Free Questions for HPE6-A84 by braindumpscollection

Shared by Hurley on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which element helps to lay the foundation for solid network security forensics?

Options:

A- Enable BPDU protection and loop protection on edqe switch ports

B- Enabling debug-level information for network infrastructure device logs

C- Implementing 802.1X authentication on switch ports that connect to APs

D- Ensuring that all network devices use a correct, consistent clock

Answer:

D

Explanation:

This is because network forensics relies on the analysis of network traffic data, which is often time-stamped by the devices that generate or transmit it.Having a synchronized and accurate clock across all network devices helps to establish a reliable timeline of events and

correlate different sources of evidence12

A)Enable BPDU protection and loop protection on edge switch ports is not related to network security forensics, but rather to preventing network loops and topology changes caused by rogue switches or bridges3

B) Enabling debug-level information for network infrastructure device logs might provide more details about the network activity, but it also consumes more resources and storage, and might not be relevant or useful for forensic analysis.Moreover, debug-level information might not be available for long-term retention or legal purposes4

C) Implementing 802.1X authentication on switch ports that connect to APs is a good security practice to prevent unauthorized access to the network, but it does not directly help with network security forensics.802.1X authentication does not capture or record network traffic data, which is the main source of evidence for network forensics

Question 2

Question Type: MultipleChoice

Refer to the scenario.

This customer is enforcing 802.1X on AOS-CX switches to Aruba ClearPass Policy Manager (CPPM). The customer wants switches to download role settings from CPPM. The "reception-domain" role must have these settings:

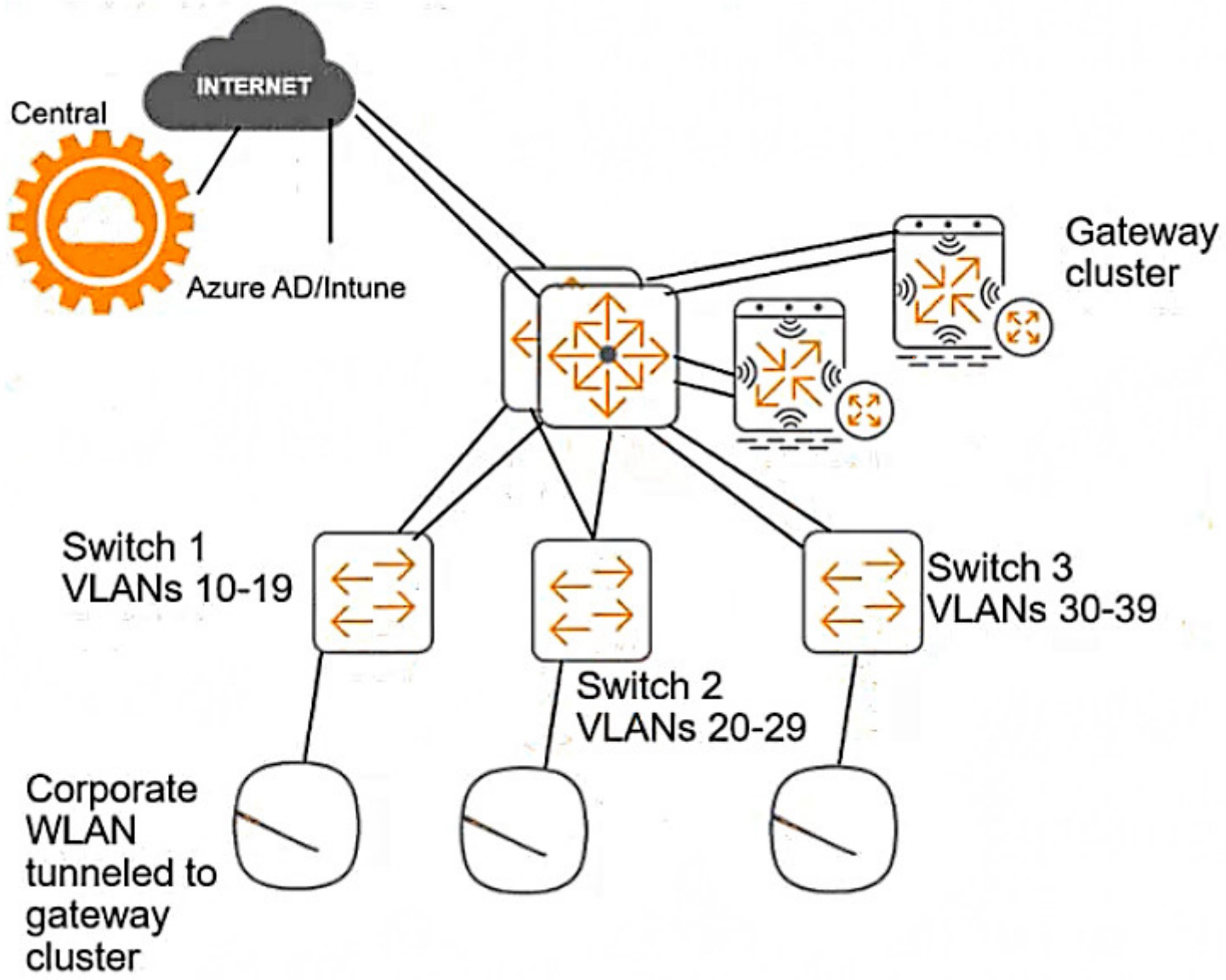
--- Assigns clients to VLAN 14 on switch 1, VLAN 24 on switch 2, and so on.

--- Filters client traffic as follows:

--- Clients are permitted full access to 10.1.5.0/24 and the Internet

--- Clients are denied access to 10.1.0.0/16

The switch topology is shown here:


INTERNET
Central
Azure AD/Intune
Gateway
cluster
Switch 1
VLANs 10-19
Switch 2
VLANs 20-29
Switch 3
VLANs 30-39
Corporate
WLAN
tunneled to
gateway
cluster

How should you configure the VLAN setting for the reception role?

Options:

A- Assign a consistent name to VLAN 14, 24, or 34 on each access layer switch and reference that name in the enforcement profile VLAN settings.

B- Configure the enforcement profile as a downloadable role, but specify only the role name and leave the VLAN undefined. Then define a 'reception' role with the correct VLAN setting on each individual access layer switch.

C- Assign a number-based ID to the access layer switches. Then use this variable in the enforcement profile VLAN settings: %(NAS-ID]4.

D- Create a separate enforcement profile with a different VLAN ID for each switch. Add all profiles to the profile list in the appropriate enforcement policy rule.

Answer:

A

Explanation:

According to the AOS-CX User Guide, one way to configure the VLAN setting for the reception role is to assign a consistent name to VLAN 14, 24, or 34 on each access layer switch and reference that name in the enforcement profile VLAN settings. This way, the switches can download the role settings from CPPM and apply the correct VLAN based on the name, rather than the ID. For example, the enforcement profile VLAN settings could be:

```
vlan-name reception-vlan
```

And the VLAN configuration on each switch could be:

```
vlan 14
name reception-vlan
exit
```

```
vlan 24
name reception-vlan
exit
```

```
vlan 34
name reception-vlan
exit
```

Question 3

Question Type: **MultipleChoice**

You are setting up Aruba ClearPass Policy Manager (CPPM) to enforce EAP-TLS authentication with Active Directory as the authentication source. The company wants to prevent users with disabled accounts from connecting even if those users still have valid certificates.

As the first part of meeting these criteria, what should you do to enable CPPM to determine where accounts are enabled in AD or not?

Options:

A- Add an Endpoint Context Server to the domain controller with actions for querying the domain controller for account status.

B- Enable OCSP in the EAP-TLS authentication method settings and configure an OCSP override to the domain controller FQDN.

C- Add a custom attribute for userAccountControl to the filters in the AD authentication source.

D- Install a Microsoft Active Directory extension in Aruba ClearPass Guest and set up an HTTP authentication source that points to that extension.

Answer:

C

Explanation:

According to the ClearPass Policy Manager User Guide1, userAccountControl is a custom attribute in Active Directory that contains a set of flags that define the properties and behavior of user accounts. One of these flags is ACCOUNTDISABLE, which indicates whether the account is disabled or not. By adding this attribute to the filters in the AD authentication source, CPPM can retrieve this attribute for

each user and use it as a condition in the enforcement policies to prevent users with disabled accounts from connecting even if they have valid certificates. Therefore, option C is the correct answer.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

Device Insight Integration:	(•) Enable ( ) Disable
Registration Token:	4ROAMDNKLG
Bypass Proxy:	[ ] Enable to bypass proxy server
Activation Status:	Activated
Activation Timestamp:	Dec 15, 2022 17:33:02 EST
Registration Status:	Registered
Master ClearPass Server:	cp1.acnsxtest.com (10.38.1.113)
Standby ClearPass Server:	cp2.acnsxtest.com (10.38.1.114) (optional)
Polling Interval:	15 minutes
Device Sync Interval:	30 days Endpoints active in the date range specified will be synced between ClearPass Policy Manage

Device Tag Updates Action

Tags Update Action:	( ) No action ( ) Apply action for all Tag updates (•) Apply action for selected Tag updates only
Selected Tags for Action:	suspicious Remove Add
RADIUS Action:	[AOS-CX - Disconnect]

Aruba ClearPass Policy Manager (CPPM) is using the settings shown in the exhibit. You reference the tag shown in the exhibit in enforcement policies related to NASes of several types, including Aruba APs, Aruba gateways, and AOS-CX switches.

What should you do to ensure that clients are reclassified and receive the correct treatment based on the tag?

Options:

A- Change the RADIUS action to [Aruba Wireless -Terminate Session] which is supported by all the NASes in question.

B- Change the RADIUS action to [Aruba Wireless - Bounce Switch Port] which is supported by all the NASes in question.

C- Enable profiling in each service using one of these enforcement profiles. Set the profiling action to the correct one for the NASes using that service.

D- Set the Tags Update Action to No Action. Then instead enable the RADIUS CoAs using enforcement profiles in the rules that match clients with the tag shown in the exhibit.

Answer:

C

Explanation:

According to the ClearPass Policy Manager User Guide1, the tag shown in the exhibit is a Device Insight tag, which is used to classify and identify devices based on their behavior and characteristics. Device Insight tags can be used as conditions in enforcement policies to apply different actions or roles to devices based on their tags. However, in order to ensure that devices are reclassified and receive

the correct treatment based on their tags, profiling must be enabled in each service that uses one of these enforcement profiles. Profiling is a feature that allows ClearPass to dynamically discover and profile devices on the network, and update their attributes and tags accordingly. Profiling also allows ClearPass to send RADIUS Change of Authorization (CoA) messages to the network access servers (NASes) that control the access of the devices, and instruct them to reauthenticate or terminate the sessions of the devices that have changed their tags. The profiling action must be set to the correct one for the NASes using that service, as different NASes may support different types of CoA messages. Therefore, option C is the correct answer.

Question 5

Question Type: MultipleChoice

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
```

What is one immediate remediation that you should recommend?

Options:

A- Changing the switch's DNS server to the mgmt VRF

B- Setting the clock manually instead of using NTP

C- Either disabling DHCPv4-snoopinq or leaving it enabled, but also enabling ARP inspection

D- Disabling Telnet

Answer:

D

Explanation:

According to the AOS-CX Switches Multiple Vulnerabilities1, one of the vulnerabilities (CVE-2021-41001) affects the Telnet 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 Telnet packets. The impact of this vulnerability is high, as it could result in a loss of management access and network disruption. Therefore, one immediate remediation that you should recommend is to disable Telnet on the switch. This way, the switch can prevent any malicious Telnet traffic from reaching it and avoid the exploitation of this vulnerability.

Question 6

Question Type: MultipleChoice

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
AQBapYn45h7mDzxcLhAYWBH6biegegFASS1kvTQPPgICEfaLCAAAAMIb48QNRhSg
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
```

What is one recommendation to make?

Options:

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.

Answer:

D

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.

Question 7

Question Type: MultipleChoice

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

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

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?

Options:

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.

Answer:

C

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 8

Question Type: **MultipleChoice**

You want to use Device Insight tags as conditions within CPPM role mapping or enforcement policy rules.

What guidelines should you follow?

Options:

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.

Answer:

D

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 9

Question Type: **MultipleChoice**

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?

Options:

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

Answer:

B

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 10

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

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 11

Question Type: MultipleChoice

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 C

Options:

A- 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

Answer:

C

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.