HP ACX - Campus Access Mobility HPE7-A07 Practice Questions

Shared by Combs on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

After onboarding three new AOS 10 gateways using the full-setup method into the same Central group, a customer cannot log in to one of the gateways using the HPE Aruba Networking Central remote console due to an incorrect password.

Options:

A- The admin password created using full-setup does not match the global Central admin password.
B- The admin password created during the run-setup process is not configured to allow me remote console access
C- The admin password created during the full-setup process does not match the Central group admin password
D- The admin password created at the Central group level has expired

Answer:

C

Explanation:

When onboarding devices into a centralized management system, each device can have its individual admin password set during the onboarding process. If this password doesn't match what is expected at the group level in the central management platform, login issues such as the one described can occur.

Question 2

Question Type: MultipleChoice

Your customer asked for help to apply an ACL for wireless guest users with the following criteria:

* Wi-Fi guests are on VLAN 555

* allow internet access

* only allow access to public DNS servers

* deny access to all internal networks except for any DHCP server

These session ACLs are already present in the CLI of the mobility gateway group:

```
ip access-list session dns-acl
    any any svc-dns permit
ip access-list session dhcp-acl
    any any svc-dhcp permit
ip access-list session allowall
    any any any permit
    ipv6 any any any permit
ip access-list session internal-networks
    user network 172.16.0.0 255.240.0.0 any deny
    user network 192.168.0.0 255.255.0.0 any deny
    user network 10.0.0.0 255.0.0.0 any deny
```

You have access to the CLl. Which user role meets all the criteria?

A)

```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session internal-networks
    access-list session dns-acl
    vlan 555
```

B)

```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session dns-acl
    access-list session internal-networks
    access-list session allowall
    vlan 555
```

C)

```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session dns-acl
    access-list session internal-networks
    access-list session allowall
    vlan 555
```

D)

```
user-role "WiFi-guest"
    access-list session dns-acl
    access-list session internal-networks
    access-list session dhcp-acl
    access-list session allowall
    vlan 555
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

A

Explanation:

Based on the criteria provided for wireless guest users, the correct user role configuration must allow internet access, only allow access to public DNS servers, deny access to all internal networks except for any DHCP server, and place the Wi-Fi guests on VLAN 555. The ACLs must permit services necessary for basic internet access (such as DNS and DHCP) and block access to internal networks.

Option A satisfies these criteria with the following configurations:

user-role 'WiFi-guest': This defines the role for Wi-Fi guests.

access-list session dhcp-acl: This applies the access list that likely permits DHCP, which is necessary for guests to obtain an IP address.

access-list session dns-acl: This applies the DNS access list, which likely restricts guests to using public DNS servers.

access-list session internal-networks: This applies the internal networks access list, which denies access to internal networks.

vlan 555: This sets the VLAN for Wi-Fi guests to 555.

Options B, C, and D are incorrect because they include access-list session allowall which would permit all traffic, contradicting the requirement to deny access to all internal networks.

Question 3

Question Type: MultipleChoice

A customer's infrastructure is set up to use both primary and secondary gateway clusters on the SSID profile based on best practices What is a valid cause tor having an equal spirt in APs connected to the primary and secondary gateway clusters?

Options:

A- The secondary gateway cluster is heterogeneous
B- The secondary gateway cluster is homogeneous
C- The primary gateway cluster is up. out some APs are unable to reach the primary gateway cluster. These APs would connect to the secondary gateway cluster
D- The primary gateway cluster is up. out some APs cannot reach the secondary gateway cluster. These APs would connect to the secondary gateway cluster

Answer:

C

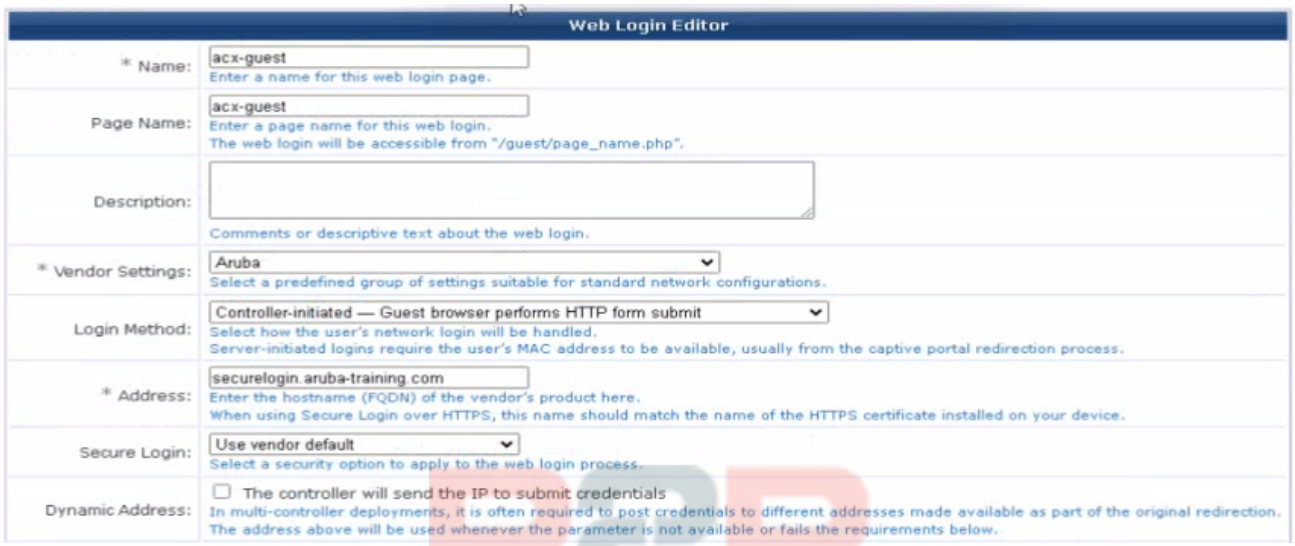
Explanation:

In a high availability setup where both primary and secondary gateway clusters are present, APs are typically designed to connect to the primary cluster. If the APs are equally split between the primary and secondary, this may indicate that some APs cannot reach the primary cluster due to connectivity issues or reachability constraints, thus falling back to the secondary cluster.

Question 4

Question Type: MultipleChoice

Exhibit.



Which would explain this issue?

Options:

A- HTTPS wildcard certificates are not supported
B- HTTPS certificate is not required in ClearPass Guest.
C- captiveportal-login aruba-training com needs to be entered m the Address field for the ClearPass Guest
D- '.aruba-training com needs to be entered in the Address field for the ClearPass Guest

Answer:

D

Explanation:

The correct address for the ClearPass Guest should match the FQDN of the HTTPS certificate installed on the device, which is often the FQDN of the vendor's product. This ensures secure and proper redirection to the captive portal during the authentication process. The FQDN should be entered in the Address field for ClearPass Guest configuration.

Question 5

Question Type: MultipleChoice

You deployed UBT to securely tunnel traffic from user desktop PCs connected behind VOIP phones Ail other non-UBT dents are connected to a different network. After the deployment users reported interruptions lo their phone service

Options:

A- The VLAN on which UBT clients are placed is not configured on the switch uplink and traffic from the VoIP phones is being dropped
B- You tailed to correctly configure a user-defined VRF to support the UBT clients behind the VoIP phones, causing traffic to drop.
C- Broadcast/multicast packets are copied to both the tunnel and locally, causing duplicate packets and network instability
D- The UBT client broadcast/multicast packets returned to the same switch port and corrupted the phones IMC table

Answer:

A

Explanation:

If users report interruptions to their phone service after the deployment of User-Based Tunneling (UBT), it can be due to the VLAN designated for UBT clients not being configured on the switch uplink. As a result, traffic from VoIP phones, which may be trying to use the same VLAN, could be dropped, leading to service interruptions. Ensuring that the VLAN is properly configured on the switch uplink is crucial for the seamless operation of UBT clients and VoIP services.

Question 6

Question Type: MultipleChoice

Which statement is true given the following CLI output from a CX 6300?

```
Central-3-Edge# show bgp l2 evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 172.21.10.3

     Network                                          Nexthop          Metric     LocPrf     Weight
-------------------------------------------------------------------------------------------------------
Route Distinguisher: 172.21.11.2:200      (L2VNI 200)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]      172.21.11.2      0          100        0
*>i [3]:[0]:[172.21.11.2]                             172.21.11.2      0          100        0

Route Distinguisher: 172.21.11.3:200      (L2VNI 200)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]      172.21.11.3      0          100        0
*>  [3]:[0]:[172.21.11.3]                             172.21.11.3      0          100        0

Route Distinguisher: 172.21.11.2:201      (L2VNI 201)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.201.1.1]      172.21.11.2      0          100        0
*>i [2]:[0]:[0]:[78:98:e8:c0:c7:f2]:[10.201.1.100]    172.21.11.2      0          100        0
*>i [2]:[0]:[0]:[78:98:e8:c0:c7:f2]:[]                172.21.11.2      0          100        0
*>i [3]:[0]:[172.21.11.2]                             172.21.11.2      0          100        0

Route Distinguisher: 172.21.10.1:10010      (L3VNI 10010)
*>i [5]:[0]:[0]:[0]:[0.0.0.0]                         172.21.11.1      0          100        0
*>i [5]:[0]:[0]:[24]:[172.21.111.0]                   172.21.11.1      0          100        0

Route Distinguisher: 172.21.10.2:10010      (L3VNI 10010)
*>i [5]:[0]:[0]:[24]:[10.200.1.0]                     172.21.11.2      0          100        0
*>i [5]:[0]:[0]:[24]:[10.201.1.0]                     172.21.11.2      0          100        0

Route Distinguisher: 172.21.10.3:10010      (L3VNI 10010)
*>  [5]:[0]:[0]:[24]:[10.200.1.0]                     172.21.11.3      0          100        0
*>  [5]:[0]:[0]:[24]:[10.201.1.0]                     172.21.11.3      0          100        0

Route Distinguisher: 172.21.11.2:200      (L3VNI 10010)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]      172.21.11.2      0          100        0

*>i [2]:[0]:[0]:her: 172.21.11.2:201      (L3VNI 10010)  172.21.11.2  0  100  0
*>i [2]:[0]:[0]:[78:98:e8:c0:c7:f2]:[]                172.21.11.2      0          100        0

Route Distinguisher: 172.21.11.3:200      (L3VNI 10010)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]      172.21.11.3      0          100        0

Route Distinguisher: 172.21.11.3:201      (L3VNI 10010)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.201.1.1]      172.21.11.3      0          100        0
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[10.201.1.101]   172.21.11.3      0          100        0
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[]                172.21.11.3      0          100        0
Total number of entries 26
```

Options:

A- The underlay loopback addresses are in the 172 21 11 x range.
B- There are two anycast addresses m me overlay fabric.
C- Duplicate MAC addresses were detected in the overlay fabric
D- There are three active client overlay VLANs in the overlay fabric

Answer:

A

Explanation:

The CLI output displays EVPN routes and their corresponding next hops. The 'Route Distinguisher' entries followed by IP addresses in the 172.21.11.x range indicate these are loopback addresses used by the underlay network. The underlay network provides the basic routing and forwarding plane for the overlay network that EVPN is part of. These loopback addresses are crucial for the proper functioning of the EVPN control plane.

Question 7

Question Type: MultipleChoice

Your customer added third-party USB dongles to the USB ports of their AOS 10 access points. The customer uses AP-615 and AP-635 Each AP is connected with a Cat 6A cable to a CX 6300F Class 4 PoE switch All APs are in the same group in HPE Aruba Networking Central and share the same configuration However, many of the dongles do not come up.

Which option will solve this issue?

Options:

A- Replace the Class a PoE switches with Class 6 PoE switches.
B- Create two separate service profiles in the loT tab of the Central configuration settings.
C- Perform a 'poe disable' followed by a 'poe enable' for the switch ports which connect to the APs so that the APs reboot.
D- Move the AP-635 access points to a different group in Central to configure the dongles separately from the AP-615.

Answer:

A

Explanation:

USB dongles often require additional power, which may exceed the power delivery capabilities of Class 4 PoE switches. Aruba AP-615 and AP-635 are designed to work with USB dongles that require additional power for proper operation. Since the Cat 6A cable can support higher power levels, replacing the Class 4 PoE switches with Class 6 PoE switches, which can deliver higher power, should resolve the issue with the dongles not powering up.

Question 8

Question Type: MultipleChoice

You recently added ClearPass as an authentication server to an HPE Aruba Networking Central group. RADIUS authentication with Local User Roles (LUR) works fine Out the same access points cannot use Downloadable User Roles (DUR).

What should he corrected in this configuration to fa the issue with DUR?

Options:

A- Add a new Enforcement Policy of type ''WEBAUTH'' on ClearPass and associate it with the matching service on ClearPass
B- Add the correct IP addresses or IP subnets of the Network Access Devices (NADs) under the 'Devices' tab on ClearPass
C- Replace the AP's expiree digital certificate using the 'crypto pki-import pem serverCert' command.
D- Add the correct values for 'CPPM username' and 'CPPM Password' m the authentication server configuration on HPE Aruba Networking Central

Answer:

B

Explanation:

For Downloadable User Roles (DUR) to function correctly with ClearPass, the Network Access Devices (NADs) need to be correctly defined in ClearPass under the 'Devices' tab. This ensures that ClearPass can identify and communicate with the NADs to deliver the appropriate user roles. If the NADs are not correctly defined, ClearPass will not be able to provide the DURs to the access points for enforcement. This is a common configuration step that is required to integrate ClearPass with network devices for advanced role-based access control.

Question 9

Question Type: MultipleChoice

A customer is evaluating device profiles on a CX 6300 switch. The test device has the following attributes:

* MAC address = 81:cd:93:13:ab:31

* LLDP sys-desc = iotcontroller

The test device is being assigned to the ''lot-dev'' role However, the customer requires the "lot-prod'' role be applied.

```
mac-group iot
     seq 10 match mac-oui 81:cd:93
port-access lldp-group iot-lldp
     seq 10 match sys-desc iot
port-access cdp-group iot-cdp
     seq 10 match platform accesspoint

port-access device-profile iot-dev
    associate role iot-dev
    associate lldp-group iot-lldp
port-access device-profile iot-prod
    associate role iot-prod
    associate mac-group iot
port-access device-profile iot-test
    associate role iot-test
    associate cdp-group iot-cdp
```

Given the configuration, What is causing the "iot-dev" role to be applied to the device'?

Options:

A- The test device does not support CDP.
B- The device-profile precedence order is not configured.
C- An external RADIUS server is unreachable.
D- The LLDP system description matches the IIdp-group configuration.

Answer:

D

Explanation:

In device profile configuration, the device role is often determined by matching attributes such as MAC address, LLDP system description, and CDP information against defined conditions. The test device is being assigned the 'iot-dev' role because its LLDP system description matches the 'iot-lldp' group configuration that is associated with the 'iot-dev' role.

Question 10

Question Type: MultipleChoice

A BGP routing table contains multiple routes to the same destination prefix.

Referring to the table below which route would be marked with a ">" symbol?

Route	Distance	Metric	Origin Code	Local Preference
A		200	i	0
B		0	?	100
C		20	?	0
D	200	0	i	100
E	20	0	i	100

Options:

A- Option A
B- Option B
C- Option C
D- Option D
E- Option E

Answer:

E

Explanation:

In BGP, the route marked with a '>' symbol is the best route that is chosen based on BGP attributes in the following order: highest weight (Cisco-specific), highest local preference, originated by BGP running on the local router, shortest AS path, lowest origin type, lowest MED, eBGP over iBGP, closest IGP neighbor, and lowest BGP router ID. Based on the table provided, Option E would be marked with a '>' symbol as it has the highest local preference of 100 which is a decisive factor in the BGP best path selection process.