Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://de.fast2test.com

Anbieter der Studienmaterialien zur IT-Zertifizierung! Sicher, einfach und schnell. 100%-Pass-Garantie!

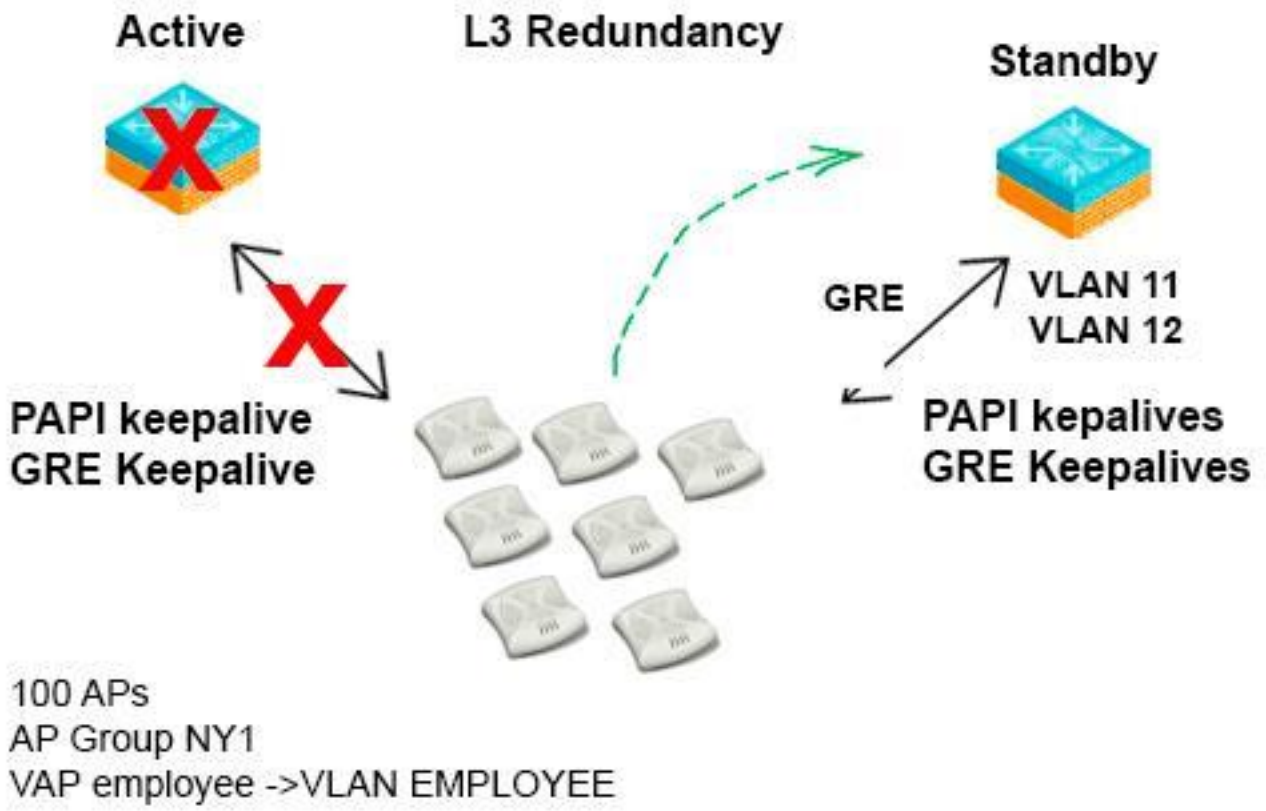
Exam : **HPE6-A40**

Title : Aruba Certified Mobility Expert 6.4 Written Exam

Vendor : HP

Version : DEMO

NO.1 Refer to the exhibit.



The network shown in the exhibits is configured with an active and standby controller that uses Layer 3 redundancy for AP termination. There are 100 APs provisioned into the AP Group NY1. The active local controller fails and the APs terminate on the standby local controller. Centralized licensing is enabled on the controller cluster with capacity for 100 APs. The WLAN clients are not able to SSID. What could be the source of the problem?

A. There are not enough licenses on the standby local controller lo support the APs.

B. The VLAN mapping is not configured on the standby local controller.

C. The uplink trunk of the standby controller does not permit the user VIANs for the SSIO Layer 3 deployment.

D. The IP helper address on the interface VLAN AN is not configured on the standby local controller

Answer: B

NO.2 A network engineer configures guest authentication for a WLAN. The company requires guest to get authenticated through the captive portal. The company's policy allows guests access to the Internet, but not to video streaming sites such as YouTube.
What else should the engineer do to meet these requirements?

A. Deny Web content type video streaming in the network

B. Configure the HTTP and HTTPS traffic for NAT in the Authenticated Guest role.

C. Add*.youtube.com and *.yimg.com to the Walled Garden for the Authenticated Guest role.

D. Utilize AppRF for the Authenticated Guest role to block video streaming

Answer: C

NO.3 Refer to the exhibits on the tabs.

Exhibit 1

```
(Master) #show ap database

AP Database
-----------
Name  Group   Ap Type  IP Address     Status    Flags  Switch IP      Standby IP
----  ------- -------  ------------   --------  -----  ----------     ---------------
AP-1  Local-1 103      172.16.150.254 Up 19m:15s       172.16.100.254 172.16.110.254
AP-2  Local-2 125      172.16.150.251 Up 19m:17s       172.16.110.254 172.16.100.254
AP-2  ACMX    125      172.16.150.252 Up 19m:12s       172.16.99.254  0.0.0.0

Flags:  U = Unprovisioned; N = Duplicate name; G = No such group; L = Unlicensed
        I = Inactive; D = Dirty or no config; E = Regulatory Domain Mismatch
        X = Maintenance Mode; P = PPPoE AP; B = Built-in AP, S = LACP striping
        R = Remote AP; R- = Remote AP requires Auth; C = Cellular RAP;
        C = CERT-based RAP; I = 802.1x authenticated AP; 2 = Using IKE version 2
        u = Custom-Cert RAP; C - Standby-mode AP; J = USB sert at AP
        i = Indoor; o = Outdoor
        M = Mesh node; Y = Mesh Recovery
```

Exhibit 2

```
(Master) #show ap system-profile ACMX

AP system system profile "ACMX"
-------------------------------
Parameter                                   Value
-------------------------                   -------------
RF Band                                     g
RF Band for AM mode scanning                all
Native VLAN ID                              1
Tunnel Heartbeat Interval                   1
Session ACL                                 ap-uplink-acl
Corporate DNS Domain                        N/A
SNMP sysContact                             N/A
LED operating mode (11n/11ac APs only)      normal
LED override                                Disabled
Driver log level                            emergencies
SAP MTU                                     N/A
RAP MTU                                     1200 bytes
LMS IP                                      172.16.99.254
Backup LMS IP                               N/A
LMS IPv6                                    N/A
Backup LMS IPv6                             N/A
LMS Preemption                              Enabled
LMS Hold-down Period                        60 sec
LMS ping interval                           20
```

Exhibit 3

(Master) #show ap system-profile local-1

AP system profile "local-1"

Parameter	Value
RF Band	g
RF Band for AM mode scanning	all
Native VLAN ID	1
Tunnel Heartbeat Interval	1
Session ACL	ap-uplink-ac1
Corporate DNS Domain	N/A
SNMP sysContact	N/A
LED operating mode (11n/11ac APs only)	normal
LED override	Disabled
Driver log level	emergencies
SAP MTU	N/A
RAP MTU	1200 bytes
LMS IP	172.16.100.254
Backup LMS IP	172.16.110.254
LMS IPv6	N/A
Backup LMS IPv6	N/A
LMS Preemption	Enabled
LMS Hold-down Period	60 sec
LMS ping interval	20

(Master) #show ap system-profile local-1

AP system profile "local-1"

Parameter	Value
RF Band	g
RF Band for AM mode scanning	all
Native VLAN ID	1
Tunnel Heartbeat Interval	1
Session ACL	ap-uplink-ac1
Corporate DNS Domain	N/A
SNMP sysContact	N/A
LED operating mode (11n/11ac APs only)	normal
LED override	Disabled
Driver log level	emergencies
SAP MTU	N/A
RAP MTU	1200 bytes
LMS IP	172.16.110.254
Backup LMS IP	172.16.100.254
LMS IPv6	N/A
Backup LMS IPv6	N/A
LMS Preemption	Enabled
LMS Hold-down Period	60 sec
LMS ping interval	20

A network engineer configures AP termination with redundancy. The engineer executes the show ap database command on a master controller. The output is shown in the exhibit.
What can the engineer determine from this output?

A. AP-Groups Local-1, Local-2 are configured with High Availability: Fast Failover LMS, and Backup LMS IP; Backup LMS of the ACMX group is down.

B. AP-Groups Local-1 and Local-2 are configured with High Availability: Fast Failover LMS, and Backup LMS IP; AP-Group ACMX is configured with only HA not LMS or Backup LMS IP.

C. AP-Groups Local-1 and Local-2 are configured with High Availability: Fast Failover LMS, and Backup LMS IP; Backup LMS of the ACMX group is down.

D. AP-Groups Local-1 and Local-2 are configured with High Availability: Fast Failover but not LMS and Backup LMS IP; AP-Groups ACMX is not configured with HA, LMS, or Backup LMS IP.

Answer: C

NO.4 A network engineer troubleshoots a provisioned RAP backup SSID issue that occurs when a user tries to connect to the Internet from a hotel. The engineer test the connection and sees backup SSID from an AP broadcast. The engineer can connect to it and receives an IP address form the RAP's HDCP pool, but the captive portal of the hotel will not come up. The backup SSID is always there, and the enterprise SSID does not appear.
What is a cause of this?

A. The RAP does not Source-NATs user traffic.

B. The hotel blocks UDP port 4500 on the hotel edge firewall

C. The hotel blocks IKE prtocol on the hotel edge firewall

D. The RAP is added into the RAP whitelist of the controller.

Answer: D

NO.5 Refer to the exhibit.

```
(Master) # show aaa authentication captive-portal CP-Auth

Captive Portal Authentication Profile "CP-Auth"
-----------------------------------------------
Parameter                                          Value
---------                                          -----
Default Role                                       guest
Default Guest Role                                 guest
Server Group                                       internal
Redirect Pause                                     10 sec
User Login                                         Enabled
Guest Login                                        Disabled
Logout popup window                                Enabled
Use HTTP for authentication                        Disabled
Logon wait minimum wait                            5 sec
Logon wait maximum wait                            10 sec
Logon wait CPU utilization threshold               60%
Max Authentication failure                         0
Show FQDN                                          Disabled
Authentication Protocol                            PAP
Login page                                         /auth/index.html
Welcome page                                       /auth/welcome.html
Show Welcome Page                                  Yes
Add switch IP address in the redirection URLDisabled Disabled
Adding user vlan in redirection URL                Disabled
Add a controller interface in the redirection URL  N/A
Allow only one active user session                 Disabled
White List                                         N/A
Black List                                         N/A
Show the acceptable use policy page                Disabled
User idle timeout                                  N/A
Redirect URL                                       N/A
Bypass Apple Captive Network Assistant             Disabled
URL Hash Key                                       N/A
```

A network engineer configures a guest WLAN for username and password authentication. As per the company requirements, guests should be authenticated through the captive portal and should accept the terms and conditions. The engineer configures the guest WLAN for authentication, but the guest does not see the terms and conditions page.
What is the issue?

A. The Guest Login should be enabled

B. The Use HTTP For authentication option should be enabled

C. The welcome page should be User_policy.html

D. The Show the Acceptable User Policy Page should be enabled

Answer: D

NO.6 Review to the exhibits on the tabs.
Exhibit 1

```
#show rights logon

Derived Role = "logon"
 Up BW:No Limit  Down BW:No Limit
 L2TP Pool = default-l2tp-pool
 PPTP Pool = default-pptp-pool
 Periodic reauthentication: Disabled
 ACL Number = 1/0
 Max Sessions = 65535

access-list List
------------------
Position   Name              Location
---------  ------            -------------
1          logon-control
2          captiveportal
3          vpnlogon
4          v6-logon-control

logon-control
---------------
Priority    Source   Destination    Service   Action
----------  -------  -----------    --------  -----------
1           user     any            udp 68    deny
2           any      any            svc-icmp  permit
3           any      any            svc-dns   permit
4           any      any            svc-dhcp  permit
5           any      any            svc-natt  permit

captiveportal
---------------
Priority   Source   Destination     Service          Action
---------  -------  -------------   ----------       ----------
1          user     controller      svc-https        dst-nat 8081
2          user     any             svc-http         dst-nat 8080
3          user     any             svc-https        dst-nat 8081
4          user     any             svc-http-proxy1  dst-nat 8088
5          user     any             svc-http-proxy2  dst-nat 8088
6          user     any             svc-http-proxy3  dst-nat 8088
```

Exhibit 2

```
vpnlogon
----------
Priority    Source    Destinition    Service    Action
----------  -------   ------------   ---------  ---------
1           user      any            svc-ike    permit
2           user      any            svc-esp    permit
3           any       any            svc-12tp   permit
4           any       any            svc-pptp   permit
5           any       any            svc-qre    permit

v6-logon-control
-----------------
Priority   Source    Destination   Service      Action
---------- --------  ------------ --------     --------
1          user      any           udp 6a       deny
2          any       any           svc-v6-icmp  permit
3          any       any           svc-v6-dhcp  permit
4          any       any           svc-dns      permit
```

The exhibit shows truncated output from an Aruba controller. An unauthenticated user assigned to the logon role attempts to start n HTTP session to IP address 172.16.43.170. What happens?

A. The user's traffic is password to the IP address 172.16.43.170 because of the policy statement user any svc-https dst-nat 8081.

B. The user's traffic is password to the IP address 172.16.43.170 because of the policy statement user any svc-http dst-nat 8080.

C. The user's traffic is password to the IP address 172.16.43.170 because of the policy statement user any svc-http-proxy 1 dst-nat 8088.

D. The user will not reach the IP address 172.16.43.170 because of the policy statement user any svc-http dst-nat 8080.

Answer: D