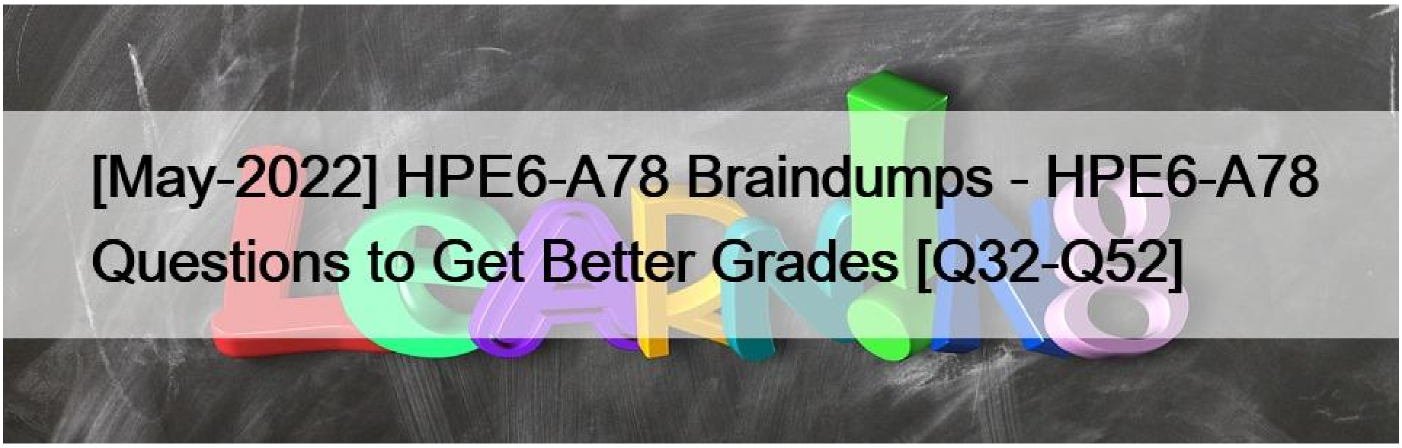
[May-2022 HPE6-A78 Braindumps - HPE6-A78 Questions to Get Better Grades [Q32-Q52



[May-2022] HPE6-A78 Braindumps &ndash; HPE6-A78 Questions to Get Better Grades
HPE6-A78 Exam Dumps - Try Best HPE6-A78 Exam Questions - Actualtests4sure

NEW QUESTION 32

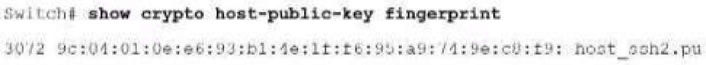
How does the ArubaOS firewall determine which rules to apply to a specific client&#8217;s traffic?
* The firewall applies every rule that includes the dent&#8217;s IP address as the source.
* The firewall applies the rules in policies associated with the client&#8217;s wlan
* The firewall applies thee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

NEW QUESTION 33

What is a benefit of deploying Aruba ClearPass Device insight?
* Highly accurate endpoint classification for environments with many devices types, including Internet of Things (loT)
* visibility into devices&#8217; 802.1X supplicant settings and automated certificate deployment
* Agent-based analysts of devices&#8217; security settings and health status, with the ability to implement quarantining
* Simpler troubleshooting of ClearPass solutions across an environment with multiple ClearPass Policy Managers

NEW QUESTION 34

Refer to the exhibit.



```
Switch# show crypto host-public-key fingerprint
3072 9c:04:01:0e:e6:93:b1:4e:1f:f6:95:a9:74:9e:c8:f9: host_ssh2.pu
```

How can you use the thumbprint?
* Install this thumbprint on management stations to use as two-factor authentication along with manager usernames and passwords,

this will ensure managers connect from valid stations
* Copy the thumbprint to other Aruba switches to establish a consistent SSH Key for all switches this will enable managers to connect to the switches securely with less effort
* When you first connect to the switch with SSH from a management station, make sure that the thumbprint matches to ensure that a man-in-t he-mid die (MITM) attack is not occurring
* install this thumbprint on management stations the stations can then authenticate with the thumbprint instead of admins having to enter usernames and passwords.

NEW QUESTION 35

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

NEW QUESTION 36

A company has Aruba Mobility Controllers (MCs). Aruba campus APs. and ArubaOS-CX switches. The company plans to use ClearPass Policy Manager (CPPM) to classify endpoints by type The ClearPass admins tell you that they want to run Network scans as part of the solution What should you do to configure the infrastructure to support the scans?
* Create a TA profile on the ArubaOS-Switches with the root CA certificate for ClearPass&#8217;s HTTPS certificate
* Create device fingerprinting profiles on the ArubaOS-Switches that include SNMP. and apply the profiles to edge ports
* Create remote mirrors on the ArubaOS-Swrtches that collect traffic on edge ports, and mirror it to CPPM&#8217;s IP address.
* Create SNMPv3 users on ArubaOS-CX switches, and make sure that the credentials match those configured on CPPM

NEW QUESTION 37

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)
* users are logging in with the wrong usernames and passwords or invalid certificates.
* Clients are configured to use a mismatched EAP method from the one In the CPPM service.
* The RADIUS shared secret does not match between the switch and CPPM.
* CPPM does not have a network device defined for the switch&#8217;s IP address.
* Clients are not configured to trust the root CA certificate for CPPM&#8217;s RADIUS/EAP certificate.

NEW QUESTION 38

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.

NEW QUESTION 39

What is one way that Control Plane Security (CPsec) enhances security for me network?
* It protects wireless clients&#8217; traffic tunneled between APs and Mobility Controllers, from eavesdropping
* It prevents Denial of Service (DoS) attacks against Mobility Controllers&#8217; (MCs&#8221;) control plane.
* It prevents access from unauthorized IP addresses to critical services, such as SSH on Mobility Controllers (MCs).
* It protects management traffic between APs and Mobility Controllers (MCs) from eavesdropping.

NEW QUESTION 40

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

NEW QUESTION 41

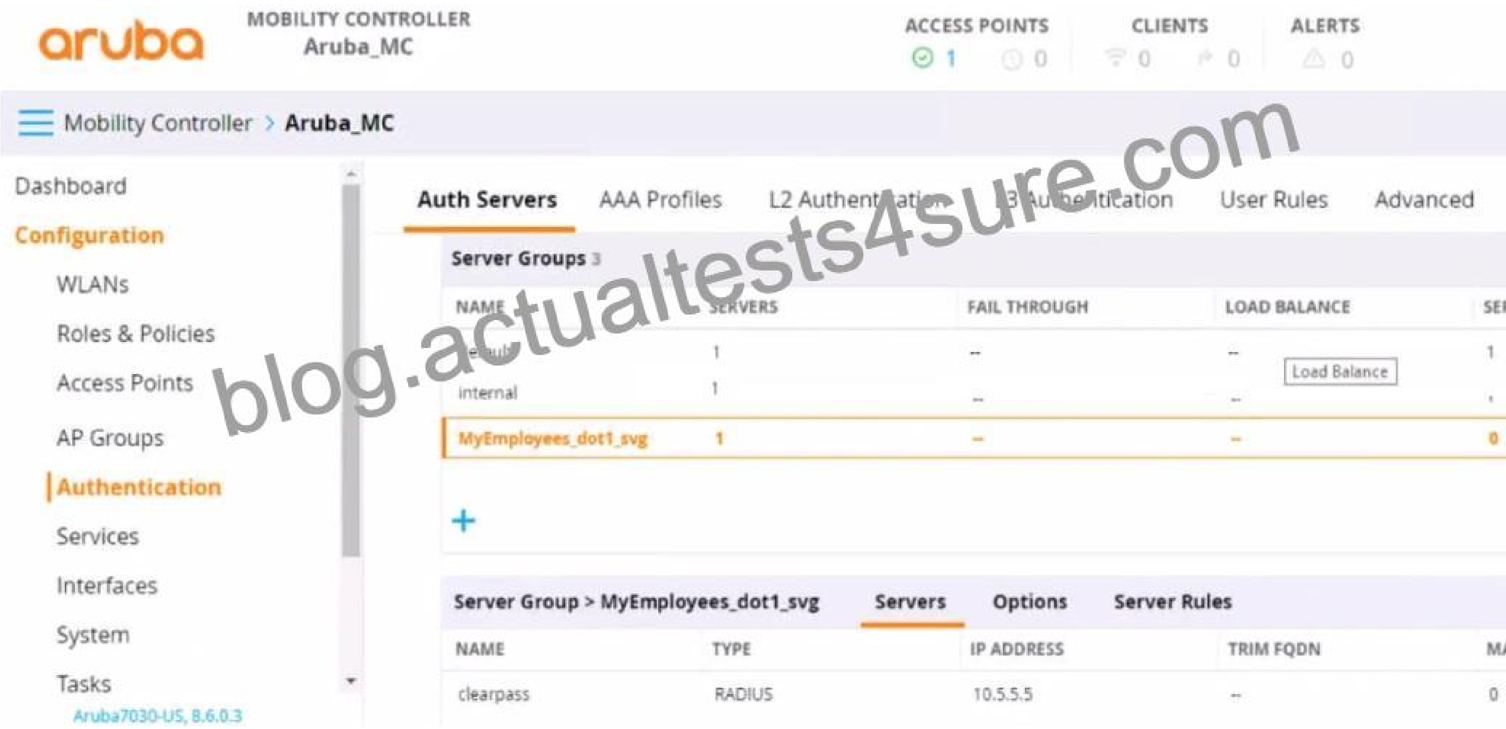
What is one of the roles of the network access server (NAS) in the AAA framewonx?
* It authenticates legitimate users and uses policies to determine which resources each user is allowed to access.
* It negotiates with each user&#8217;s device to determine which EAP method is used for authentication
*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

NEW QUESTION 42

What is an example or phishing?
* An attacker sends TCP messages to many different ports to discover which ports are open.
* An attacker checks a user&#8217;s password by using trying millions of potential passwords.
* An attacker lures clients to connect to a software-based AP that is using a legitimate SSID.
* An attacker sends emails posing as a service team member to get users to disclose their passwords.

NEW QUESTION 43

Refer to the exhibit.



Server Groups 3

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

Server Group > MyEmployees_dot1_svg   Servers   Options   Server Rules

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

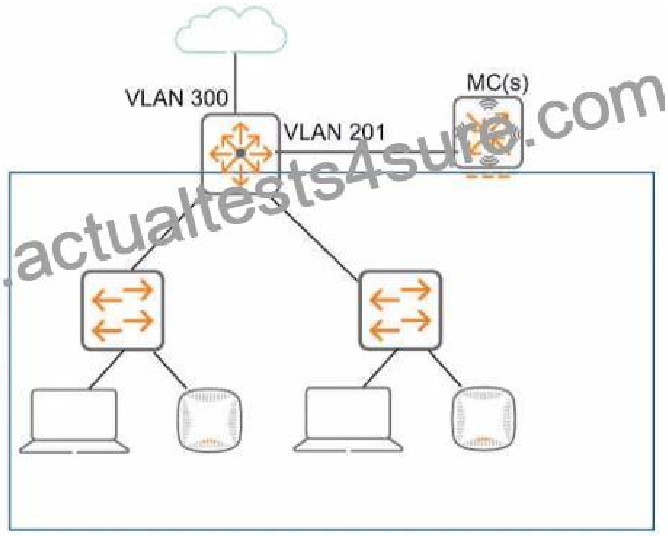
You have set up a RADIUS server on an ArubaOS Mobility Controller (MC) when you created a WLAN named &#8220;MyEmployees .You now want to enable the MC to accept change of authorization (CoA) messages from this server for wireless sessions on this WLAN.

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.

NEW QUESTION 44

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

NEW QUESTION 45

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.

NEW QUESTION 46

You have detected a Rogue AP using the Security Dashboard Which two actions should you take in responding to this event? (Select two)
* There is no need to locale the AP If you manually contain It.
* This is a serious security event, so you should always contain the AP immediately regardless of your company&#8217;s specific policies.
* You should receive permission before containing an AP. as this action could have legal Implications.
* For forensic purposes, you should copy out logs with relevant information, such as the time mat the AP was detected and the AP&#8217;s MAC address.
* There is no need to locate the AP If the Aruba solution is properly configured to automatically contain it.

NEW QUESTION 47

You have been instructed to look in the ArubaOS Security Dashboard&#8217;s client list Your goal is to find clients mat belong to the company and have connected to devices that might belong to hackers Which client fits this description?
* MAC address d8:50:e6:f3;6d;a4; Client Classification Authorized; AP Classification, interfering
* MAC address d8:50:e6 f3;6e;c5; Client Classification Interfering. AP Classification Neighbor
* MAC address d8:50:e6:f3;6e;60; Client Classification Interfering. AP Classification Interfering
* MAC address d8:50:e6:f3;TO;ab; Client Classification Interfering. AP Classification Rogue

NEW QUESTION 48

A company is deploying ArubaOS-CX switches to support 135 employees, which will tunnel client traffic to an Aruba Mobility Controller (MC) for the MC to apply firewall policies and deep packet inspection (DPI).

This MC will be dedicated to receiving traffic from the ArubaOS-CX switches.

What are the licensing requirements for the MC?
* one AP license per-switch
* one PEF license per-switch

* one PEF license per-switch. and one WCC license per-switch
* one AP license per-switch. and one PEF license per-switch

NEW QUESTION 49

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

NEW QUESTION 50

What is a benefit or using network aliases in ArubaOS firewall policies?
* You can associate a reputation score with the network alias to create rules that filler traffic based on reputation rather than IP.
* You can use the aliases to translate client IP addresses to other IP addresses on the other side of the firewall
* You can adjust the IP addresses in the aliases, and the rules using those aliases automatically update
* You can use the aliases to conceal the true IP addresses of servers from potentially untrusted clients.

NEW QUESTION 51

What is one way a noneypot can be used to launch a man-in-the-middle (MITM) attack to wireless clients?
* it uses a combination or software and hardware to jam the RF band and prevent the client from connecting to any wireless networks
* it runs an NMap scan on the wireless client to And the clients MAC and IP address. The hacker then connects to another network and spoofs those addresses.
* it examines wireless clients&#8217; probes and broadcasts the SSlDs in the probes, so that wireless clients will connect to it automatically.
* it uses ARP poisoning to disconnect wireless clients from the legitimate wireless network and force clients to connect to the hacker&#8217;s wireless network instead.

NEW QUESTION 52

What are some functions of an AruDaOS user role?
* The role determines which authentication methods the user must pass to gain network access
* The role determines which firewall policies and bandwidth contract apply to the clients traffic
* The role determines which wireless networks (SSiDs) a user is permitted to access
* The role determines which control plane ACL rules apply to the client&#8217;s traffic

HP HPE6-A78 Exam Syllabus Topics:

TopicDetailsTopic 1- Explain common security protocols and their use cases- Compare endpoint classifications methodsTopic 2-

Identify and evaluate discovered endpoints- Describe common security threatsTopic 3- Collect and monitor historical network pattern data- Describe firewall (PEF), dynamic segmentation, RBAC, AppRFTopic 4- Describe and deploy basic user roles for wireless users- Define and deploy basic user roles for wired usersTopic 5- View and acknowledge WIPS and WIDS, alarms- Troubleshoot with access tracker