

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : **HPE7-A07**

Title : Aruba Certified Campus
Access Mobility Expert
Written Exam

Version : DEMO

1.Exhibit.

Web Login Editor	
* Name:	acx-guest <small>Enter a name for this web login page.</small>
Page Name:	acx-guest <small>Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".</small>
Description:	 <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	Aruba <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	Controller-initiated — Guest browser performs HTTP form submit <small>Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.</small>
* Address:	securelogin.aruba-training.com <small>Enter the hostname (FQDN) of the vendor's product here. When using Secure Login over HTTPS, this name should match the name of the HTTPS certificate installed on your device.</small>
Secure Login:	Use vendor default <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials <small>In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.</small>

Which would explain this issue?

- 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 in 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.

2.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 "iot-dev" role. However, the customer requires the "iot-prod" role to 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'?

- 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 lldp-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.

- 3.You configured" a bridgedmode SSID with WPA3-Enterprise and EAP-TLS security. When you connect an Active Directory joined client that has valid client certificates. ClearPass shows the following error.

The screenshot shows a 'Request Details' window with the following information:

Summary	Input	Output	Alerts
Error Code:	201		
Error Category:	Authentication failure		
Error Message:	User not found		
Alerts for this Request			
RADIUS	ACX-AD - dc01.aruba-training.com: User not found.		
	EAP-TLS: Authentication failure, unknown user		

At the bottom of the window, there are navigation buttons: 'Showing 1 of 1-4 records', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

What is needed to resolve this issue?

- A. Enable authorization in your Authentication Method.
- B. Recreate the SSID in tunneled mode.
- C. Modify your ACX-AD authentication source to include the UPN in the search.
- D. Configure ClearPass to trust the client certificate.

Answer: C

Explanation:

The error message "User not found" indicates that the authentication source, in this case, Active Directory (AD), is not able to locate the user account based on the current search parameters. This often occurs when the User Principal Name (UPN) that the client is using to authenticate is not included in the search parameters of the AD authentication source within ClearPass. By modifying the AD authentication source to include the UPN in the search, ClearPass will be able to correctly locate the user account and proceed with the authentication using the valid client certificates.

- 4.Exhibit.



```
R1(config-if)# show run cur
interface 1/1/1
no shutdown
mtu 9100
ip address 10.255.1.0/31
ip ospf 1 area 0.0.0.0
ip ospf cost 100
exit
```

```
R2(config-if)# show run cur
interface 1/1/1
no shutdown
mtu 9100
ip address 10.255.1.1/31
ip mtu 9100
ip ospf 1 area 0.0.0.0
exit
```

An engineer has applied the above configuration to R1 and R2. However, the routers' OSPF adjacency never progresses past the "EXSTART-DR" state as shown below.

```
R2(config)# show ip ospf neighbors
VRF : default                               Process : 1
-----
Total Number of Neighbors : 1
Neighbor ID    Priority  State           Nbr Address      Interface
-----
10.255.1.0    1        EXSTART/DR      10.255.1.0       1/1/1
```

Which configuration action on either router will allow R1 and R2 to progress past the "EXSTART/DR" state?

- A. Change R1 and R2 to a network type of point-to-point.
- B. Remove the layer 3 MTU configuration.
- C. Ensure the OSPF process is not configured with passive-interface default.
- D. Change the IP address and mask applied to interface 1/1/1.

Answer: A

Explanation:

In OSPF, the "EXSTART/DR" state indicates that the routers are trying to establish an adjacency but are unable to progress. This can happen if the OSPF network type is incorrectly configured for the type of connection between the routers. Given that R1 and R2 are connected via a point-to-point link (as suggested by the /31 subnet), setting the network type to point-to-point on both routers will remove the need for DR/BDR election, which is unnecessary on a point-to-point link, and allow OSPF to progress past the "EXSTART" state and form a full adjacency.

5.Exhibit.

```
IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
    Timestamp: 6455669452801
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x1411
  v Tagged parameters (249 bytes)
    > Tag: SSID parameter set: "hpe"
    > Tag: Supported Rates 12(B), 18(B), 24(B), 36(B), 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 36
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    > Tag: TPC Report Transmit Power: 18, Link Margin: 0
    > Tag: RSN Information
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: AP Channel Report: Operating Class 1, Channel List : 36, 40, 44, 48,
    > Tag: AP Channel Report: Operating Class 3, Channel List : 149, 153, 157, 161,
    > Tag: AP Channel Report: Operating Class 5, Channel List : 165,
    > Tag: BSS Available Admission Capacity
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    > Tag: Vendor Specific: Aruba, a Hewlett Packard Enterprise Company: Unknown (Data: 0812)
```

Which statement is true?

- A. The SSID supports HR-DSSS data rates
- B. The SSID is supports 6 GHz clients.
- C. The SSID supports 802 11ax clients.
- D. The SSID supports 802 11ac clients.

Answer: C

Explanation:

The exhibit shows that the SSID supports 802.11ax clients, which is indicated by the presence of HT (High Throughput) information, VHT (Very High Throughput) capabilities, and HE (High-Efficiency) operation, which are all features associated with 802.11ax, also known as Wi-Fi 6.