Number: HPE6-A84
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: HPE6-A84

Exam Name: Aruba Certified Network Security Expert Written

Exam A

QUESTION 1
Refer to the exhibit.

*Lab NIC

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
7124	1745.313106	10.1.7.100	10.1.26.151	TLSv1.2	1389	Application Data, Application Data
7125	1745.313138	10.1.26.151	10.1.7.100	TCP	54	21379 → 443 [ACK] Seq=59293 Ack=555740 Win=2102272 Len=0
7126	1745.335486	10.1.26.151	10.1.7.100	TCP	54	21411 → 443 [ACK] Seq=22221 Ack=47130 Win=2101248 Len=0
7127	1752.091170	94:60:d5:bf:36:40	Broadcast	ARP	60	Gratuitous ARP for 10.1.26.1 (Request)
7128	1753.261660	10.1.26.151	10.254.1.21	DNS	84	Standard query 0x0001 PTR 21.1.254.10.in-addr.arpa
7129	1753.262268	10.254.1.21	10.1.26.151	DNS	126	Standard query response 0x0001 PTR 21.1.254.10.in-addr.arpa PTR TrainingLab-AD.acnsxtest.com
7130	1753.263452	10.1.26.151	10.254.1.21	DNS	98	Standard query 0x0002 A QW55IG9yZGVycz8.djdkduep62kz4nzx.onion
7131	1754.747844	10.1.26.150	224.0.0.251	MDNS	83	Standard query 0x0000 PTR _anywhereusb._tcp.local, "QM" question
7132	1755.275570	10.1.26.151	10.254.1.21	DNS	98	Standard query 0x0003 AAAA QW55IG9yZGVycz8.djdkduep62kz4nzx.onion
7133	1755.303070	10.1.26.151	10.1.7.100	TLSv1.2	920	Application Data
7134	1755.303255	10.1.7.100	10.1.26.151	TCP	60	443 → 21379 [ACK] Seq=555740 Ack=60159 Win=63360 Len=0
7135	1755.318864	10.1.26.151	10.1.7.100	TLSv1.2	882	Application Data
7136	1755.323597	10.1.7.100	10.1.26.151	TLSv1.2	604	Application Data
7137	1755.343521	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=555740 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7138	1755.343521	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=557200 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7139	1755.343573	10.1.26.151	10.1.7.100	TCP	54	21379 → 443 [ACK] Seq=60159 Ack=558660 Win=2102272 Len=0
7140	1755.343650	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=558660 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7141	1755.343650	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=560120 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7142	1755.343650	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [PSH, ACK] Seq=561580 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7143	1755.343650	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=563040 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7144	1755.343650	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=564500 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7145	1755.343650	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=565960 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7146	1755.343650	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=567420 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7147	1755.343650	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [PSH, ACK] Seq=568880 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7148	1755.343704	10.1.26.151	10.1.7.100	TCP	54	21379 → 443 [ACK] Seq=60159 Ack=570340 Win=2102272 Len=0
7149	1755.343749	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=570340 Ack=60159 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7150	1755.343784	10.1.7.100	10.1.26.151	TLSv1.2	1389	Application Data, Application Data
7151	1755.343797	10.1.26.151	10.1.7.100	TCP	54	21379 → 443 [ACK] Seq=60159 Ack=573135 Win=2102272 Len=0
7152	1755.368072	10.1.26.151	10.1.7.100	TCP	54	21411 → 443 [ACK] Seq=23049 Ack=47680 Win=2102272 Len=0
7153	1755.763334	10.1.26.150	224.0.0.251	MDNS	83	Standard query 0x0000 PTR _anywhereusb._tcp.local, "QM" question
7154	1760.159146	10.1.26.151	10.1.7.100	TLSv1.2	868	Application Data
7155	1760.159402	10.1.7.100	10.1.26.151	TCP	60	443 → 21379 [ACK] Seq=573135 Ack=60973 Win=63360 Len=0
7156	1760.162772	10.1.7.100	10.1.26.151	TLSv1.2	599	Application Data
7157	1760.165496	10.1.26.151	10.1.7.100	TLSv1.2	888	Application Data
7158	1760.165720	10.1.7.100	10.1.26.151	TCP	60	443 → 21379 [ACK] Seq=573680 Ack=61807 Win=63360 Len=0
7159	1760.171166	10.1.7.100	10.1.26.151	TLSv1.2	852	Application Data
7160	1760.212643	10.1.26.151	10.1.7.100	TCP	54	21379 → 443 [ACK] Seq=61807 Ack=574478 Win=2100992 Len=0
7161	1761.449829	10.254.1.21	10.1.26.151	DNS	146	Standard query response 0x0002 A QW55IG9yZGVycz8.djdkduep62kz4nzx.onion CNAME cnVuIGEgc2NhbiBhdCAxMC4xLjAuMCBxNg
7162	1761.449879	10.1.26.151	10.254.1.21	ICMP	174	Destination unreachable (Port unreachable)
7163	1765.337103	10.1.26.151	10.1.7.100	TLSv1.2	920	Application Data
7164	1765.349819	10.1.26.151	10.1.7.100	TLSv1.2	882	Application Data
7165	1765.355148	10.1.7.100	10.1.26.151	TLSv1.2	604	Application Data
7166	1765.379168	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=574478 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7167	1765.379168	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [PSH, ACK] Seq=575938 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7168	1765.379168	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=577398 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7169	1765.379168	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [PSH, ACK] Seq=578858 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7170	1765.379168	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=580318 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7171	1765.379168	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [PSH, ACK] Seq=581778 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
7172	1765.379235	10.1.26.151	10.1.7.100	TCP	54	21379 → 443 [ACK] Seq=62673 Ack=583238 Win=2102272 Len=0
7173	1765.379296	10.1.7.100	10.1.26.151	TCP	1514	443 → 21379 [ACK] Seq=583238 Ack=62673 Win=64128 Len=1460 [TCP segment of a reassembled PDU]

Which security issue is possibly indicated by this traffic capture?

A. An attempt at a DoS attack by a device acting as an unauthorized DNS server
B. A port scan being run on the 10.1.7.0/24 subnet
C. A command and control channel established with DNS tunneling
D. An ARP poisoning or man-in-the-middle attempt by the device at 94:60:d5:bf:36:40

Correct Answer: C
Section:
Explanation:
DNS tunneling is a technique that abuses the DNS protocol to tunnel data or commands between a compromised host and an attacker's server. DNS tunneling can be used to establish a command and control channel, which allows the attacker to remotely control the malware or exfiltrate data from the infected host1 The traffic capture in the exhibit shows some signs of DNS tunneling. The source IP address is 10.1.7.2, which is likely an internal host behind a firewall. The destination IP address is 8.8.8.8, which is a public DNS resolver. The DNS queries are for subdomains of badsite.com, which is likely a malicious domain registered by the attacker. The subdomains have long and random names, such as 0x2a0x2a0x2a0x2a0x2a0x2a0x2a0x2a0x2a.badsite.com, which could be used to encode data or commands. The DNS responses have large sizes, such as 512 bytes, which could be used to carry data or commands back to the host2

QUESTION 2
You are working with a developer to design a custom NAE script for a customer. You are helping the developer find the correct REST API resource to monitor.
Refer to the exhibit below.

What should you do before proceeding?

A. Go to the v1 API documentation interface instead of the v10.10 interface.
B. Use your Aruba passport account and collect a token to use when trying out API calls.
C. Enable the switch to listen to REST API calls on the default VRF.
D. Make sure that your browser is set up to store authentication tokens and cookies.

Correct Answer: B
Section:
Explanation:
The exhibit shows the ArubaOS-CX REST API documentation interface, which allows you to explore the available resources and try out the API calls using the "Try it out" button. However, before you can use this feature, you need to authenticate yourself with your Aruba passport account and collect a token that will be used for subsequent requests. This token will expire after a certain time, so you need to refresh it periodically. You can find more details about how to use the documentation interface and collect a token in the ArubaOS-CX REST API Guide1.

QUESTION 3
A customer has an AOS 10 architecture, consisting of Aruba AP and AOS-CX switches, managed by Aruba Central. The customer wants to obtain information about the clients, such as their general category and OS. What should you explain?

A. The customer must deploy Aruba gateways in order to receive any client profiling information.
B. You will need to set up Aruba Central as a secondary IP helper for client VLANs, but this will not interfere with existing operations.
C. Aruba Central will automatically derive this information using telemetry from the Aruba devices.
D. The customer should set up a dedicated switch VSX group to sniff packets and direct them to Aruba Central.

Correct Answer: C
Section:
Explanation:
Aruba Central can provide visibility and profiling of clients using the Client Insights feature, which is an AI-powered solution that uses native infrastructure telemetry to identify and classify clients based on their OS and general category. This feature does not require any additional hardware or software, such as gateways, IP helpers, or packet sniffers. It works by collecting and analyzing data from the Aruba APs and AOS-CX switches that are managed by Aruba Central. You can find more information about Client Insights in the Visibility and profiling solutions | HPE Aruba Networking page and the Clients Profile - Aruba page.

QUESTION 4
You are reviewing an endpoint entry in ClearPass Policy Manager (CPPM) Endpoints Repository.
What is a good sign that someone has been trying to gain unauthorized access to the network?

A. The entry shows multiple DHCP options under the fingerprints.
B. The entry shows an Unknown status.
C. The entry shows a profile conflict of having a new profile of Computer for a profiled Printer.
D. The entry lacks a hostname or includes a hostname with long seemingly random characters.

Correct Answer: C
Section:
Explanation:
A profile conflict occurs when ClearPass Policy Manager (CPPM) detects a change in the device category or OS family of an endpoint that has been previously profiled. This could indicate that someone has spoofed the MAC address of a legitimate device and is trying to gain unauthorized access to the network. For example, if an endpoint that was previously profiled as a Printer suddenly shows a new profile of Computer, this could be a sign of an attack. You can find more information about profile conflicts and how to resolve them in the ClearPass Policy Manager User Guide1. The other options are not necessarily signs of unauthorized access, as they could have other explanations. For example, multiple DHCP options under the fingerprints could indicate that the device has connected to different networks or subnets, an Unknown status could indicate that the device has not been authenticated yet, and a lack of hostname or a random hostname could indicate that the device has not been configured properly or has been reset to factory settings.

QUESTION 5
Refer to the scenario.
A customer is using an AOS 10 architecture with Aruba APs and Aruba gateways (two per site).
Admins have implemented auto-site clustering for gateways with the default gateway mode disabled. WLANs use tunneled mode to the gateways.
The WLAN security is WPA3-Enterprise with authentication to an Aruba ClearPass Policy Manager (CPPM) cluster VIP. RADIUS communications use RADIUS, not RadSec.
CPPM is using the service shown in the exhibits.

Services - written-exam wireless service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Service:

Name:	written-exam wireless service
Description:	
Type:	802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Profile Endpoints

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)

Authentication:

Authentication Methods:	Exam TLS
Authentication Sources:	ExamAD [Active Directory]

Which step can you take to improve operations during a possible gateway failover event?

A. Chanqe the WLANs to mixed-mode forwardinq so that vou can select multiple qatewav clusters.
B. Set up qatewav clusters manually and set VRRP IP addresses for dynamic authorization.
C. Use auto-group clustering instead of auto-site clustering for the gateways.
D. Enable default gateway mode for the gateway clusters.

Correct Answer: B
Section:
Explanation:
Auto-site clustering is a feature that allows gateways in the same site and group to form a cluster automatically. However, this mode does not support VRRP IP addresses, which are required for dynamic

authorization (CoA) from ClearPass Policy Manager (CPPM) to the gateways. Dynamic authorization is a mechanism that allows CPPM to change the attributes or status of a client session on the gateways without requiring re-authentication. This is useful for applying policies, roles, or bandwidth limits based on various conditions. Without VRRP IP addresses, CPPM would not be able to send CoA messages to the correct gateway in case of a failover event, resulting in inconsistent or incorrect client behavior.
To enable VRRP IP addresses for dynamic authorization, you need to set up gateway clusters manually and assign a VRRP VLAN and a VRRP IP address to each cluster. This way, CPPM can use the VRRP IP address as the NAS IP address for RADIUS communications and CoA messages. The VRRP IP address will remain the same even if the active gateway in the cluster changes due to a failover event, ensuring seamless operations.
You can find more information about how to set up gateway clusters manually and configure VRRP IP addresses in the Gateway Cluster Deployment - Aruba page and the ClearPass Policy Manager User Guide1.

QUESTION 6
Refer to the scenario.
A customer is using an AOS 10 architecture with Aruba APs and Aruba gateways (two per site).
Admins have implemented auto-site clustering for gateways with the default gateway mode disabled. WLANs use tunneled mode to the gateways.
The WLAN security is WPA3-Enterprise with authentication to an Aruba ClearPass Policy Manager (CPPM) cluster VIP. RADIUS communications use RADIUS, not RadSec.
For which devices does CPPM require network device entries?

A. Forgateways' actual IP addresses and dynamic authorization VRRP addresses
B. For gateways' actual IP addresses and AP clusters' virtual IP addresses for dynamic authorization
C. For APs' actual IP addresses
D. ForAP clusters'virtual IP addresses

Correct Answer: A
Section:
Explanation:
ClearPass Policy Manager (CPPM) requires network device entries for the devices that communicate with it using RADIUS or TACACS+ protocols. In this scenario, the gateways are the devices that act as RADIUS clients and send authentication requests to CPPM for the WLAN users. Therefore, CPPM needs to have network device entries for the gateways' actual IP addresses and the shared secrets that match the ones configured on the gateways.
Additionally, CPPM also requires network device entries for the gateways' dynamic authorization VRRP addresses, which are used for sending CoA messages to the gateways. CoA messages are used to change the attributes or status of a user session on the gateways without requiring reauthentication.
For example, CPPM can use CoA to apply policies, roles, or bandwidth limits based on various conditions. To enable VRRP IP addresses for dynamic authorization, you need to set up gateway clusters manually and assign a VRRP VLAN and a VRRP IP address to each cluster. This way, CPPM can use the VRRP IP address as the NAS IP address for RADIUS communications and CoA messages. The VRRP IP address will remain the same even if the active gateway in the cluster changes due to a failover event, ensuring seamless operations.

QUESTION 7
A customer wants CPPM to authenticate non-802.1X-capable devices. An admin has created the service shown in the exhibits below:

Services - Written-exam-service-3

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	Written-exam-service-3
Description:	MAC-based Authentication Service
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO
2.	Radius:IETF	Service-Type	BELONGS_TO
3.	Connection	Client-Mac-Address	EQUALS

Authentication:

Authentication Methods:	[MAC AUTH]
Authentication Sources:	[Endpoints Repository] [Local SQL DB]
Strip Username Rules:	-

Roles:

Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	written-exam-policy-3

Services - Written-exam-service-3

Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	written-exam-policy-3 Modify

Enforcement Policy Details

Description:

What is one recommendation to improve security?

A. Adding an enforcement policy rule that denies access to endpoints with the Conflict flaq
B. Using Active Directory as the authentication source
C. Creating and using a custom MAC-Auth authentication method
D. Enabling caching of posture and roles

Correct Answer: C
Section:
Explanation:
MAC Authentication Bypass (MAB) is a technique that allows non-802.1X-capable devices to bypass the 802.1X authentication process and gain network access based on their MAC addresses. However, MAB has some security drawbacks, such as the possibility of MAC address spoofing or unauthorized devices being added to the network. Therefore, it is recommended to use a custom MAC-Auth authentication method that adds an additional layer of security to MAB.
A custom MAC-Auth authentication method is a method that uses a combination of the MAC address and another attribute, such as a username, password, or certificate, to authenticate the device. This way, the device needs to provide both the MAC address and the additional attribute to gain access, making it harder for an attacker to spoof or impersonate the device. A custom MAC-Auth authentication method can be created and configured in ClearPass Policy Manager (CPPM) by following the steps in the Customizing MAC Authentication - Aruba page.

QUESTION 8
You are working with a developer to design a custom NAE script for a customer. The NAE agent should trigger an alert when ARP inspection drops packets on a VLAN. The customer wants the admins to be able to select the correct VLAN ID for the agent to monitor when they create the agent.
What should you tell the developer to do?

A. Use this variable, %{vlan-id} when defining the monitor URI in the NAE agent script.
B. Define a VLAN ID parameter; reference that parameter when defining the monitor URI.
C. Create multiple monitors within the script from which admins can select when they create the agent.
D. Use a callback action to collect the ID of the VLAN on which admins have enabled NAE monitoring.

Correct Answer: B
Section:
Explanation:
A custom NAE script is a Python script that defines the monitors, the alert-trigger logic, and the remedial actions for an NAE agent. A monitor is a URI that specifies the data source and the data type that the NAE agent should collect and analyze. For example, to monitor the ARP inspection statistics on a VLAN, the monitor URI would be something like this:

```
/rest/v1/system/vlans/<vlan-id>/arp_inspection_stats
```

where <vlan-id> is the ID of the VLAN to be monitored.
To allow the admins to select the correct VLAN ID for the agent to monitor when they create the agent, you need to define a VLAN ID parameter in the NAE script. A parameter is a variable that can be set by the user when creating or modifying an agent. A parameter can be referenced in other parts of the script by using the syntax ${parameter-name}. For example, to define a VLAN ID parameter and reference it in the monitor URI, you would write something like this:

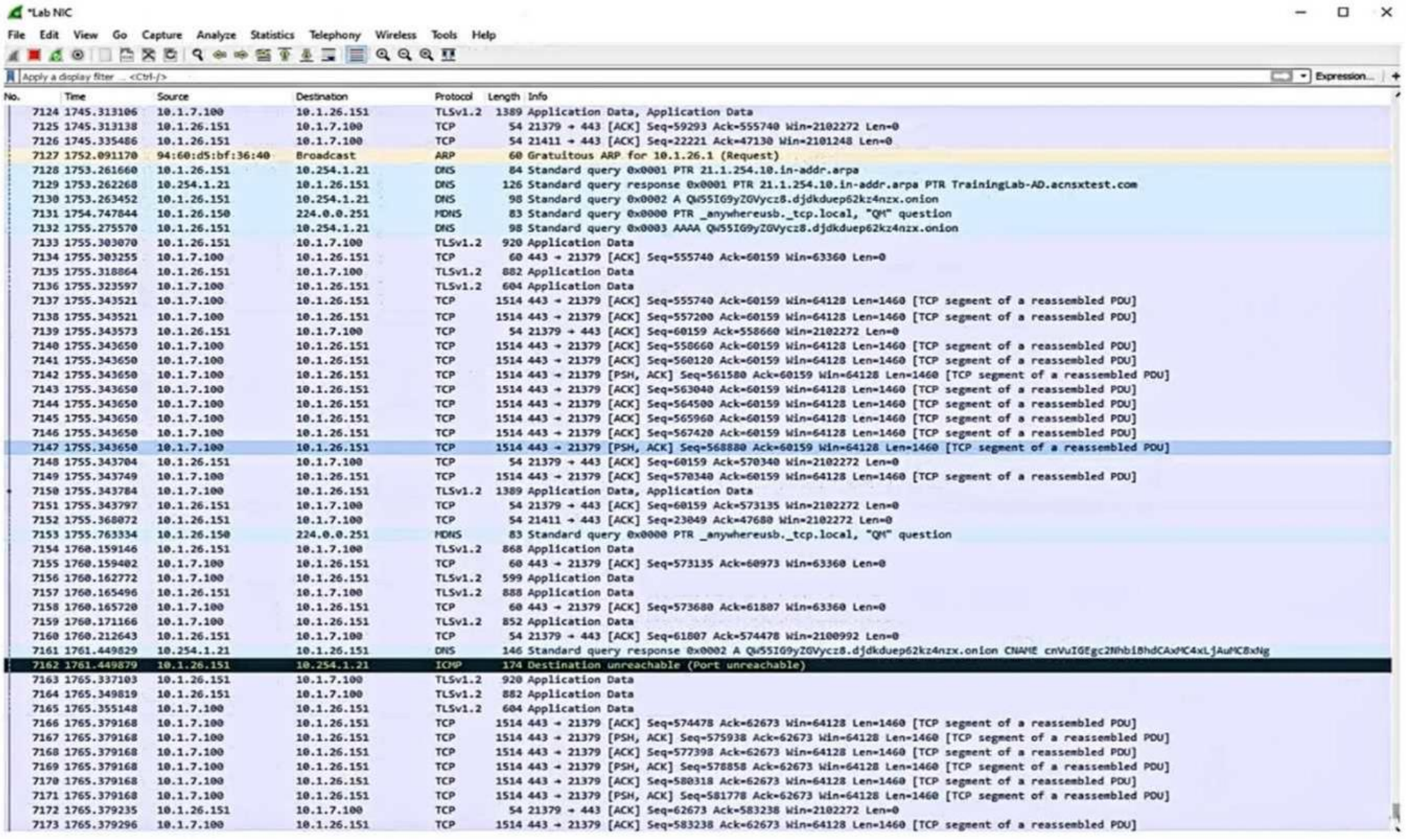
```
parameters = [{"name": "vlan-id", "type": "integer", "description": "VLAN ID to be
monitored"}]

monitor = [{"uri": "/rest/v1/system/vlans/${vlan-id}/arp_inspection_stats", "type": "json"}]
```

This way, when the admins create or modify the agent, they can enter the VLAN ID that they want to monitor, and the NAE script will use that value in the monitor URI.
You can find more information about how to write custom NAE scripts and use parameters in the NAE Scripting Guide

QUESTION 9

Refer to the exhibit.



Which IP address should you record as a possibly compromised client?

A. 10.1.26.151
B. 10.1J.100
C. 10.1.26.1
D. 10.254.1.21

Correct Answer: A
Section:
Explanation:
The exhibit shows a screenshot of a Malwarebytes alert that indicates that a website was blocked due to compromise. The alert contains the following information:
The type of protection: Web Protection
The website that was blocked: 10.254.1.21
The port that was used: 80
The process that initiated the connection: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
The IP address of the device that initiated the connection: 10.1.26.151
The IP address of the device that initiated the connection is the one that should be recorded as a possibly compromised client, as it indicates that the device tried to access a malicious website that could infect it with malware or steal its data. In this case, the IP address of the possibly compromised client is 10.1.26.151.

QUESTION 10
You need to install a certificate on a standalone Aruba Mobility Controller (MC). The MC will need to use the certificate for the Web UI and for implementing RadSec with Aruba ClearPass Policy Manager. You have been given a certificate with these settings:
Subject: CN=mc41.site94.example.com
No SANs
Issuer: CN=ca41.example.com
EKUs: Server Authentication, Client Authentication
What issue does this certificate have for the purposes for which the certificate is intended?

A. It has conflicting EKUs.
B. It is issued by a private CA.
C. It specifies domain info in the CN field instead of the DC field.
D. It lacks a DNS SAN.

Correct Answer: D
Section:
Explanation:
A DNS SAN (Subject Alternative Name) is an extension of the X.509 certificate standard that allows specifying additional hostnames or IP addresses that the certificate can be used for. A DNS SAN is useful for validating the identity of the server or client that presents the certificate, especially when the common name (CN) field does not match the hostname or IP address of the server or client.
In this case, the certificate has a CN of mc41.site94.example.com, which is the fully qualified domain name (FQDN) of the standalone Aruba Mobility Controller (MC). However, this CN may not match the hostname or IP address that the MC uses for the Web UI or for implementing RadSec with Aruba ClearPass Policy Manager. For example, if the MC uses a different FQDN, such as mc41.example.com, or an IP address, such as 192.168.1.41, for these purposes, then the certificate would not be valid for them. Therefore, the certificate should have a DNS SAN that includes all the possible hostnames or IP addresses that the MC may use for the Web UI and RadSec.

QUESTION 11
A customer has an AOS 10-based mobility solution, which authenticates clients to Aruba ClearPass Policy Manager (CPPM). The customer has some wireless devices that support WPA2 in personal mode only.
How can you meet these devices' needs but improve security?

A. Use MPSK on the WLAN to which the devices connect.
B. Configure WIDS policies that apply extra monitoring to these particular devices.
C. Connect these devices to the same WLAN to which 802.1X-capable clients connect, using MACAuth fallback.
D. Enable dynamic authorization (RFC 3576) in the AAA profile for the devices.

Correct Answer: A
Section:

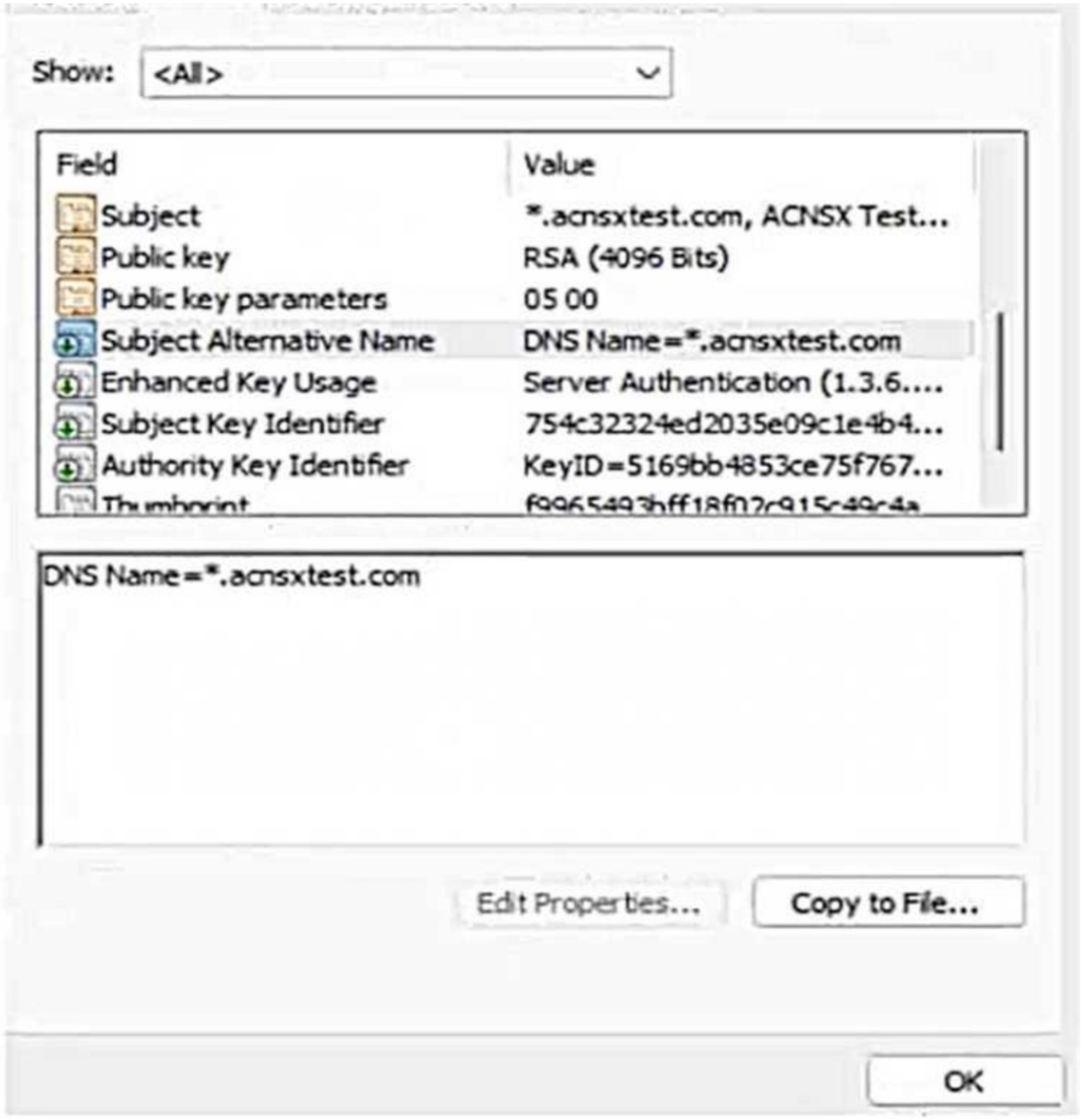
Explanation:
MPSK (Multi Pre-Shared Key) is a feature that allows assigning different pre-shared keys (PSKs) to different devices or groups of devices on the same WLAN. MPSK improves security over WPA2 in personal mode, which uses a single PSK for all devices on the WLAN. With MPSK, you can create and manage multiple PSKs, each with its own role, policy, and expiration date. You can also revoke or change a PSK for a specific device or group without affecting other devices on the WLAN. MPSK is compatible with devices that support WPA2 in personal mode only, as they do not need to support any additional protocols or certificates.
To use MPSK on the WLAN to which the devices connect, you need to enable MPSK in the WLAN settings and configure the PSKs in Aruba ClearPass Policy Manager (CPPM). You can find more information about how to configure MPSK in the [Configuring Multi Pre-Shared Key - Aruba] page and the [ClearPass Policy Manager User Guide] . The other options are not correct because they either do not improve security or are not applicable for devices that support WPA2 in personal mode only. For example, configuring WIDS policies that apply extra monitoring to these particular devices would not prevent them from being compromised or spoofed, but rather detect and mitigate potential attacks. Connecting these devices to the same WLAN to which 802.1X-capable clients connect, using MAC-Auth fallback, would not provide strong authentication or encryption, as MAC addresses can be easily spoofed or captured. Enabling dynamic authorization (RFC 3576) in the AAA profile for the devices would not affect the authentication process, but rather allow CPPM to change the attributes or status of a user session on the controller without requiring re-authentication.

QUESTION 12
When would you implement BPDU protection on an AOS-CX switch port versus BPDU filtering?

A. Use BPDU protection on edge ports to protect against rogue devices when the switch implements MSTP; use BPDU filtering to protect against rogue devices when the switch implements PVSTP+.
B. Use BPDU protection on edge ports to prevent rogue devices from connecting; use BPDU filtering on inter-switch ports for specialized use cases.
C. Use BPDU protection on inter-switch ports to ensure that they are selected as root; use BPDU filtering on edge ports to prevent rogue devices from connecting.
D. Use BPDU protection on edge ports to permanently lock out rogue devices; use BPDU filtering on edge ports to temporarily lock out rogue devices.

Correct Answer: B
Section:
Explanation:
BPDU (Bridge Protocol Data Unit) is a message that is exchanged between switches to maintain the spanning tree topology and prevent loops. BPDU protection and BPDU filtering are two features that can be configured on AOS-CX switch ports to enhance security and performance.
BPDU protection is a feature that disables a port if it receives a BPDU, indicating that an unauthorized switch or device has been connected to the port. BPDU protection is typically used on edge ports, which are ports that connect to end devices such as PCs or printers, and are not expected to receive BPDUs. BPDU protection prevents rogue devices from connecting to the network and affecting the spanning tree topology.
BPDU filtering is a feature that prevents a port from sending or receiving BPDUs, effectively isolating the port from the spanning tree topology. BPDU filtering is typically used on inter-switch ports, which are ports that connect to other switches, for specialized use cases such as creating a separate spanning tree domain or reducing the overhead of BPDUs. BPDU filtering should be used with caution, as it can create loops or inconsistencies in the network.
You can find more information about how to configure BPDU protection and BPDU filtering on AOSCX switch ports in the [Configuring Spanning Tree Protocol - Aruba] page and the [AOS-CX Switching Configuration Guide] page. The other options are not correct because they either use BPDU protection or BPDU filtering on the wrong type of ports or for the wrong purpose. For example, using BPDU protection on inter-switch ports would disable the ports if they receive BPDUs, which are expected in normal operation. Using BPDU filtering on edge ports would allow rogue devices to connect to the network and create loops or affect the spanning tree topology.

QUESTION 13
Refer to the exhibit.



You have been given this certificate to install on a ClearPass server for the RADIUS/EAP and RadSec usages.
What is one issue?

A. The certificate has a wildcard in the subject common name.
B. The certificate uses a fully qualified the '.local" domain name.
C. The certificate does not have a URI subject alternative name
D. The certificate does not have an IP subject alternative name

Correct Answer: B
Section:
Explanation:
The exhibit shows a screenshot of a certificate that has the following information:
The subject common name (CN) is *.clearpass.local, which is a wildcard domain name that matches any subdomain under clearpass.local.
The subject alternative names (SANs) are DNS Name=clearpass.local and DNS
Name=*.clearpass.local, which are the same as the subject CN.
The issuer CN is clearpass.local, which is the same as the subject domain name.
The key usage (KU) is Digital Signature and Key Encipherment, which are required for RADIUS/EAP and RadSec usages.
The extended key usage (EKU) is Server Authentication and Client Authentication, which are also required for RADIUS/EAP and RadSec usages.
The issue with this certificate is that it uses a fully qualified the '.local' domain name, which is a reserved domain name for local networks that cannot be registered on the public Internet. This means that the certificate cannot be verified by any public certificate authority (CA), and therefore cannot be trusted by any external devices or servers that communicate with ClearPass. This could cause problems for RADIUS/EAP and RadSec usages, as they rely on secure and authenticated connections between ClearPass and other devices or servers.
To avoid this issue, the certificate should use a valid domain name that can be registered on the public Internet, such as clearpass.com or clearpass.net. This way, the certificate can be issued by a public CA that is trusted by most devices and servers, and can be verified by them. Alternatively, if the certificate is intended to be used only within a private network, it should be issued by a private CA that is trusted by all devices and servers within that network.

QUESTION 14
A customer needs you to configure Aruba ClearPass Policy Manager (CPPM) to authenticate domain users on domain computers. Domain users, domain computers, and domain controllers receive certificates from a Windows CA. CPPM should validate these certificates and verify that the users and computers have accounts in Windows AD. The customer requires encryption for all communications between CPPM and the domain controllers.
You have imported the root certificate for the Windows CA to the ClearPass CA Trust list.
Which usages should you add to it based on these requirements?

A. Radec and Aruba infrastructure
B. EAP and AD/LDAP Server
C. EAP and Radsec
D. LDAP and Aruba infrastructure

Correct Answer: C
Section:
Explanation:
EAP (Extensible Authentication Protocol) is a framework that allows different authentication methods to be used for network access. EAP is used for RADIUS/EAP authentication, which is a common method for authenticating domain users on domain computers using certificates. EAP requires that the RADIUS server, such as ClearPass Policy Manager (CPPM), validates the certificates presented by the clients and verifies their identity against an identity source, such as Windows AD.
Therefore, the root certificate for the Windows CA that issues the certificates to the clients should have the EAP usage in the ClearPass CA Trust list.
Radsec (RADIUS over TLS) is a protocol that allows secure and encrypted communication between RADIUS servers and clients using TLS. Radsec is used for encrypting all communications between CPPM and the domain controllers, which act as RADIUS clients. Radsec requires that both the RADIUS server and the RADIUS client validate each other's certificates and establish a TLS session.
Therefore, the root certificate for the Windows CA that issues the certificates to the domain controllers should have the Radsec usage in the ClearPass CA Trust list.

QUESTION 15
A customer's admins have added RF Protect licenses and enabled WIDS for a customer's AOS 8-based solution. The customer wants to use the built-in capabilities of APs without deploying dedicated air monitors (AMs). Admins tested rogue AP detection by connecting an unauthorized wireless AP to a switch. The rogue AP was not detected even after several hours.
What is one point about which you should ask?

A. Whether APs' switch ports support all the VLANs that are accessible at the edge
B. Whether admins enabled wireless containment

C. Whether admins set at least one radio on each AP to air monitor mode
D. Whether the customer is using non-standard Wi-Fi channels in the deployment

Correct Answer: C
Section:
Explanation:
RF Protect is a feature that enables wireless intrusion detection and prevention system (WIDS/WIPS) capabilities on AOS 8-based solutions. WIDS/WIPS allows detecting and mitigating rogue APs, unauthorized clients, and other wireless threats. RF Protect requires RF Protect licenses to be installed and WIDS to be enabled on the Mobility Master (MM).
To use the built-in capabilities of APs for WIDS/WIPS, without deploying dedicated air monitors (AMs), admins need to set at least one radio on each AP to air monitor mode. Air monitor mode allows the AP to scan the wireless spectrum and report any wireless activity or anomalies to the MM.
Air monitor mode does not affect the other radio on the AP, which can still serve clients in access mode. By setting at least one radio on each AP to air monitor mode, admins can achieve full coverage and visibility of the wireless environment and detect rogue APs.
If admins do not set any radio on the APs to air monitor mode, the APs will not scan the wireless spectrum or report any wireless activity or anomalies to the MM. This means that the APs will not be able to detect rogue APs, even if they are connected to the same network. Therefore, admins should check whether they have set at least one radio on each AP to air monitor mode.

QUESTION 16
A customer has an AOS 10-based solution, including Aruba APs. The customer wants to use Cloud Auth to authenticate non-802.1X capable IoT devices.
What is a prerequisite for setting up the device role mappings?

A. Configuring a NetConductor-based fabric
B. Configuring Device Insight (client profile) tags in Central
C. Integrating Aruba ClearPass Policy Manager (CPPM) and Device Insight
D. Creating global role-to-role firewall policies in Central

Correct Answer: B
Section:
Explanation:
According to the Aruba Cloud Authentication and Policy Overview1, one of the prerequisites for configuring Cloud Authentication and Policy is to configure Device Insight (client profile) tags in Central. Device Insight tags are used to identify and classify IoT devices based on their behavior and characteristics. These tags can then be mapped to client roles, which are defined in the WLAN configuration for IAPs2. Client roles are used to enforce role-based access policies for the IoT devices.
Therefore, option B is the correct answer.
Option A is incorrect because NetConductor is not related to Cloud Authentication and Policy.
NetConductor is a cloud-based network management solution that simplifies the deployment and operation of Aruba Instant networks.
Option C is incorrect because integrating Aruba ClearPass Policy Manager (CPPM) and Device Insight is not a prerequisite for setting up the device role mappings. CPPM and Device Insight can work together to provide enhanced visibility and control over IoT devices, but they are not required for Cloud Authentication and Policy.
Option D is incorrect because creating global role-to-role firewall policies in Central is not a prerequisite for setting up the device role mappings. Global role-to-role firewall policies are used to define the traffic rules between different client roles across the entire network, but they are not required for Cloud Authentication and Policy.

QUESTION 17
You want to use Device Insight tags as conditions within CPPM role mapping or enforcement policy rules.
What guidelines should you follow?

A. Create an HTTP authentication source to the Central API that queries for the tags. To use that source as the type for rule conditions, add it an authorization source for the service in question.
B. Use the Application type for the rule conditions; no extra authorization source is required for services that use policies with these rules.
C. Use the Endpoints Repository type for the rule conditions; Add Endpoints Repository as a secondary authentication source for services that use policies with these rules.
D. Use the Endpoint type for the rule conditions; no extra authorization source is required for services that use policies with these rules.

Correct Answer: D
Section:
Explanation:
According to the Aruba Cloud Authentication and Policy Overview1, Device Insight tags are stored in the Endpoint Repository and can be used as conditions within CPPM role mapping or enforcement policy rules. The rule condition type should be Endpoint, and the attribute should be Device Insight Tags. No extra authorization source is required for services that use policies with these rules.
Therefore, option D is the correct answer.
Option A is incorrect because creating an HTTP authentication source to the Central API is not necessary to use Device Insight tags as conditions. Device Insight tags are already synchronized between Central and CPPM, and can be accessed from the Endpoint Repository.
Option B is incorrect because using the Application type for the rule conditions is not applicable to Device Insight tags. The Application type is used to match attributes from the Application Authentication source, which is used to integrate with third-party applications such as Microsoft Intune or Google G Suite.
Option C is incorrect because using the Endpoints Repository type for the rule conditions is not valid for Device Insight tags. The Endpoints Repository type is used to match attributes from the Endpoints Repository source, which is different from the Endpoint type. The Endpoints Repository source contains information about endpoints that are manually added or imported into CPPM, while the Endpoint type contains information about endpoints that are dynamically discovered and profiled by CPPM or Device Insight. Adding Endpoints Repository as a secondary authentication source for services that use policies with these rules is also unnecessary and redundant.

QUESTION 18
A customer has an AOS 10 architecture, which includes Aruba APs. Admins have recently enabled WIDS at the high level. They also enabled alerts and email notifications for several events, as shown in the exhibit.

USER | ACCESS POINT | SWITCH | GATEWAY | CONNECTIVITY | AUDIT | SITE

By Clicking on + icon, you can quickly generate notifications with default notification policy. You can also define the policy by clicking on the tiles. GOT IT

New Virtual Controller Detected	+	Virtual Controller Disconnected	
AP Disconnected	✓	Rogue AP Detected	
Client Attack Detected	✓	Uplink Changed	
Modem Unplugged	+	Insufficient Power Supplied	
AP CPU Utilization	+	AP Memory Utilization	
Radio Noise Floor	+	Connected Clients Per VC	
Radio Frames Retry Percent	+	AP Tunnel Down	
Radio Non Wi-Fi Utilization	+	IAP Firmware Upgrade Failed	

Admins are complaining that they are getting so many emails that they have to ignore them, so they are going to turn off all notifications.
What is one step you could recommend trying first?

A. Send the email notifications directly to a specific folder, and only check the folder once a week.
B. Disable email notifications for Roque AP, but leave the Infrastructure Attack Detected and Client Attack Detected notifications on.
C. Change the WIDS level to custom, and enable only the checks most likely to indicate real threats.
D. Disable just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert.

Correct Answer: C
Section:
Explanation:
According to the AOS 10 documentation1, WIDS is a feature that monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. WIDS can be configured at different levels, such as low, medium, high, or custom. The higher the level, the more checks are enabled and the more alerts are generated. However, not all checks are equally relevant or indicative of real threats. Some checks may generate false positives or unnecessary alerts that can overwhelm the administrators and reduce the effectiveness of WIDS.
Therefore, one step that could be recommended to reduce the number of email notifications is to change the WIDS level to custom, and enable only the checks most likely to indicate real threats. This way, the administrators can fine-tune the WIDS settings to suit their network environment and security needs, and avoid getting flooded with irrelevant or redundant alerts. Option C is the correct answer.
Option A is incorrect because sending the email notifications directly to a specific folder and only checking the folder once a week is not a good practice for security management. This could lead to missing or ignoring important alerts that require immediate attention or action. Moreover, this does not solve the problem of getting too many emails in the first place.
Option B is incorrect because disabling email notifications for Rogue AP, but leaving the Infrastructure Attack Detected and Client Attack Detected notifications on, is not a sufficient solution.
Rogue APs are unauthorized access points that can pose a serious security risk to the network, as they can be used to intercept or steal sensitive data, launch attacks, or compromise network performance. Therefore, disabling email notifications for Rogue APs could result in missing critical alerts that need to be addressed.
Option D is incorrect because disabling just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert, is not a valid assumption. The Infrastructure Attack Detected alert covers a broad range of attacks that target the network infrastructure, such as deauthentication attacks, spoofing attacks, denial-of-service attacks, etc. The Rogue AP and Client Attack Detected alerts are more specific and focus on detecting and classifying rogue devices and clients that may be involved in such attacks. Therefore, disabling these alerts could result in losing valuable information about the source and nature of the attacks.

QUESTION 19
Refer to the scenario.
A customer has asked you to review their AOS-CX switches for potential vulnerabilities. The configuration for these switches is shown below:

```
hostname Access-Switch-$$

ntp authentication-key 1 sha1 ciphertext
AQBapYn45h7mDzxcLhAYWBH6biegegFASS1kvTQPPglCEfaLCAAAAMIb48QNRhSg
ntp trusted-key 1
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst key-id 1
ntp enable
ntp authentication
!
radius-server host rad.example.com tls
!
tacacs-server host rad.example.com
!
aaa authentication login ssh group tacacs local
aaa authentication login telnet group tacacs local
!
aaa accounting port-access start-stop interim group radius
!
radius dyn-authorization enable
!
radius dyn-authorization client rad.example.com tls
ssh server vrf default
ssh server vrf mgmt
telnet server vrf default
telnet server vrf mgmt
crypto pki application radsec-client certificate device-identity
crypto pki ta-profile privateca
ta-certificate
        -----BEGIN CERTIFICATE-----
MIIGAzCCA+ugAwIBAgIUEVfsxopuixT2QHZDJ/UYAAbYsdowDQYJKoZIhvcNAQEL
BQAwgYgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQH
DAlTdW5ueXZhbGUxHDAaBgNVBAoME0FydWJhIFRyYWluaW5nIExhYnMxEzARBgNV
BAsMCkFDTlNYIFRlc3QxHTAbBgNVBAMMFHJvb3RjYS5hY25zeHRlc3QuY29tMB4X
DTIyMTEyMjIwNTQxOFoXDTMyMTExOTIwNTQxOFowgYgxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUxHDAaBgNVBAoM
E0FydWJhIFRyYWluaW5nIExhYnMxEzARBgNVBAsMCkFDTlNYIFRlc3QxHTAbBgNV
BAMMFHJvb3RjYS5hY25zeHRlc3QuY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAsiUzsBkJcUgcdsbRyoLd0ZNqpcXfphk2VsSzZngP1LCu3lea3OHU
V9GchhJXOQaI3HDUTcLp4b5If63z4nKzA36T6tyWXOe0PSgUjy+61XXMA9Rp5DKc
CyoY9F8spVJiEo2n2hqL4m/DLFYlhxo5Z2UKav/08DMfzD/yVUzGNiQKDP/L7ivk
CWF+l5WIGSrH10i/rgIM/+W20n58aDx5f1AWaH9bYdRTwFMuklUXQ/f8+7+9PXju
B95Mt4b77RaWWj6CkW9k8WhmyjE7MMPSHtuJ4t3evh7jd/lTkm5ZOg/V8kvNTtW5
fif7lkWLevmlLlvcxYnj+S3CWhAFdaR7S33a6xwdZxCDOLfPB6L1oOnKeOVM4mO2
lOZtJNPFueBt16BRolR+IMANQkj3B2lB0whSLHF6JmLr0L6y/edV8XhIUhMxOfIp
JKeSw38TDm3t1k98PBCOaLj5s4tYJRxcZLDnrg7Oz1e37sxENYoBtgRp77cdfePr
cP/sp8U66gti2F0ijkU6k37moL3sMs2uHgC0YWpfRyFI09BWCRbxmy81UePiSlsW
0goOaPDr35W/0443I/z6A+q/ciwVrALS+zEfHbMDFxo4VMygJttaiWZ05GAQQSHj
redQmQEQPMwkgbzaELtAgYOWGkB56T/XifRLVxneYU8woAEZwmscI3kCAwEAAaNj
MGEwHQYDVR0OBBYEFGXCH/z475pdNKIHhjDxFCfjz8khMB8GA1UdIwQYMBaAFGXC
H/z475pdNKIHhjDxFCfjz8khMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgGGMA0GCSqGSIb3DQEBCwUAA4ICAQB5TGIspaamHQXtsnWgmux6PANdEdPZ0Ele
wDnpUxkVbeSPr9wl8luRJMptRO25rwVwEtrM8t5JD4jAK+d0usr4TDKwWqPPqFi0
F5svFK9aEJ59ceD+eDWl4LAJJi3zjb9ZBuBa3LkaP7kyTlSnI0+opN+vdV43LNXh
T23xEmLC9OUolq3bb8zpkWXieeFwSo2BafFMscPdf75DVY+x+Qo1SgpjbWBAS80B
jRdZHrKmsqcrIG+37bixqaFj9nMzWpX0n2HfKCVcl6uk2pDNbiYVbU3k9b/ZWQmW
DRYkAuR8dFBN3lKDyQo86T/chT/DY77FoStfg0gDZEj3EqaM76rf8S2z1GCsrfkp
Crp5oKP6jiOCi2EcidkZSsmbzAHWKXNaF7vWRj0OiypgEFRkIVu/kce9O2KaxNYd
sIKlNh7gG4pcQqhFfDddFD9vXvjOwKnXKkKppUpN6w+Quc+jhqFpP8GVPOy7ayZo
z5cz5yEaVXtbfXRhVSg9oooq7xImBT14SK1pyrHSj8sD67Og3zgnNot/v8fHhI3O
zUtBe4UPGWfraO4gkHH3mbb1qYeJnxKpMz56A0APBkKV9icY0uTQOsHk6bA91G+Q
sjqyWwKApf7RB4lHjF+7FfMU6UJnZBm75zQ89CPAPCoVeJ6fNNr/aO+3VrNz4j9l
Nr63M6xeYw==
-----END CERTIFICATE-----
    END OF CERTIFICATE
```

What is one recommendation to make?

A. Let the RADIUS server configure VLANs on LAG 1 dynamically.
B. Use MDS instead of SHA1 for the NTP authentication key.
C. Encrypt the certificate in the TA-profile.
D. Create a control plane ACL to limit the sources that can access the switch with SSH.

Correct Answer: D
Section:
Explanation:
According to the AOS-CX Switches Multiple Vulnerabilities1, one of the vulnerabilities (CVE-2021-41000) affects the SSH service on AOS-CX switches. This vulnerability allows an unauthenticated remote attacker to cause a denial-of-service condition on the switch by sending specially crafted SSH packets. The impact of this vulnerability is high, as it could result in a loss of management access and network disruption.
Therefore, one recommendation to make is to create a control plane ACL to limit the sources that can access the switch with SSH. This way, the switch can filter out unwanted or malicious SSH traffic and reduce the risk of exploitation.