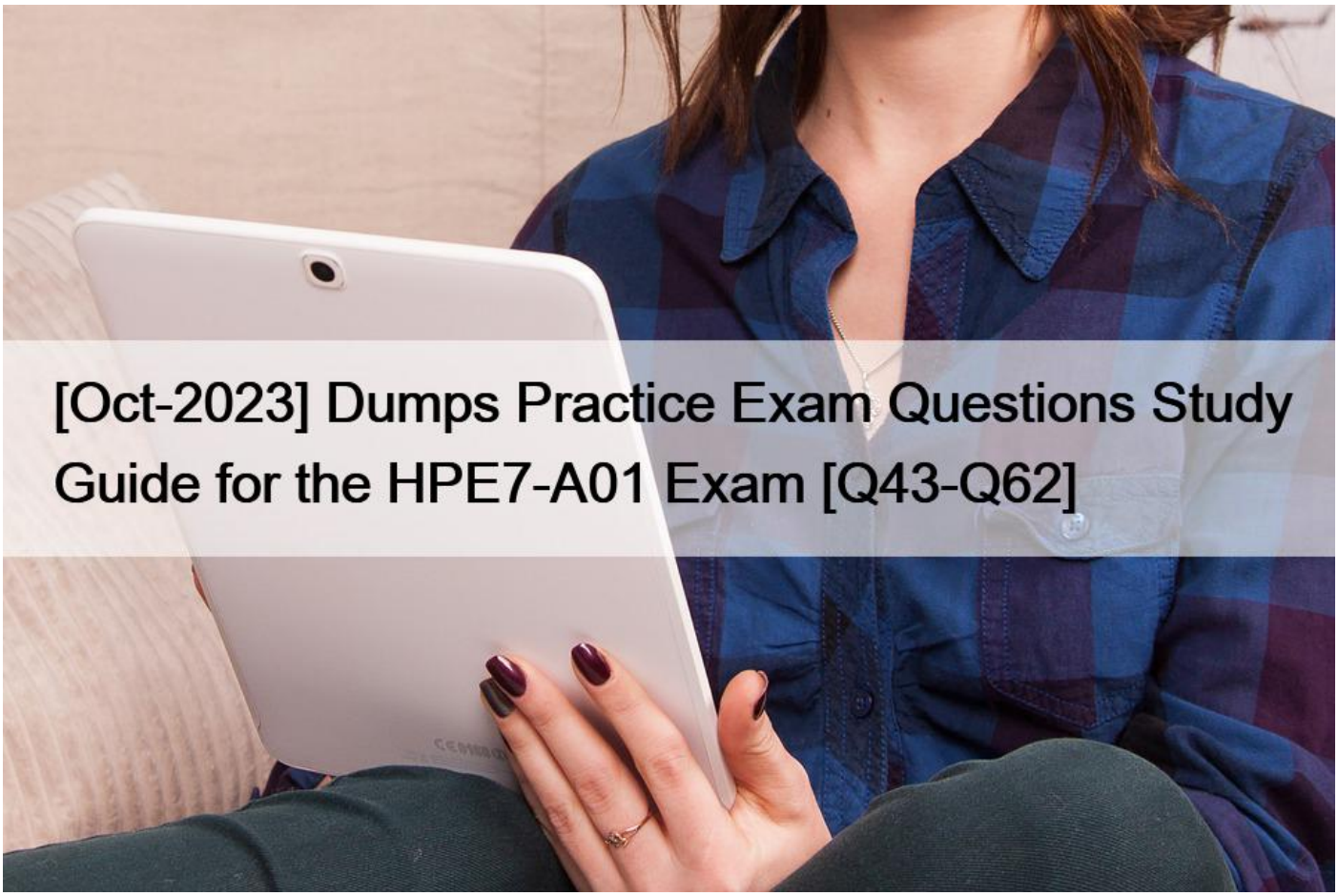
[Oct-2023 Dumps Practice Exam Questions Study Guide for the HPE7-A01 Exam [Q43-Q62



[Oct-2023] Dumps Practice Exam Questions Study Guide for the HPE7-A01 Exam
HPE7-A01 Dumps with Practice Exam Questions Answers

HP HPE7-A01 certification exam is a valuable credential for IT professionals who wish to enhance their skills and knowledge in Aruba wireless networking solutions. Aruba Certified Campus Access Professional Exam certification not only validates the candidate's knowledge and skills in designing and implementing Aruba wireless networks but also demonstrates their commitment to professional development and career advancement.

NO.43 What is the order of operations tor Key Management service for a wireless client roaming from AP1 to AP2?

Explanation

https://www.arubanetworks.com/techdocs/Instant_85_WebHelp/Content/instant-ug/wlan-ssid-conf/conf-fast-roa

NO.44 Your customer has asked you to assign a switch management role for a new user The customer requires the user role to only have Web Ul access to the System > Log page and only have access to the GET method for REST API for the /logs/event resource Which default AOS-CX user role meets these requirements?

* administrators
* auditors
* sysops
* operators

The auditors role is the default AOS-CX user role that meets the requirements of having Web UI access to the System > Log page and having access to the GET method for REST API for the /logs/event resource. The auditors role has a level of 1 and allows read-only access to most commands except those related to security or passwords. It also allows access to the Web UI and REST API with limited permissions. The other options are incorrect because they either have higher levels of access or do not allow access to the Web UI or REST API. Reference:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch01.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch04.html

NO.45 The administrator notices that wired guest users that have exceeded their bandwidth limit are not being disconnected Access Tracker in ClearPass indicates a disconnect CoA message is being sent to the AOS-CX switch.

An administrator has performed the following configuration

```
Access1(config)# ip dns host cppm.arubatraining.com 10.254.1.23 vrf mgmt
Access1(config)# radius-server host cppm.arubatraining.com key plaintext aruba123 vrf mgmt
Access1(config)# aaa group server radius cppm
Access1(config-sg)# server cppm.arubatraining.com vrf mgmt
Access1(config-sg)# exit
Access1(config)# aaa accounting port-access start-stop interim 5 group cppm
Access1(config)# radius dyn-authorization client cppm.arubatraining.com secret-key plaintext aruba1
Access1(config)# radius dyn-authorization enable
```


What is the most likely cause of this issue?
* Change of Authorization has not been globally enabled on the switch
* The SSL certificate for CPPM has not been added as a trust point on the switch
* There is a mismatch between the RADIUS secret on the switch and CPPM.
* There is a time difference between the switch and the ClearPass Policy Manager

Explanation

Change of Authorization (CoA) is a feature that allows ClearPass Policy Manager (CPPM) to send messages to network devices such as switches to change the authorization state of a user session. CoA requires that both CPPM and the network device support this feature and have it enabled. For AOS-CX switches, CoA must be globally enabled using the command radius-server coa enable. If CoA is not enabled on the switch, the disconnect CoA message from CPPM will be ignored and the user session will not be terminated. References:

https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/index.htm#CPPM_UserGuide/Admin/C

https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-9B8F6E8F-9C7A-4F0D-AE7B-9D8E

NO.46 In an ArubaOS 10 architecture using an AP and a gateway, what happens when a client attempts to join the network and the WLAN is configured with OWE?
* Authentication information is not exchanged
* The Gateway will not respond.
* No encryption is applied.
* RADIUS protocol is utilized.

Explanation

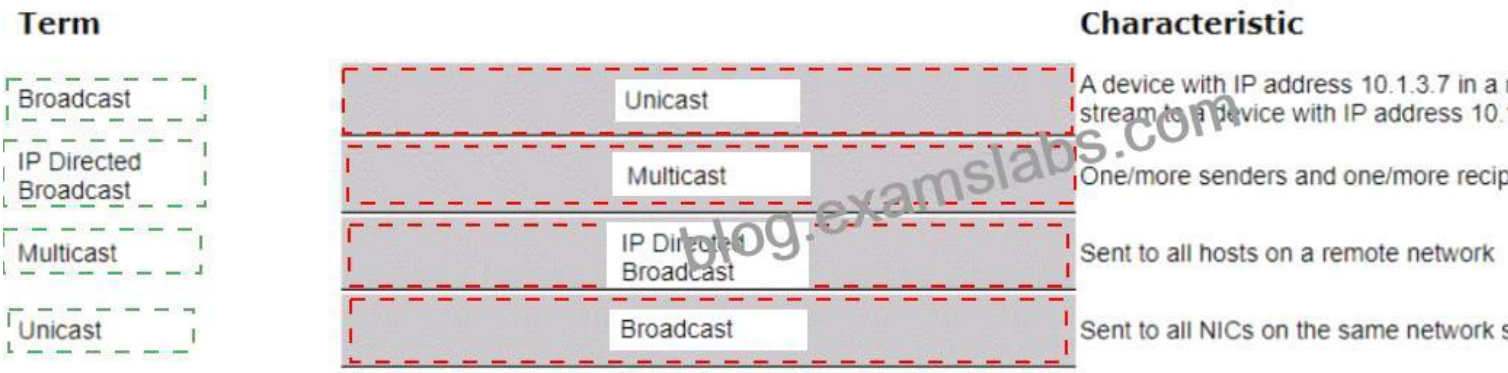
This is the correct statement about what happens when a client attempts to join the network and the WLAN is configured with OWE (Opportunistic Wireless Encryption). OWE is a standard that provides encryption for open networks without requiring any

authentication or credentials from the client or the network. OWE uses a Diffie-Hellman key exchange mechanism to establish a secure session between the client and the AP without exchanging any authentication information. The other options are incorrect because they either describe scenarios that require authentication or encryption methods that are not used by OWE. References:

https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf

https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

NO.47 Match the terms below to their characteristics (Options may be used more than once or not at all.)



Explanation

a) A device with IP address 10.1.3.7 in a network wants to send the traffic stream to a device with IP address

10.13.4.2 in the other network -> Unicast

b) One/more senders and one/more recipients participate in data transfer traffic -> Multicast c) Sent to all hosts on a remote network -> IP Directed Broadcast d) Sent to all NICs on the same network segment as the source NIC -> Broadcast References: 1 https://www.thestudygenius.com/unicast-broadcast-multicast/ The terms broadcast, IP directed broadcast, multicast, and unicast are different types of communication or data transmission over a network. They differ in how many devices are involved in the

communication and how they address the messages. The following table summarizes the characteristics of each term1:

A screenshot of a computer Description automatically generated with medium confidence

Term	Definition	Example
Broadcast	One-to-all communication, where data is sent to every device on the network	A device with IP address 10.1.3.7 sends a DHCP request to 255.255.255.255
IP Directed Broadcast	One-to-all communication, where data is sent to all hosts on a remote network	A device with IP address 10.1.3.7 sends a ping request to 10.13.4.255
Multicast	One-to-many or many-to-many communication, where data is sent to a group of devices that have joined a multicast group	A device with IP address 10.1.3.7 sends a video stream to 239.0.0.1
Unicast	One-to-one communication, where data is sent to only one device	A device with IP address 10.1.3.7 sends an email to a device with IP address 10.13.4.2

NO.48 You must ensure the HPEAruba network you are configuring for a client is capable of plug-and-play provisioning of access points. What enables this capability?
* UCC Service
* LLDP-MED
* SRTP
* CSMA
Explanation

The capability that enables plug-and-play provisioning of access points in an HPE Aruba network is the UCC Service. The UCC Service is a cloud-based service that allows the access points to automatically discover and connect to the Aruba Central management platform without any manual intervention. The UCC Service also provides zero-touch configuration, firmware updates, and monitoring for the access points1.

The other options are incorrect because:

* B. LLDP-MED: LLDP-MED is a protocol that enhances the interoperability between network devices

* and IP phones. It does not enable plug-and-play provisioning of access points2.

* C. SRTP: SRTP is a protocol that provides encryption and authentication for voice and video traffic. It does not enable plug-and-play provisioning of access points3.

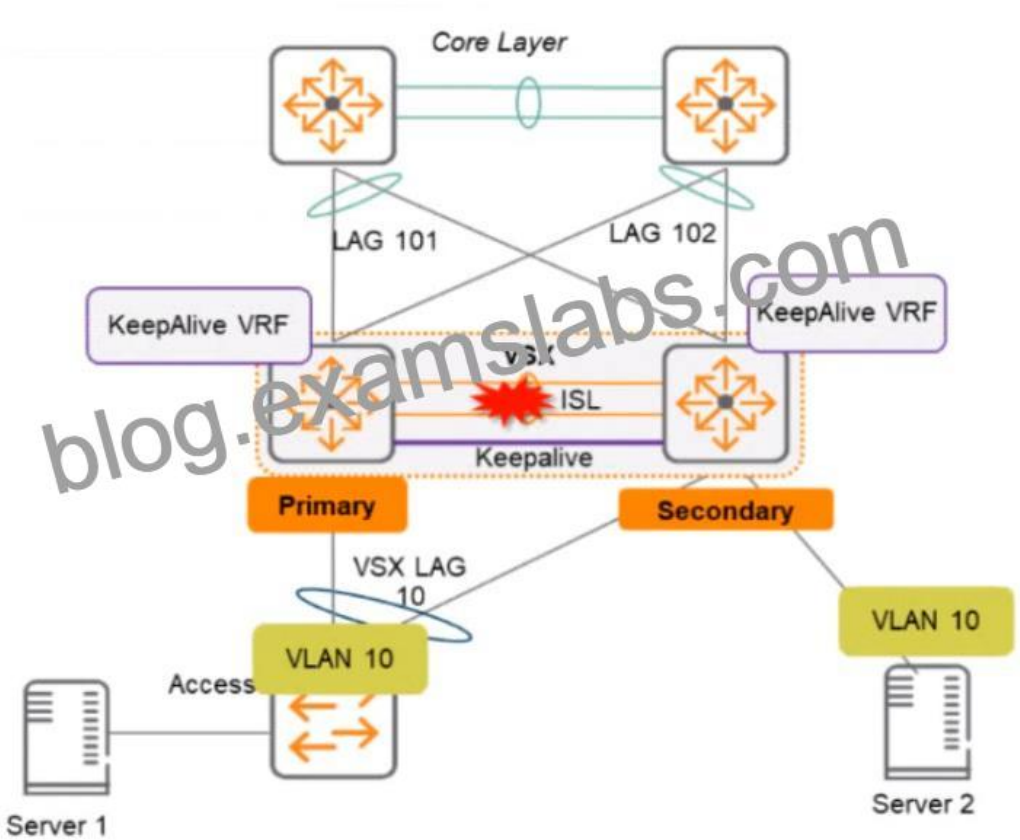
* D. CSMA: CSMA is a protocol that regulates how devices share a common medium, such as a wireless channel. It does not enable plug-and-play provisioning of access points.

NO.49 You are helping an onsite network technician bring up an Aruba 9004 gateway with ZTP for a branch office The technician was to plug in any port for the ZTP process to start Thirty minutes after the gateway was plugged in new users started to complain they were no longer able to get to the internet. One user who reported the issue stated their IP address is 172.16 0.81 However, the branch office network is supposed to be on 10.231 81.0/24.

What should the technician do to alleviate the issue and get the ZTP process started correctly?
* Turn off the DHCP scope on the gateway, and set DNS correctly on the gateway to reach Aruba Activate
* Move the cable on the gateway from port G0/0V1 tc port G0 0.0
* Move the cable on the gateway to G0/0/1. and add the device’s MAC and Serial number in Central
* Factory default and reboot the gateway to restart the process.

Aruba 9004 gateway supports ZTP on port G0/0/0 by default1. If the gateway is connected to a different port, such as G0/0/V1, it will not be able to communicate with Aruba Activate and Aruba Central, which are required for ZTP2. Moreover, port G0/0/V1 is configured as a DHCP server by default, which can cause IP address conflicts with the existing network3. Therefore, the technician should move the cable on the gateway to port G0/0/0, which will allow the gateway to obtain an IP address from the network DHCP server and start the ZTP process. The other options are not correct because they will not solve the issue or enable ZTP. For example, option D will not work because factory defaulting and rebooting the gateway will not change the port configuration or behavior3.

NO.50 Two AOS-CX switches are configured with VSX at the the Access-Aggregation layer where servers attach to them An SVI interface is configured for VLAN 10 and serves as the default gateway for VLAN 10. The ISL link between the switches fails, but the keepalive interface functions. Active gateway has been configured on the VSX switches.



What is correct about access from the servers to the Core? (Select two.)
* Server 1 can access the core layer via the keepalrve link
* Server 2 can access the core layer via the keepalive link

* Server 2 cannot access the core layer.
* Server 1 can access the core layer via both uplinks
* Server 1 and Server 2 can communicate with each other via the core layer
* Server 1 can access the core layer on only one uplink

These are the correct statements about access from the servers to the Core when the ISL link between the switches fails, but the keepalive interface functions. Server 1 can access the core layer via both uplinks because it is connected to VSX-A, which is still active for VLAN 10. Server 2 can also access the core layer via its uplink to VSX-B, which is still active for VLAN 10 because of Active Gateway feature. Server 1 and Server 2 can communicate with each other via the core layer because they are in the same VLAN and subnet, and their traffic can be routed through the core switches. The other statements are incorrect because they either describe scenarios that are not possible or not relevant to the question. Reference: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-

NO.51 For the Aruba CX 6400 switch, what does virtual output queueing (VOQ) implement that is different from most typical campus switches?

* large ingress packet buffers
* large egress packet buffers
* per port ASICs
* VSX

Explanation

The Aruba CX 6400 switch is a modular switch that supports high-performance and high-density Ethernet switching for campus and data center networks. One of the features that distinguishes the Aruba CX 6400 switch from most typical campus switches is virtual output queueing (VOQ). VOQ is a technique that implements large ingress packet buffers on each port to prevent head-of-line blocking and packet loss due to congestion2. VOQ allows each port to have multiple queues for different output ports and prioritize packets based on their destination and QoS class2. VOQ enables the Aruba CX 6400 switch to achieve high throughput and low latency for various traffic types and scenarios. References: 2

https://www.arubanetworks.com/assets/ds/DS_CX6400Series.pdf

NO.52 For the Aruba CX 6400 switch, what does virtual output queueing (VOQ) implement that is different from most typical campus switches?

* large ingress packet buffers
* large egress packet buffers
* per port ASICs
* VSX

The Aruba CX 6400 switch is a modular switch that supports high-performance and high-density Ethernet switching for campus and data center networks. One of the features that distinguishes the Aruba CX 6400 switch from most typical campus switches is virtual output queueing (VOQ). VOQ is a technique that implements large ingress packet buffers on each port to prevent head-of-line blocking and packet loss due to congestion2. VOQ allows each port to have multiple queues for different output ports and prioritize packets based on their destination and QoS class2. VOQ enables the Aruba CX 6400 switch to achieve high throughput and low latency for various traffic types and scenarios. Reference: 2 https://www.arubanetworks.com/assets/ds/DS_CX6400Series.pdf

NO.53 A company recently deployed new Aruba Access Points at different branch offices Wireless 802.1X authentication will be against a RADIUS server in the cloud. The security team is concerned that the traffic between the AP and the RADIUS server will be exposed.

What is the appropriate solution for this scenario?

* Enable EAP-TLS on all wireless devices
* Configure RadSec on the AP and Aruba Central.
* Enable EAP-TTLS on all wireless devices.

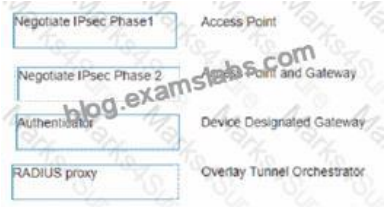
* Configure RadSec on the AP and the RADIUS server

Explanation

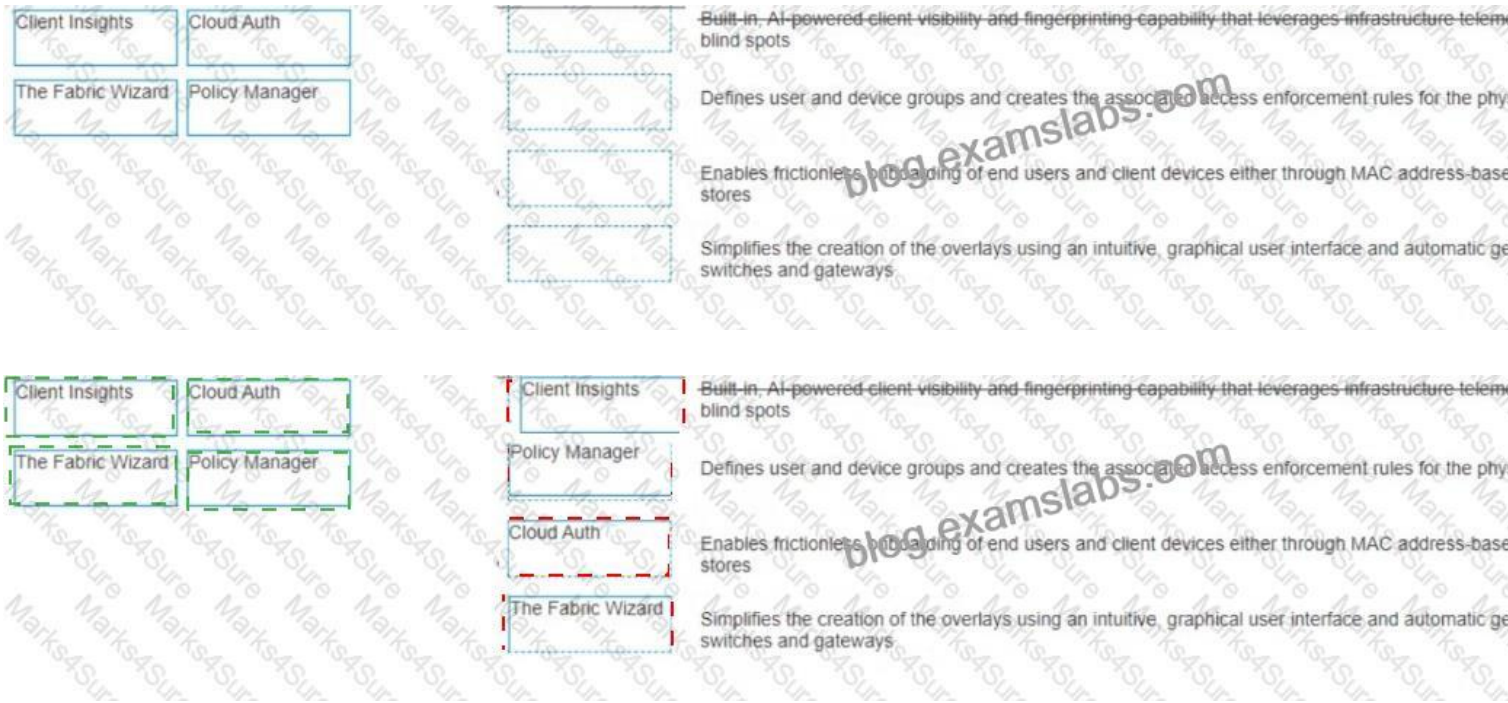
This is the appropriate solution for this scenario where wireless 802.1X authentication will be against a RADIUS server in the cloud and the security team is concerned that the traffic between the AP and the RADIUS server will be exposed. RadSec, also known as RADIUS over TLS, is a protocol that provides encryption and authentication for RADIUS traffic over TCP and TLS. RadSec can be configured on both the AP and the RADIUS server to establish a secure tunnel for exchanging RADIUS packets. The other options are incorrect because they either do not provide encryption or authentication for RADIUS traffic or do not involve RadSec.
References: https://www.securew2.com/blog/what-is-radsec/

https://www.cloudradius.com/radsec-vs-radius/

NO.54 Match the topics of an AOS10 Tunneled mode setup between an AP and a Gateway. (Options may be used more than once or not at all.)



NO.55 Match the solution components of NetConductor (Options may be used more than once or not at all.)



Explanation

Client Insights matches with Built in , AI powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML based classification models to eliminate network bling spots Client Insights is a solution component of NetConductor that provides built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots. Client Insights uses machine learning to automatically detect, identify, and classify devices on the network, such as IoT devices, BYOD devices, or rogue devices. Client Insights also provides behavioral analytics and anomaly detection to monitor device performance and security posture.

Client Insights helps network administrators gain visibility into the device landscape, enforce granular access policies, and troubleshoot issues faster. References:

https://www.arubanetworks.com/products/network-management-operations/central/netconductor/

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

Cloud Auth matches with Enables fictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores Cloud Auth is a solution component of NetConductor that enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores. Cloud Auth is a cloud-native network access control (NAC) solution that is delivered via Aruba Central. Cloud Auth allows network administrators to define user and device groups, assign roles and policies, and enforce access control across wired and wireless networks. Cloud Auth supports MAC authentication for devices that do not support 802.1X, as well as integrations with cloud identity providers such as Azure AD, Google Workspace, Okta, etc. References:

https://www.arubanetworks.com/products/network-management-operations/central/netconductor/

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

The Fabric Wizard matches with Simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways The Fabric Wizard is a solution component of NetConductor that simplifies the creation of the overlays using an intuitive graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways. The Fabric Wizard is a tool that allows network administrators to design, deploy, and manage overlay networks using VXLAN and EVPN protocols. The Fabric Wizard provides a graphical representation of the network topology, devices, and links, and allows users to drag and drop virtual components such as VRFs, VLANs, and subnets. The Fabric Wizard also generates the configuration commands for each device based on the user input and pushes them to the switches and gateways via Aruba Central. References:

https://www.arubanetworks.com/products/network-management-operations/central/netconductor/

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

Policy Manager matches with Defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network Policy Manager is a solution component of NetConductor that defines user and device groups and creates the associated traffic routing and access enforcement rules for the physical network. Policy Manager is a tool that allows network administrators to create and manage network policies based on user and device identities, roles, and contexts. Policy Manager uses Group Policy Identifier (GPID) to carry policy information in traffic for in-line enforcement. Policy Manager also integrates with Cloud Auth, ClearPass, or third-party solutions to provide flexible network access control. References:

https://www.arubanetworks.com/products/network-management-operations/central/netconductor/

https://www.arubanetworks.com/assets/wp/WP_NetConductor.pdf

NO.56 Which method is used to onboard a new UXI in an existing environment with 802 1X authentication? (The sensor has no cellular connection)
* Use the UXI app on your smartphone and connect the UXI via Bluetooth
* Use the Aruba installer app on your smartphone to scan the barcode
* Connect the new UXI from an already installed one and adjust the initial configuration.
* Use the CLI via the serial cable and adjust the initial configuration.

To onboard a new UXI in an existing environment with 802.1X authentication, you need to use the UXI app on your smartphone and connect the UXI via Bluetooth. The UXI app allows you to scan the QR code on the UXI sensor and configure its network settings, such as SSID, password, IP address, etc. The Bluetooth connection allows you to communicate with the UXI sensor without requiring any network access or cellular connection. The other options are incorrect because they either do not use the UXI app or do not use Bluetooth. Reference:
https://www.arubanetworks.com/products/network-management-operations/analytics-monitoring/user-experience-insight-sensors/
https://help.centralon-prem.arubanetworks.com/2.5.4/documentation/online_help/content/nms-on-prem/aos-cx/get-started/uxi-sensor.htm

NO.57 A network engineer recently identified that a wired device connected to a CX Switch is misbehaving on the network To address this issue, a new ClearPass policy has been put in place to prevent this device from connecting to the network again.

Which steps need to be implemented to allow ClearPass to perform a CoA and change the access for this wired device? (Select two.)
* Configure dynamic authorization on the switch.
* Bounce the switchport
* Use Dynamic Segmentation.
* Confirm that NTP is configured on the switch and ClearPass
* Configure dynamic authorization on the switchport

Explanation

CoA (Change of Authorization) is a feature that allows ClearPass to dynamically change the authorization and access privileges of a device after it has been authenticated1. CoA uses RADIUS messages to communicate with the network device and instruct it to perform an action, such as reauthenticating the device, applying a new VLAN or user role, or disconnecting the device2.

To enable CoA on a CX switch, the network engineer needs to configure dynamic authorization on the switch, which is a global command that allows the switch to accept RADIUS messages from ClearPass and execute the requested actions3. The network engineer also needs to specify the IP address and shared secret of ClearPass as a dynamic authorization client on the switch3.

To trigger CoA for a specific wired device, the network engineer needs to bounce the switchport, which is an action that temporarily disables and re-enables the port where the device is connected. This forces the device to reauthenticate and receive the new policy from ClearPass. Bouncing the switchport can be done manually by using the interface shutdown and no shutdown commands, or automatically by using ClearPass as a CoA server and sending a RADIUS message with the Port-Bounce-Host AVP (Attribute-Value Pair).

NO.58 A customer is using a legacy application that communicates at layer-2. The customer would like to keep this application working to a remote site connected via layer-3 All legacy devices are connected to a dedicated Aruba CX 6200 switch at each site.

What technology on the Aruba CX 6200 could be used to meet this requirement?
* Inclusive Multicast Ethernet Tag (IMET)
* Ethernet over IP (EolP)
* Generic Routing Encapsulation (GRE)
* Static VXLAN

Explanation

VXLAN is a technology that can be used to meet the requirement of using a legacy application that communicates at layer-2 across a layer-3 network. Static VXLAN is a feature that allows the creation of layer-2 overlay networks over a layer-3 underlay network using VXLAN tunnels. Static VXLAN does not require any control plane protocol or VTEP discovery mechanism, and can be configured manually on the Aruba CX 6200 switches. The other options are incorrect because they either do not support layer-2 communication over layer-3 network or are not supported by Aruba CX 6200 switches. References:

https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html

NO.59 A company deployed Dynamic Segmentation with their CX switches and Gateways After performing a security audit on their network, they discovered that the tunnels built between the CX switch and the Aruba Gateway are not encrypted. The company is concerned that bad actors could try to insert spoofed messages on the Gateway to disrupt communications or obtain information about the network.

Which action must the administrator perform to address this situation?
* Enable Secure Mode Enhanced
* Enable Enhanced security
* Enable Enhanced PAPI security
* Enable GRE security

Explanation

To address the situation of unencrypted tunnels between the CX switch and the Aruba Gateway, the administrator must enable Enhanced security on both devices. Enhanced security is a feature that provides encryption and authentication for GRE tunnels

between CX switches and Aruba Gateways using IPSec.

Enhanced security can be enabled globally or per tunnel on both devices using CLI commands or Web UI options. The other options are incorrect because they either do not provide encryption or authentication for GRE tunnels or do not exist as features. References:

https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html

https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

NO.60 A customer is using Aruba Cloud Guest, but visitors keep complaining that the captive portal page keeps coming up after devices go to sleep Which solution should be enabled to deal with this issue?
* MAC Caching under the splash page
* MAC Caching under the user-role
* Wireless Caching under the splash page
* MAC Caching under the WLAN

Explanation

This is the correct solution to deal with the issue where visitors keep complaining that the captive portal page keeps coming up after devices go to sleep. MAC Caching is a feature that allows an Aruba Access Point to bypass authentication for devices that have already been authenticated by a captive portal. MAC Caching can be enabled under the WLAN settings in Aruba Cloud Guest by selecting the MAC Caching checkbox and specifying the MAC Caching duration. The other options are incorrect because they either do not exist or do not apply to Aruba Cloud Guest. References:

https://www.arubanetworks.com/techdocs/CloudGuest/Content/Topics/MAC_Caching.htm

https://www.arubanetworks.com/techdocs/CloudGuest/Content/Topics/WLAN.htm

NO.61 With the Aruba CX 6200 24G switch with uplinks or 1/1/25 and 1/1/26, how do you protect client ports from forming layer-2 loops?
* int 1/1/1-1/1/24, loop-protect
* int 1/1/1-1/1/28. loop-protect
* int 1/1/1-1/1/28. loop-guard
* int 1/1/1-1/1/24. loop-guard

The command loop-protect enables loop protection on each layer 2 interface (port, LAG, or VLAN) for which loop protection is needed. Loop protection can find loops in untagged layer 2 links, as well as on tagged VLANs.

NO.62 Due to a shipping error, five (5) Aruba AP-515S and one (1) Aruba CX 6300 were sent directly to your new branch office You have configured a new group persona for the new branch office devices in Central, but you do not know their MAC addresses or serial numbers The office manager is instructed via text message on their smartphone to onboard all the new hardware into Aruba Central What application must the office manager use on their phone to complete this task?
* Aruba Onboard App
* Aruba Central App
* Aruba CX Mobile App
* Aruba installer App

Aruba Installer App is a mobile app that simplifies site installations and enables network connectivity for Aruba devices. The app allows the user to scan the barcode of the device and add it to the network using Aruba Central. The app also automates importing Aruba devices into Aruba NetEdit for intelligent configuration management and continuous conformance validation

Free Aruba Certified Professional HPE7-A01 Exam Question:
https://www.examslabs.com/HP/Aruba-Certified-Professional/best-HPE7-A01-exam-dumps.html]