESTION 36

What are the roles of 802.1X authenticators and authentication servers?
* The authenticator stores the user account database, while the server stores access policies.
* The authenticator supports only EAP, while the authentication server supports only RADIUS.
* The authenticator is a RADIUS client and the authentication server is a RADIUS server.
* The authenticator makes access decisions and the server communicates them to the supplicant.

QUESTION 37

What is one of the roles of the network access server (NAS) in the AAA framewonx?
* It authenticates legitimate users and uses policies to determine which resources each user is allowed to access.
* It negotiates with each user&#8217;s device to determine which EAP method is used for authentication
* It enforces access to network services and sends accounting information to the AAA server
* It determines which resources authenticated users are allowed to access and monitors each users session

QUESTION 38

What is a correct guideline for the management protocols that you should use on ArubaOS-Switches?
* Disable Telnet and use TFTP instead.
* Disable SSH and use https instead.
* Disable Telnet and use SSH instead
* Disable HTTPS and use SSH instead

QUESTION 39

You are deploying an Aruba Mobility Controller (MC). What is a best practice for setting up secure management access to the ArubaOS Web UP
* Avoid using external manager authentication tor the Web UI.
* Change the default 4343 port tor the web UI to TCP 443.
* Install a CA-signed certificate to use for the Web UI server certificate.
* Make sure to enable HTTPS for the Web UI and select the self-signed certificate Installed in the factory.

QUESTION 40

Which is a correct description of a stage in the Lockheed Martin kill chain?

* In the delivery stage, malware collects valuable data and delivers or exfilltrated it to the hacker.
* In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfilltrated.
* In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes Its function.
* In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker.

QUESTION 41

How should admins deal with vulnerabilities that they find in their systems?
* They should apply fixes, such as patches, to close the vulnerability before a hacker exploits it.
* They should add the vulnerability to their Common Vulnerabilities and Exposures (CVE).
* They should classify the vulnerability as malware. a DoS attack or a phishing attack.
* They should notify the security team as soon as possible that the network has already been breached.

QUESTION 42

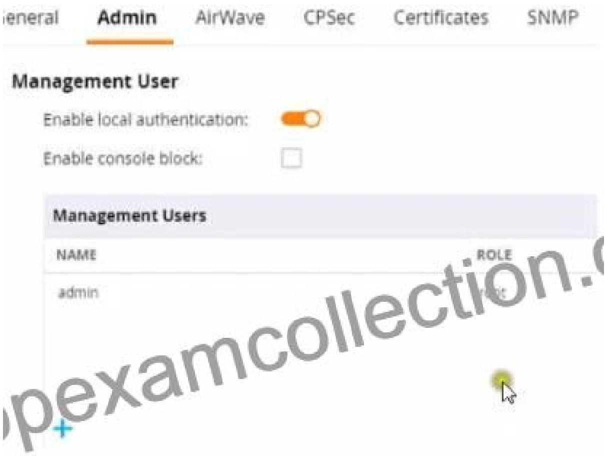
What distinguishes a Distributed Denial of Service (DDoS) attack from a traditional Denial or service attack (DoS)?
* A DDoS attack originates from external devices, while a DoS attack originates from internal devices
* A DDoS attack is launched from multiple devices, while a DoS attack is launched from a single device
* A DoS attack targets one server, a DDoS attack targets all the clients that use a server
* A DDoS attack targets multiple devices, while a DoS Is designed to Incapacitate only one device

QUESTION 43

Which correctly describes a way to deploy certificates to end-user devices?
* ClearPass Onboard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain
* ClearPass Device Insight can automatically discover end-user devices and deploy the proper certificates to them
* ClearPass OnGuard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain
* in a Windows domain, domain group policy objects (GPOs) can automatically install computer, but not user certificates

QUESTION 44

Refer to the exhibit.



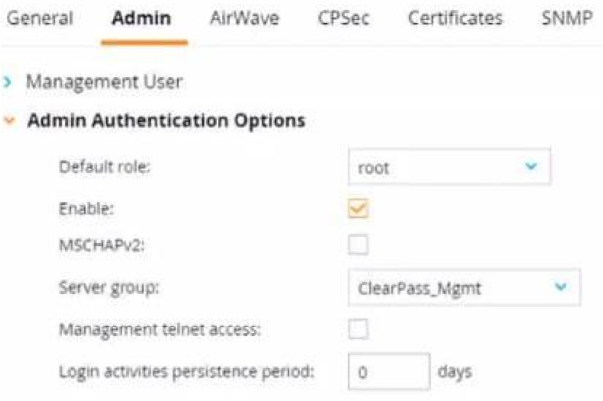
Management User

Enable local authentication: ●

Enable console block: □

Management Users

NAME	ROLE
admin	root



Admin Authentication Options

Default role: root

Enable: ☑

MSCHAPv2: □

Server group: ClearPass_Mgmt

Management telnet access: □

Login activities persistence period: 0 days

This Aruba Mobility Controller (MC) should authenticate managers who access the Web Ul to ClearPass Policy Manager (CPPM) ClearPass admins have asked you to use RADIUS and explained that the MC should accept managers&#8217; roles in Aruba-Admin-Role VSAs Which setting should you change to follow Aruba best security practices?

* Change the local user role to read-only
* Clear the MSCHAP check box
* Disable local authentication
* Change the default role to &#8220;guest-provisioning&#8221;

QUESTION 45

From which solution can ClearPass Policy Manager (CPPM) receive detailed information about client device type OS and status?

* ClearPass Onboard
* ClearPass Access Tracker
* ClearPass OnGuard
* ClearPass Guest

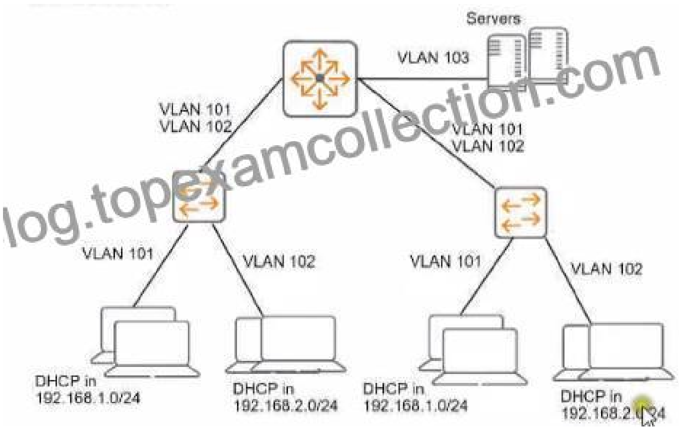
QUESTION 46

What correctly describes the Pairwise Master Key (PMK) in thee specified wireless security protocol?

* In WPA3-Enterprise, the PMK is unique per session and derived using Simultaneous Authentication of Equals.
* In WPA3-Personal, the PMK is unique per session and derived using Simultaneous Authentication of Equals.
* In WPA3-Personal, the PMK is derived directly from the passphrase and is the same tor every session.
* In WPA3-Personal, the PMK is the same for each session and is communicated to clients that authenticate

QUESTION 47

Refer to the exhibit.

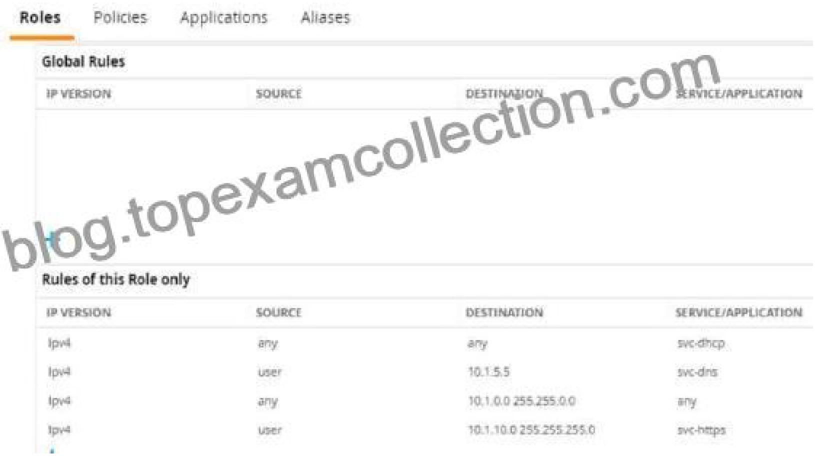


You need to ensure that only management stations in subnet 192.168.1.0/24 can access the ArubaOS-Switches&#8217; CLI. Web Ul. and REST interfaces The company also wants to let managers use these stations to access other parts of the network What should you do?

* Establish a Control Plane Policing class that selects traffic from 192.168 1.0/24.
* Specify 192.168.1.0.255.255.255.0 as authorized IP manager address
* Configure the switch to listen for these protocols on OOBM only.
* Specify vlan 100 as the management vlan for the switches.

QUESTION 48

Refer to the exhibit.



Global Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION

Rules of this Role only

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION
Ipv4	any	any	svc-dhcp
Ipv4	user	10.1.5.5	svc-dns
Ipv4	any	10.1.0.0 255.255.0.0	any
Ipv4	user	10.1.10.0 255.255.255.0	svc-https

A diem is connected to an ArubaOS Mobility Controller. The exhibit snows all Tour firewall rules that apply to this diem What correctly describes how the controller treats HTTPS packets to these two IP addresses, both of which are on the other side of the firewall

10.1 10.10

203.0.13.5

* It drops both of the packets
* It permits the packet to 10.1.10.10 and drops the packet to 203 0.13.5
* it permits both of the packets
* It drops the packet to 10.1.10.10 and permits the packet to 203.0.13.5.

QUESTION 49

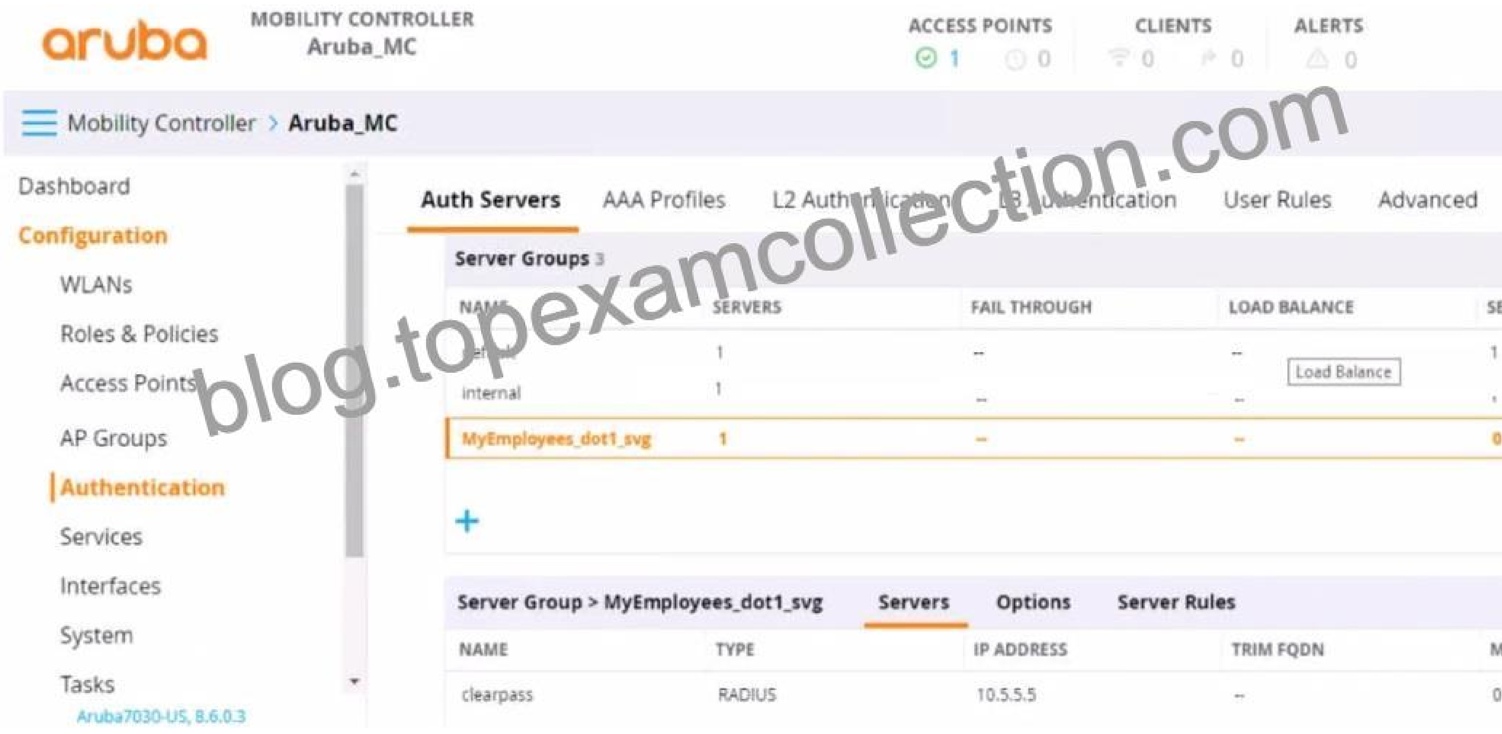
A company has an ArubaOS controller-based solution with a WPA3-Enterprise WLAN. which authenticates wireless clients to Aruba ClearPass Policy Manager (CPPM). The company has decided to use digital certificates for authentication A user&#8217;s Windows domain computer has had certificates installed on it However, the Networks and Connections window shows that authentication has tailed for the user. The Mobility Controllers (MC&#8217;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?

* the reports generated by Aruba ClearPass Insight
* the RADIUS events within the CPPM Event Viewer
* the Alerts tab in the authentication record in CPPM Access Tracker
* the packets captured on the MC control plane destined to UDP 1812

QUESTION 50

Refer to the exhibit.



Server Groups 3

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SE
default	1	--	--	1
internal	1	--	--	1
MyEmployees_dot1_svg	1	--	--	0

Server Group > MyEmployees_dot1_svg — Servers | Options | Server Rules

NAME	TYPE	IP ADDRESS	TRIM FQDN	M
clearpass	RADIUS	10.5.5.5	--	0

You have set up a RADIUS server on an ArubaOS Mobility Controller (MC) when you created a WLAN named &#8220;MyEmployees .You now want to enable the MC to accept change of authorization (CoA) messages from this server for wireless sessions on this WLAN.

What Is a part of the setup on the MC?

- Create a dynamic authorization, or RFC 3576, server with the 10.5.5.5 address and correct shared secret.
- Install the root CA associated with the 10 5.5.5 server&#8217;s certificate as a Trusted CA certificate.
- Configure a ClearPass username and password in the MyEmployees AAA profile.
- Enable the dynamic authorization setting in the &#8220;clearpass&#8221; authentication server settings.

QUESTION 51

What is one practice that can help you to maintain a digital chain or custody In your network?

- Enable packet capturing on Instant AP or Moodily Controller (MC) datepath on an ongoing basis
- Enable packet capturing on Instant AP or Mobility Controller (MC) control path on an ongoing basis.
- Ensure that all network infrastructure devices receive a valid clock using authenticated NTP
- Ensure that all network Infrastructure devices use RADIUS rather than TACACS+ to authenticate managers

QUESTION 52

What is symmetric encryption?

- It simultaneously creates ciphertext and a same-size MAC.
- It any form of encryption mat ensures that thee ciphertext Is the same length as the plaintext.
- It uses the same key to encrypt plaintext as to decrypt ciphertext.
- It uses a Key that is double the size of the message which it encrypts.