HPE6-A79 Q&As

Aruba Certified Mobility Expert Written Exam

Pass HP HPE6-A79 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/hpe6-a79.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Refer to the exhibits. Exhibit 1

```
(MC2) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP              MAC             Name    Role                  Age(d:h:m) Auth    VPN link  AP name  Roaming  Essid/Bssid/Phy
     Profile  Forward mode Type     Host Name  User Type
---------   ----------             -----   ----                  ---------- ----    -------- -------- -------- ---------------
     -------     ------------       -----  --------   -------
192.168.14.101  xx:xx:xx:xx:xx:xx           guest-guest-logon     00:00:32                  AP1      Wireless  Guest/yy:yy:yy:yy:yy:yy/a-
VHT  Guest   tunnel         Win 10            WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:2/5 Free:0/3 DVN:2 AllocErr:0 FreeErr:0
```

Exhibit 2 Exhibit 3

```
(MC2) [MDC] #show rights guest-guest-logon

Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'guest-guest-logon'
  Up BW:No Limit   Down BW:No Limit
  L2TP Pool = default-l2tp-pool
  PPTP Pool = default-pptp-pool
  Number of users referencing it = 2
  Periodic reauthentication: Disabled
  DPI Classification: Enabled
  Youtube education: Disabled
  Web Content Classification: Enabled
  IP-Classification Enforcement: Enabled
  ACL Number = 98/0
  Openflow: Enabled
  MaxSessions = 65535

  Check CP Profile for Accounting = TRUE
  Captive Portal profile = default
```

```
(MC2) [MDC] #show aaa authentication captive-portal Guest

Captive Portal Authentication Profile "Guest"
---------------------------------------------
Parameter                                   Value
---------                                   -----
Default Role                                guest
Default Guest Role                          guest
Server Group                                Guest
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 failures                 0
Show FQDN                                   Disabled
Authentication Protocol                     PAP
Login page                                  https://cp.mycompany.com/guest/web_login.php
Welcome page                                /auth/welcome.html
Show Welcome Page                           Yes
```

Exhibit 4

```
(MC2) [MDC] #show aaa authentication captive-portal default

Captive Portal Authentication Profile "default"
-----------------------------------------------
Parameter                                       Value
---------                                       -----
Default Role                                    guest
Default Guest Role                              guest
Server Group                                    Guest
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 failures                     0
Show FQDN                                       Disabled
Authentication Protocol                         PAP
Login page                                      /auth/index.html
Welcome page                                    /auth/welcome.html
Show Welcome Page                               Yes
Add switch IP addresses in the redirection URL  Disabled

(MC2) [MDC] #show aaa server-group default

Fail Through: No
Load Balance: No

Auth Servers
------------
Name        Server-Type    trim-FQDN   Match-Type  Match-Op  Match-Str
----        -----------    ---------   ----------  --------  ---------
Internal    Internal       No

Role/VLAN derivation rules
--------------------------
Priority   Attribute   Operation   Operand   Type    Action    Value   Validated
--------   ---------   ---------   -------   ----    ------    -----   ---------
1          role        value-of              String  set role          No
```

A captive portal-based solution is deployed in a Mobility Master (MM) - Mobility Controller (MC) network. A wireless station connects to the network and attempts the authentication process. The outputs are shown in the exhibits. Which names correlate with the authentication and captive portal servers?

A. ClearPass.23 is the authentication server, and cp.mycompany.com is the captive portal server.

B. ClearPass.23 is the authentication server, and MC2 is the captive portal server.

C. Internal database in MC2 is the authentication server, and cp.mycompany.com is the captive portal server.

D. cp.mycompany.com is the authentication server, and ClearPass.23 is the captive portal server.

Correct Answer: A

QUESTION 2

Refer to the exhibit.

```
(MC1) [MDC] #show aaa profile corp_aaa_prof

AAA Profile "corp_aaa_prof"
-----------------------
Parameter                                      Value
---------                                      -----
Initial role                                   logon
MAC Authentication Profile                     N/A
MAC Authentication Default Role                guest
MAC Authentication Server Group                default
802.1X Authentication Profile                  corp-employee_dot1_aut
802.1X Authentication Default Role             guest
802.1X Authentication Server Group             Radius
Download Role from CPPM                        Disabled
Set username from dhcp option 12               Disabled
L2 Authentication Fail Through                 Disabled
Multiple Server Accounting                     Disabled
User idle timeout                              N/A
Max IPv4 for wireless user                     2
RADIUS Accounting Server Group                 N/A
RADIUS Roaming Accounting                      Disabled
RADIUS Interim Accounting                      Disabled
RADIUS Acct-Session-Id In Access-Request       Disabled
XML API server                                 N/A
RFC 3576 server                                N/A
User derivation rules                          N/A
Wired to Wireless Roaming                      Enabled
Reauthenticate wired user on VLAN change       Disabled
Device Type Classification                     Enabled
Enforce DHCP                                   Disabled
PAN Firewall Integration                       Disabled
Open SSID radius accounting                    Disabled
Apply ageout mechanism on bridge mode wireless clients  Disabled
(MC1) [MDC] #
```

A network administrator has created AAA profile for the corporate VAP. In addition to the regular Radius based authentication, the administrator needs to be able to disconnect the users from either of the two servers that are part of the "Radius" server group.

What must the administrator do next in order to achieve this goal?

A. Use the "Radius" server group as the RADIUS Accounting Server Group in the AAA profile.

B. Create two new RFC 3576 servers and assign them as the RFC 3576 servers in the AAA profile.

C. Use the "Radius" server group as both the Accounting Server Group and the RFC 3576 server in the AAA profile.

D. Use the "Radius" server group as the RFC 3576 server in the AAA profile.

Correct Answer: C

Reference: https://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_UG/AP_Config.php

QUESTION 3

A network administrator assists with the migration of a WLAN from a third-party vendor to Aruba in different locations throughout the country. In order to manage the solution from a central point, the network administrator decides to deploy redundant Mobility Masters (MMs) in a datacenter that are reachable through the Internet.

Since not all locations own public IP addresses, the security team is not able to configure strict firewall polices at the datacenter without disrupting some MM to Mobility Controller (MC) communications. They are also concerned about exposing the MMs to unauthorized inbound connection attempts.

What should the network administrator do to ensure the solution is functional and secure?

A. Deploy an MC at the datacenter as a VPN concentrator.

B. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.

C. Block all ports to the MMs except UDP 500 and 4500.

D. Install a PEFV license, and configure firewall policies that protect the MM.

Correct Answer: C

QUESTION 4

A fully functional WLAN is deployed in a campus network using the following script.

```
aaa server-group group-corp
 auth-server radius1

aaa profile aaa-corp
   authentication-dot1x authenticated
   dot1x-server-group group-corp
!
wlan ssid-profile ssid-corp
   essid corp
   opmode wpa2-aes
!
wlan virtual-ap vap-corp
   aaa-profile aaa-corp
   vlan 20
   ssid-profile ssid-corp
!
ap-group building1
   virtual-ap vap-corp
```

Which part of the script can a network administrator re-use to assign a different default role to users when they connect to the same SSID in a second building?

A. server group and ssid profile

B. server group and VAP profile

C. server group, aaa profile, and ssid profile

D. server group and VAP

Correct Answer: A

QUESTION 5

A company with 535 users deploys an Aruba solution with more than 1000 Aruba APs, two 7220 Mobility Controllers, and a single Mobility Master (MM) virtual appliance at the campus server farm. The MCs run a HA Fast failover group in dual mode and operate at 50% AP capacity.

If there is an MM or MC failure, the network administrator must ensure that the network is fully manageable and the MC load does not exceed 80%.

What can the network administrator do to meet these requirements?

A. Place the APs in the same hierarchy level.

B. Create a cluster with AP load balancing.

C. Enable oversubscription in the HA group.

D. Add an MC and an MM in the server farm.

E. Add an MM and enable DC redundancy.

F. Place the APs in two different AP-Groups.

Correct Answer: E