HPE6-A84$^{Q\&As}$

Aruba Certified Network Security Expert Written

Pass HP HPE6-A84 Exam with 100% Guarantee

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

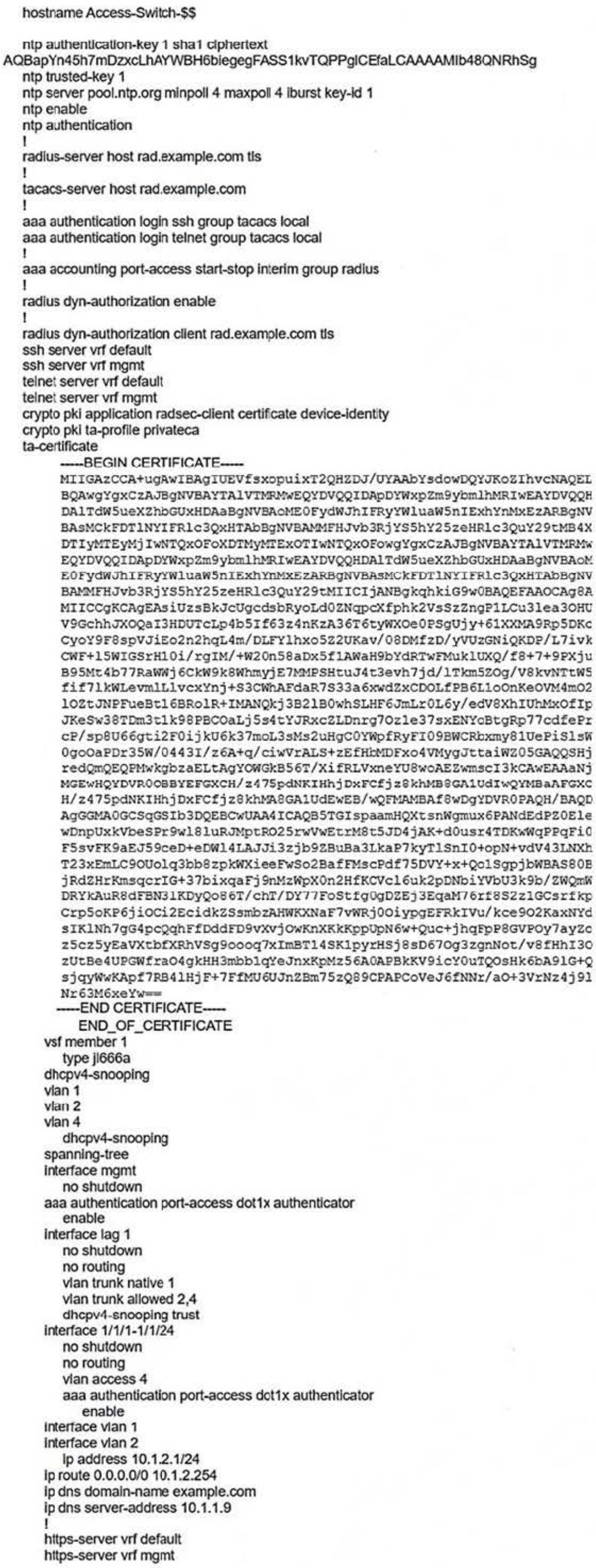
https://www.pass4itsure.com/hpe6-a84.html

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

QUESTION 1

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+15WIGSrH10i/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
      DRYkAuR8dFBN31KDyQo86T/chT/DY77FoStfg0gDZEj3EqaM76rf8S2z1GCsrfkp
      Crp5oKP6jiOCi2EcidkZSsmbzAHWKXNaF7vWRj0OiypgEFRkIVu/kce9O2KaxNYd
      sIKlNh7gG4pcQqhFfDddFD9vXvjOwKnXKkKppUpN6w+Quc+jhqFpP8GVPOy7ayZc
      z5cz5yEaVXtbfXRhVSg9oooq7xImBT14SK1pyrHSj8sD67Og3zgnNot/v8fHhI3O
      zUtBe4UPGWfraO4gkHH3mbb1qYeJnxKpMz56A0APBkKV9icY0uTQOsHk6bA91G+Q
      sjqyWwKApf7RB41HjF+7FfMU6UJnZBm75zQ89CPAPCoVeJ6fNNr/aO+3VrNz4j91
      Nr63M6xeYw==
     -----END CERTIFICATE-----
        END_OF_CERTIFICATE
    vsf member 1
      type jl666a
    dhcpv4-snooping
    vlan 1
    vlan 2
    vlan 4
      dhcpv4-snooping
    spanning-tree
    interface mgmt
      no shutdown
    aaa authentication port-access dot1x authenticator
      enable
    interface lag 1
      no shutdown
      no routing
      vlan trunk native 1
      vlan trunk allowed 2,4
      dhcpv4-snooping trust
    interface 1/1/1-1/1/24
      no shutdown
      no routing
      vlan access 4
      aaa authentication port-access dot1x authenticator
        enable
    interface vlan 1
    interface vlan 2
      ip address 10.1.2.1/24
    ip route 0.0.0.0/0 10.1.2.254
    ip dns domain-name example.com
    ip dns server-address 10.1.1.9
    !
    https-server vrf default
    https-server vrf mgmt
```

What is one immediate remediation that you should recommend?

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

Correct Answer: D

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-ofservice 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 2

Refer to the scenario.

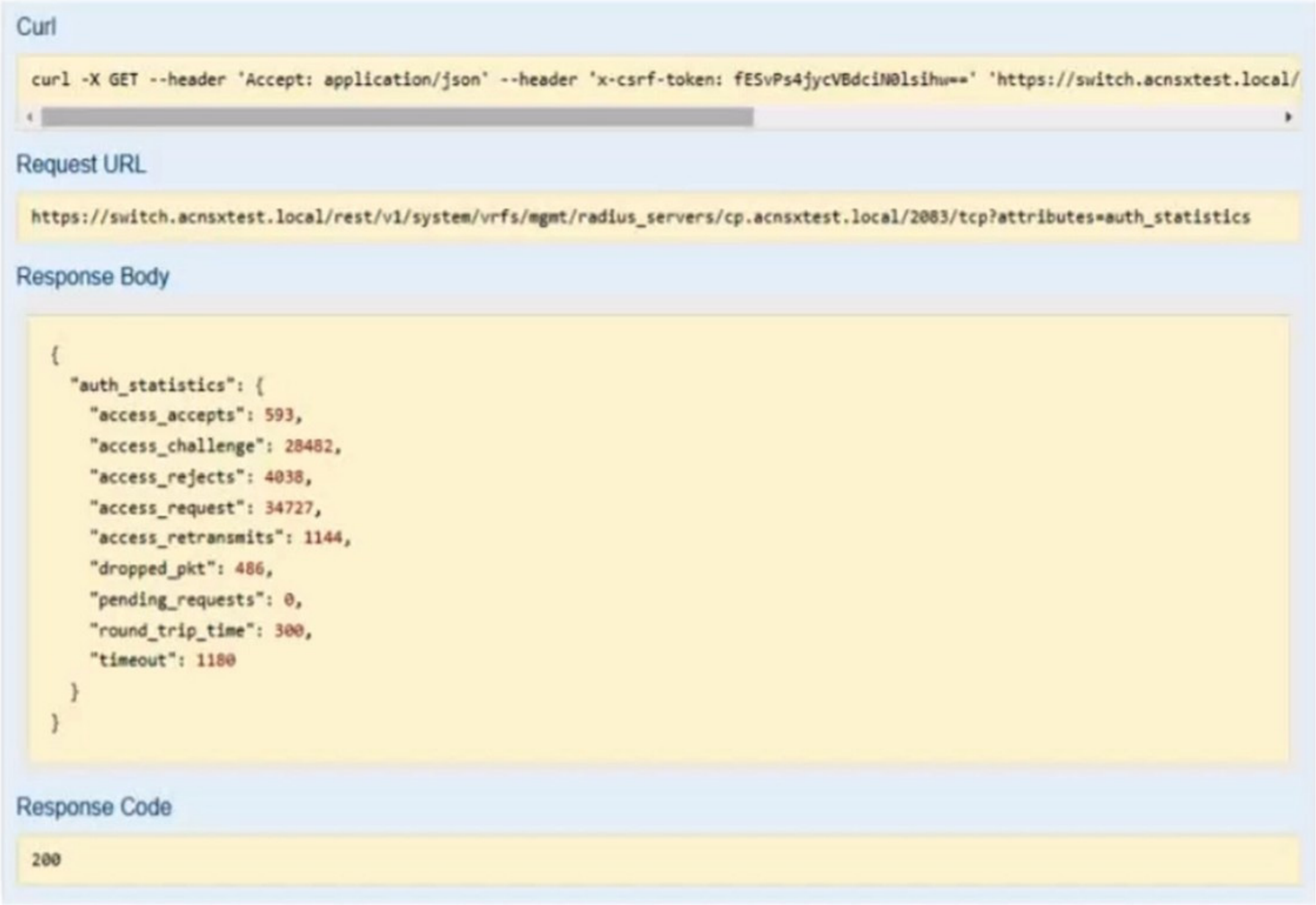
An organization wants the AOS-CX switch to trigger an alert if its RADIUS server (cp.acnsxtest.local) rejects an unusual number of client authentication requests per hour. After some discussions with other Aruba admins, you are still not sure

how many rejections are usual or unusual. You expect that the value could be different on each switch.

You are helping the developer understand how to develop an NAE script for this use case.

You are helping the developer find the right URI for the monitor.

Refer to the exhibit.



Curl

```
curl -X GET --header 'Accept: application/json' --header 'x-csrf-token: fESvPs4jycVBdciN0lsihw==' 'https://switch.acnsxtest.local/
```

Request URL

```
https://switch.acnsxtest.local/rest/v1/system/vrfs/mgmt/radius_servers/cp.acnsxtest.local/2083/tcp?attributes=auth_statistics
```

Response Body

```
{
  "auth_statistics": {
    "access_accepts": 593,
    "access_challenge": 28482,
    "access_rejects": 4038,
    "access_request": 34727,
    "access_retransmits": 1144,
    "dropped_pkt": 486,
    "pending_requests": 0,
    "round_trip_time": 300,
    "timeout": 1180
  }
}
```

Response Code

```
200
```

You have used the REST API reference interface to submit a test call. The results are shown in the exhibit.

Which URI should you give to the developer?

A. /rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs

B. /rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs?attributes=access_rejects

C. /rest/v1/system/vrfs/mgmt/radius/_servers/cp.acnsxtest.local/2083/tcp

D. /rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs.access_rejects

Correct Answer: D

This is because this URI specifies the exact attribute that contains the number of access rejects from the RADIUS server, which is the information that the NAE script needs to monitor and trigger an alert.

A.

/rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs. This is not the correct URI because it returns the entire authstatistics object, which contains more information than the access rejects, such as

access accepts, challenges, timeouts, etc. This might make the NAE script more complex and inefficient to parse and process the data.

B.

/rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs?attributes=access_rejects. This is not a valid URI because it has two question marks, which is a syntax error. The question mark is used to

indicate the start of the query string, which can have one or more parameters separated by ampersands. The correct way to specify multiple attributes is to use a comma-separated list after the question mark, such as ?

attributes=attr1,attr2,attr3.

C. /rest/v1/system/vrfs/mgmt/radius/_servers/cp.acnsxtest.local/2083/tcp. This is not a valid URI because it has an extra underscore before servers, which is a typo. The correct resource name is servers, not _servers. Moreover, this URI does

not specify any attributes, which means it will return the default attributes of the RADIUS server object, such as name, port, protocol, etc., but not the authstatistics or access_rejects.

QUESTION 3

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 MAC-Auth fallback.

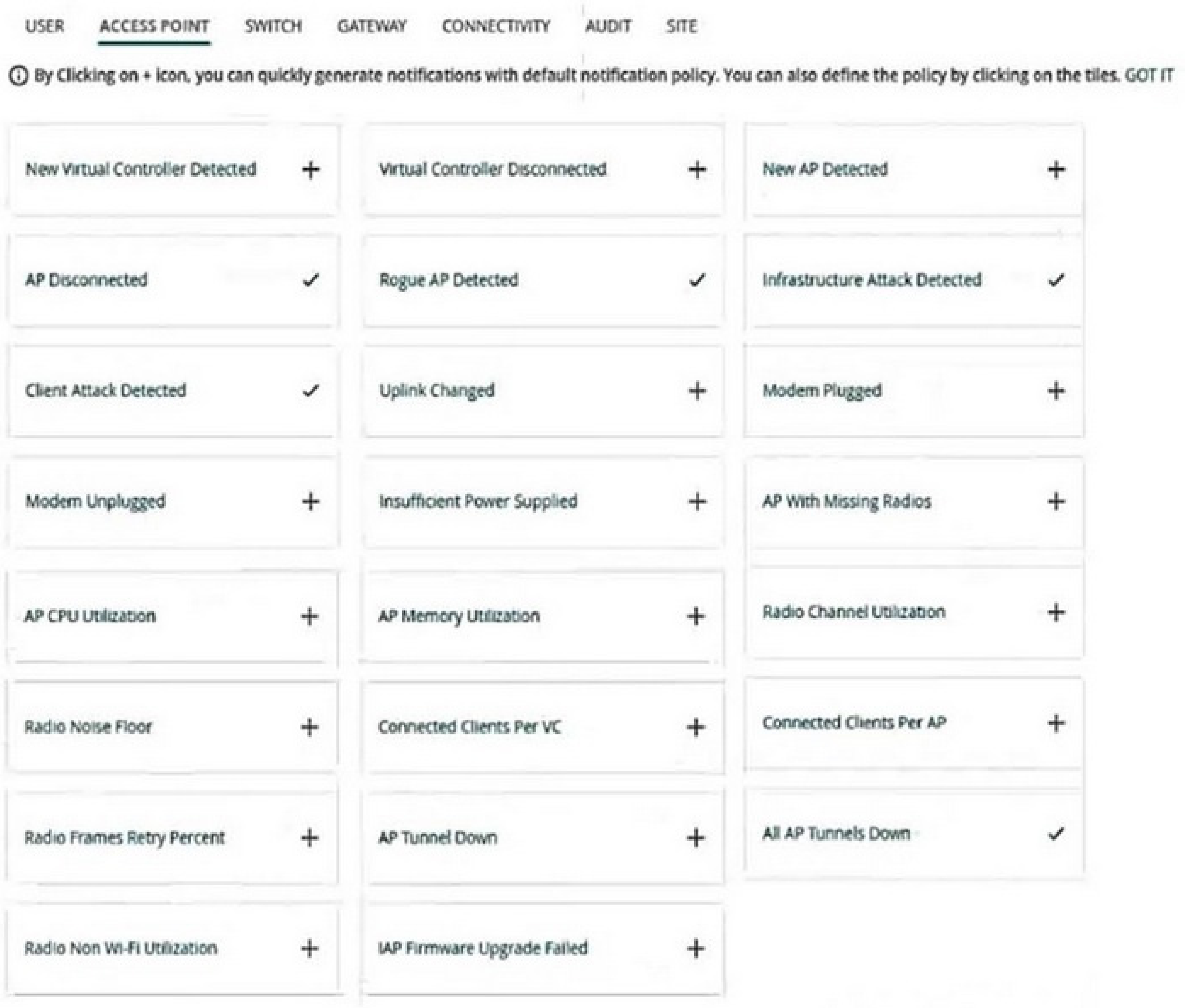
D. Enable dynamic authorization (RFC 3576) in the AAA profile for the devices.

Correct Answer: A

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 4

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	+	New AP Detected	+
AP Disconnected	✓	Rogue AP Detected	✓	Infrastructure Attack Detected	✓
Client Attack Detected	✓	Uplink Changed	+	Modem Plugged	+
Modem Unplugged	+	Insufficient Power Supplied	+	AP With Missing Radios	+
AP CPU Utilization	+	AP Memory Utilization	+	Radio Channel Utilization	+
Radio Noise Floor	+	Connected Clients Per VC	+	Connected Clients Per AP	+
Radio Frames Retry Percent	+	AP Tunnel Down	+	All AP Tunnels 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

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 5

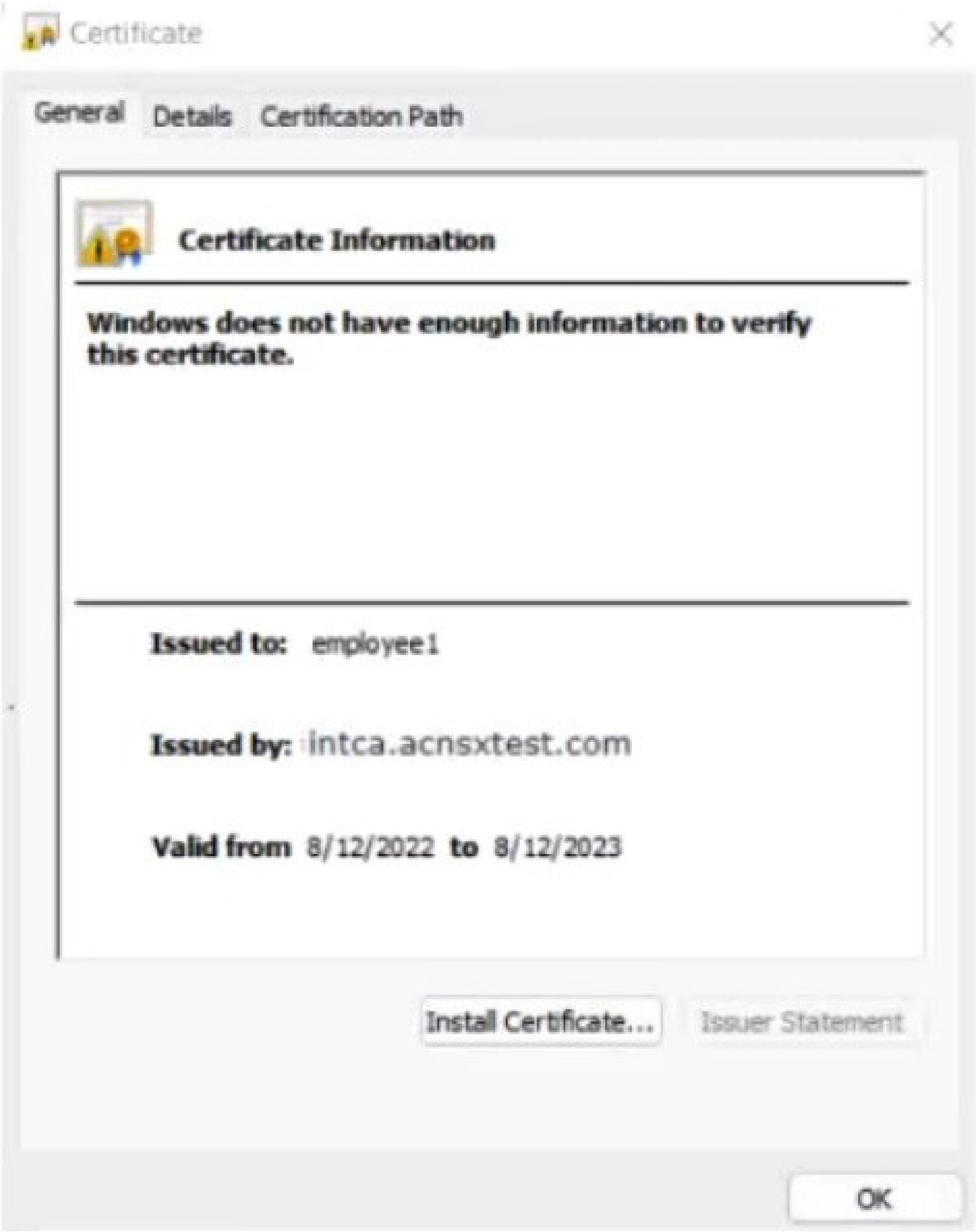
Refer to the scenario.

# Introduction to the customer

You are helping a company add Aruba ClearPass to their network, which uses Aruba network infrastructure devices.

The company currently has a Windows domain and Windows CA. The Window CA issues certificates to domain computers, domain users, and servers such as domain controllers. An example of a certificate issued by the Windows CA is

shown here.



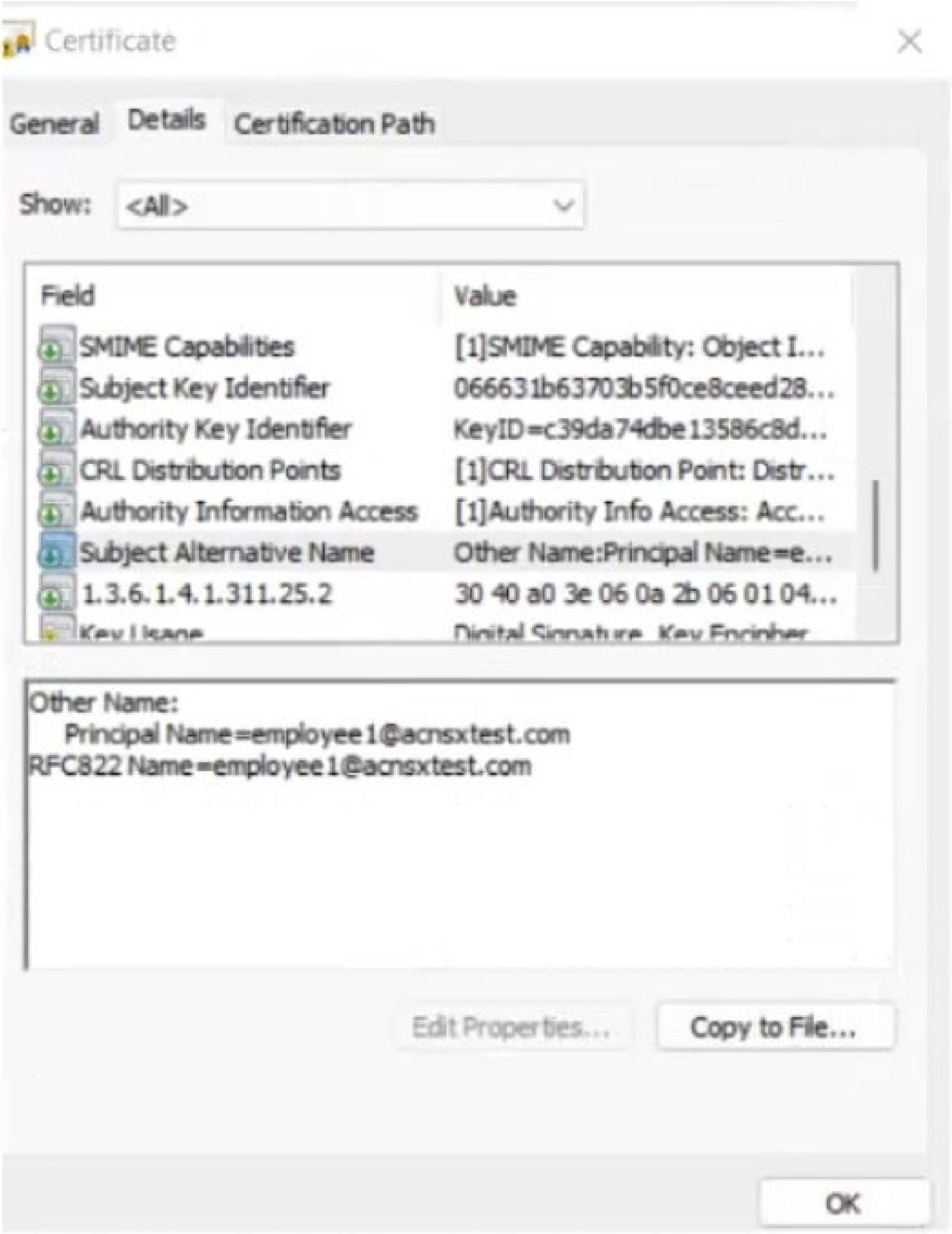
Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: employee1

Issued by: intca.acnsxtest.com

Valid from 8/12/2022 to 8/12/2023



Field	Value
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	066631b63703b5f0ce8ceed28...
Authority Key Identifier	KeyID=c39da74dbe13586c8d...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=e...
1.3.6.1.4.1.311.25.2	30 40 a0 3e 06 0a 2b 06 01 04...
Key Usage	Digital Signature, Key Encipher

```
Other Name:
    Principal Name=employee1@acnsxtest.com
RFC822 Name=employee1@acnsxtest.com
```

The company is in the process of adding Microsoft Endpoint Manager (Intune) to manage its mobile clients. The customer is maintaining the on-prem AD for now and uses Azure AD Connect to sync with Azure AD.

# Requirements for issuing certificates to mobile clients

The company wants to use ClearPass Onboard to deploy certificates automatically to mobile clients enrolled in Intune. During this process, Onboard should communicate with Azure AD to validate the clients. High availability should also be

provided for this scenario; in other words, clients should be able to get certificates from Subscriber 2 if Subscriber 1 is down.

The Intune admins intend to create certificate profiles that include a UPN SAN with the UPN of the user who enrolled the device.

# Requirements for authenticating clients

The customer requires all types of clients to connect and authenticate on the same corporate SSID.

The company wants CPPM to use these authentication methods:

1.

EAP-TLS to authenticate users on mobile clients registered in Intune

2.

TEAR, with EAP-TLS as the inner method to authenticate Windows domain computers and the users on them To succeed, EAP-TLS (standalone or as a TEAP method) clients must meet these requirements:

1.

Their certificate is valid and is not revoked, as validated by OCSP

2.

The client\\'s username matches an account in AD # Requirements for assigning clients to roles After authentication, the customer wants the CPPM to assign clients to ClearPass roles based on the following rules:

1.

Clients with certificates issued by Onboard are assigned the "mobile-onboarded" role

2.

Clients that have passed TEAP Method 1 are assigned the "domain-computer" role

3.

Clients in the AD group "Medical" are assigned the "medical-staff" role

4.

Clients in the AD group "Reception" are assigned to the "reception-staff" role The customer requires CPPM to assign authenticated clients to AOS firewall roles as follows:

1.

Assign medical staff on mobile-onboarded clients to the "medical-mobile" firewall role

2.

Assign other mobile-onboarded clients to the "mobile-other" firewall role

3.

Assign medical staff on domain computers to the "medical-domain" firewall role

4.

All reception staff on domain computers to the "reception-domain" firewall role

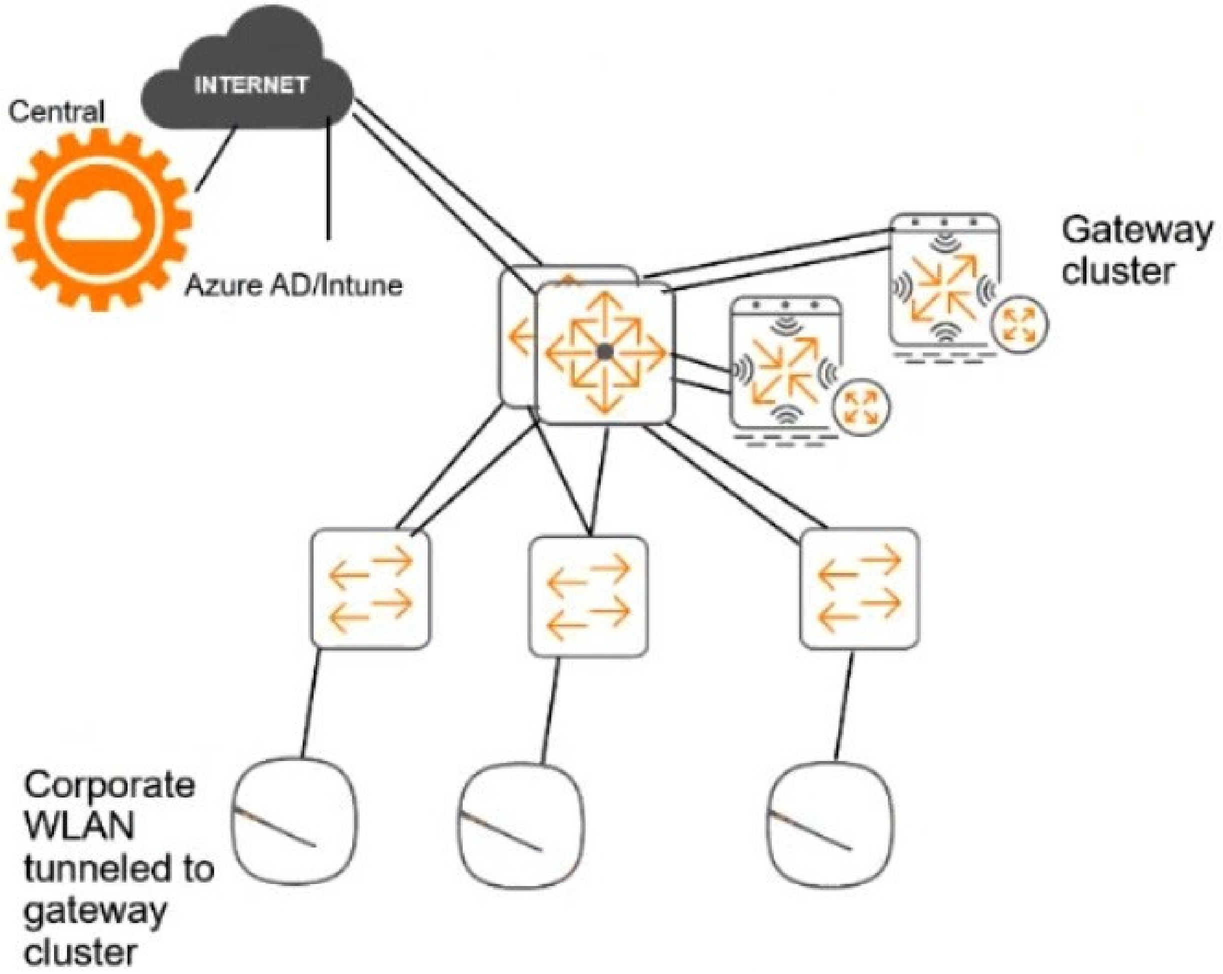
5.

All domain computers with no valid user logged in to the "computer-only" firewall role

6.

Deny other clients access # Other requirements Communications between ClearPass servers and on-prem AD domain controllers must be encrypted. # Network topology For the network infrastructure, this customer has Aruba APs and Aruba gateways, which are managed by Central. APs use tunneled WLANs, which tunnel traffic to the gateway cluster. The customer also has AOS-CX switches that are not

managed by Central at this point.



# ClearPass cluster IP addressing and hostnames A customer\\'s ClearPass cluster has these IP addresses:

1.

Publisher = 10.47.47.5

2.

Subscriber 1 = 10.47.47.6

3.

Subscriber 2 = 10.47.47.7

4.

Virtual IP with Subscriber 1 and Subscriber 2 = 10.47.47.8

The customer\\'s DNS server has these entries

1.

cp.acnsxtest.com = 10.47.47.5

2.

cps1.acnsxtest.com = 10.47.47.6

3.

cps2.acnsxtest.com = 10.47.47.7

4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

The customer has now decided that it needs CPPM to assign certain mobile-onboarded devices to a "nurse-call" AOS user role. These are mobile-onboarded devices that are communicating with IP address 10.1.18.12 using port 4343.

What are the prerequisites for fulfilling this requirement?

A. Setting up traffic classes and role mapping rules within Central\\'s global settings

B. Creating server-based role assignment rules on APs that apply roles to clients based on traffic destinations

C. Creating server-based role assignment rules on gateways that apply roles to clients based on traffic destinations

D. Creating a tag on Central to select the proper destination connection and integrating CPPM with Device Insight

Correct Answer: C