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.geekcert.com/hpe6-a84.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

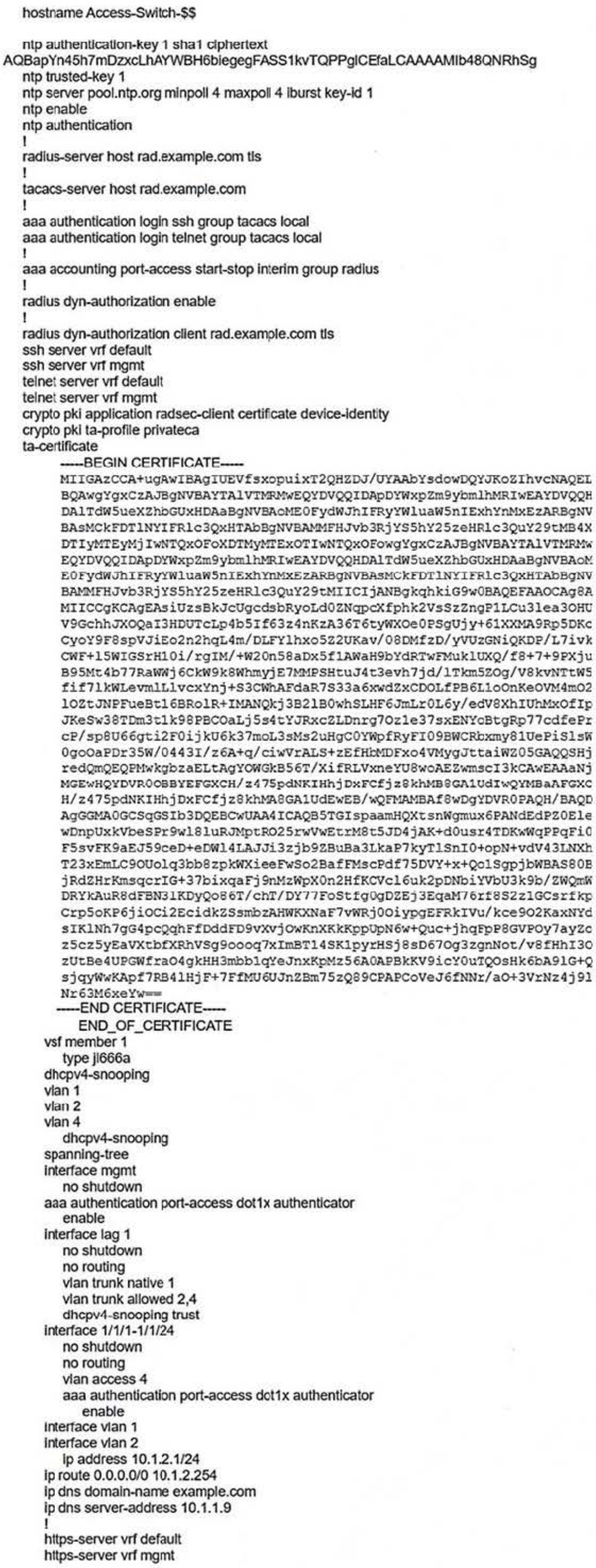
Correct Answer: B

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-torole 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 2

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+15WIGSrH10i/rgIM/+W20n58aDx5f1AWaH9bYdRTwFMuklUXQ/f8+7+9PXju
      B95Mt4b77RaWWj6CkW9k8WhmyjE7MMPSHtuJ4t3evh7jd/1Tkm5ZOg/V8kvNTtW5
      fif7lkWLevmlLlvcxYnj+S3CWhAFdaR7S33a6xwdZxCDOLfPB6L1oOnKeOVM4mO2
      lOZtJNPFueBt16BRolR+IMANQkj3B2lB0whSLHF6JmLr0L6y/edV8XhIUhMxOfIp
      JKeSw38TDm3t1k98PBCOaLj5s4tYJRxcZLDnrg7Oz1e37sxENYcBtgRp77cdfePr
      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+3VrNz4j9l
      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 3

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.

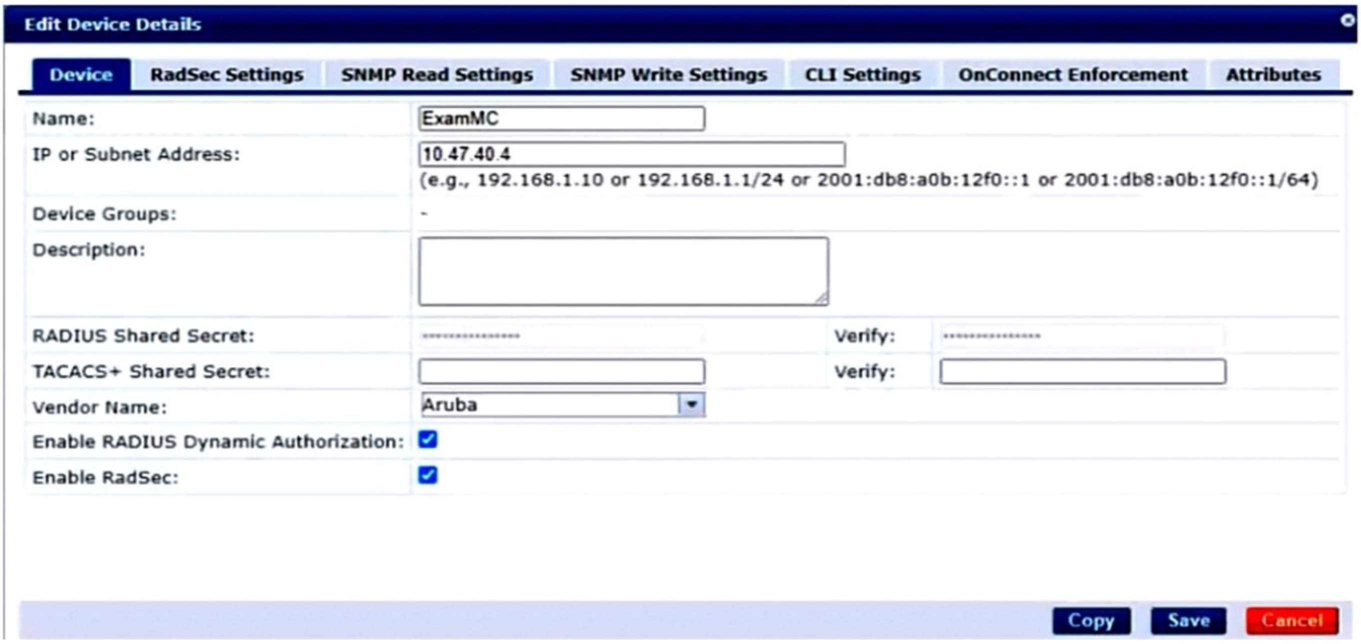
D. Use the Endpoint type for the rule conditions; no extra authorization source is required for services that use policies with these rules.

Correct Answer: D

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 4

A company has an Aruba ClearPass server at 10.47.47.8, FQDN radius.acnsxtest.local. This exhibit shows ClearPass Policy Manager\\'s (CPPM\\'s) settings for an Aruba Mobility Controller (MC).



Name: ExamMC

IP or Subnet Address: 10.47.40.4
(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)

Device Groups: -

Description:

RADIUS Shared Secret: ••••••••••••••• Verify: •••••••••••••••

TACACS+ Shared Secret: Verify:

Vendor Name: Aruba

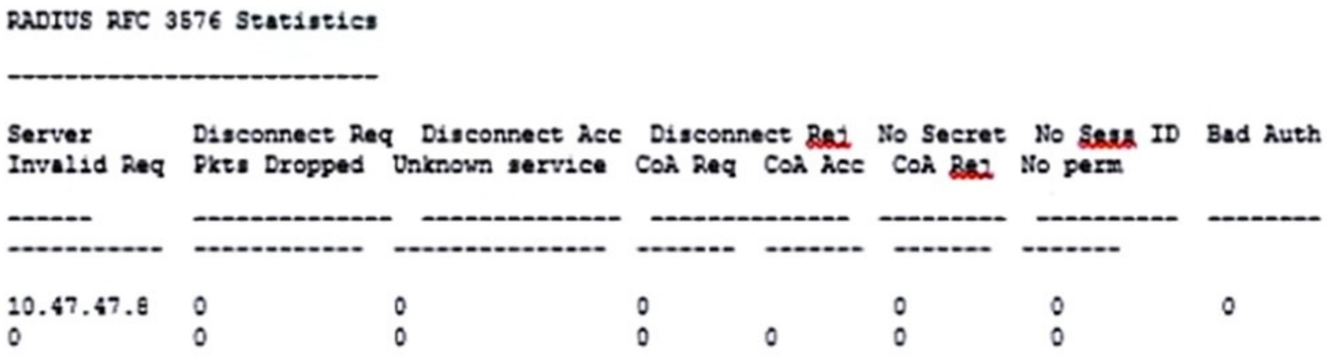
Enable RADIUS Dynamic Authorization: ☑

Enable RadSec: ☑

The MC is already configured with RADIUS authentication settings for CPPM, and RADIUS requests between the MC and CPPM are working. A network admin enters and commits this command to enable dynamic authorization on the MC:

aaa rfc-3576-server 10.47.47.8

But when CPPM sends CoA requests to the MC, they are not working. This exhibit shows the RFC 3576 server statistics on the MC:



```
RADIUS RFC 3576 Statistics
--------------------------

Server       Disconnect Req  Disconnect Acc  Disconnect Rej  No Secret  No Sess ID  Bad Auth
Invalid Req  Pkts Dropped  Unknown service  CoA Req  CoA Acc  CoA Rej  No perm

------       --------------  --------------  --------------  ---------  ----------  ---------
-----------  ------------  ---------------  -------  -------  -------  -------

10.47.47.8   0               0               0               0          0           0
0            0             0                0        0        0        0
```

How could you fix this issue?

A. Change the UDP port in the MCs\\' RFC 3576 server config to 3799.

B. Enable RadSec on the MCs\\' RFC 3676 server config.

C. Configure the MC to obtain the time from a valid NTP server.

D. Make sure that CPPM is using an ArubaOS Wireless RADIUS CoA enforcement profile.

Correct Answer: A

Dynamic authorization is a feature that allows CPPM to send change of authorization (CoA) or disconnect messages to the MC to modify or terminate a user session based on certain conditions or events 1. Dynamic authorization uses the RFC 3576 protocol, which is an extension of the RADIUS protocol 2. To enable dynamic authorization on the MC, you need to configure the IP address and UDP port of the CPPM server as the RFC 3576 server on the MC 3. The default UDP port for RFC 3576 is 3799, but it can be changed on the CPPM server . The MC and CPPM must use the same UDP port for dynamic authorization to work properly 3. In this scenario, the MC is configured with the IP address of the CPPM server (10.47.47.8) as the RFC 3576 server, but it is using the default UDP port of 3799. However, according to the exhibit, the CPPM server is using a different UDP port of 1700 for dynamic authorization . This mismatch causes the CoA requests from CPPM to fail on the MC, as shown by the statistics . To fix this issue, you need to change the UDP port in the MCs\\' RFC 3576 server config to match the UDP port used by CPPM, which is 1700 in this case. Alternatively, you can change the UDP port in CPPM to match the default UDP port of 3799 on the MC. Either way, you need to ensure that both devices use the same UDP port for dynamic authorization .

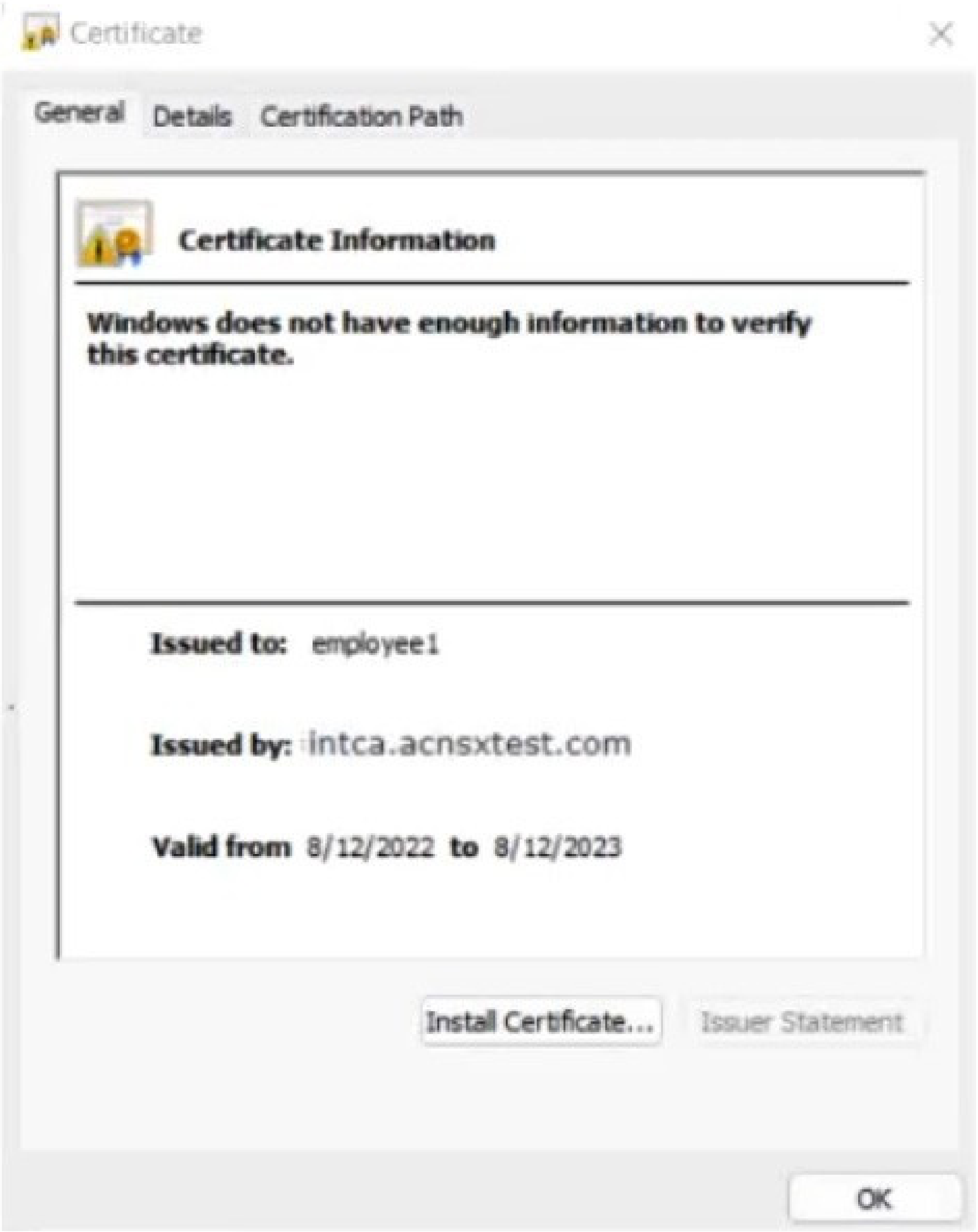
QUESTION 5

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.



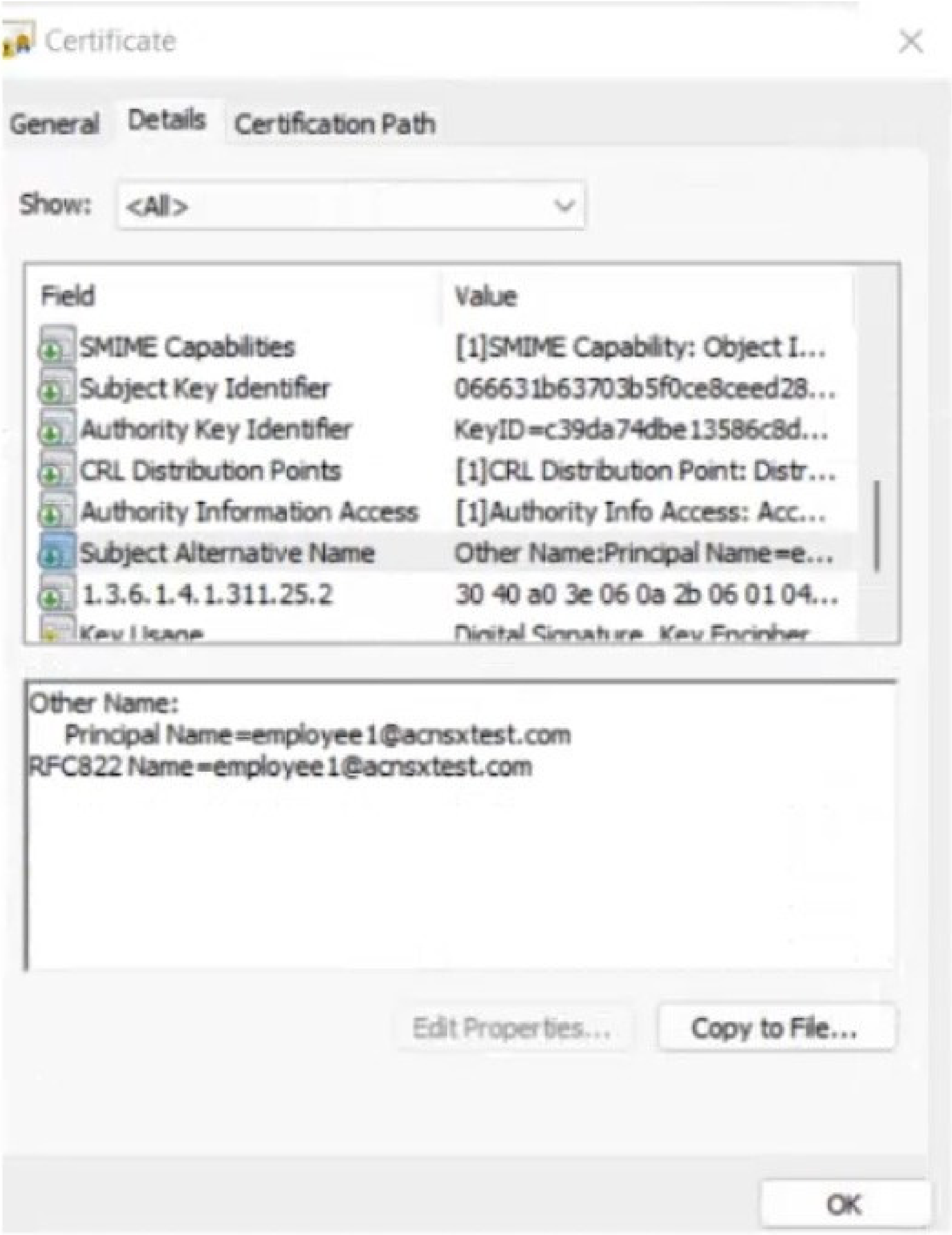
Certificate Information

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



Show: <All>

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

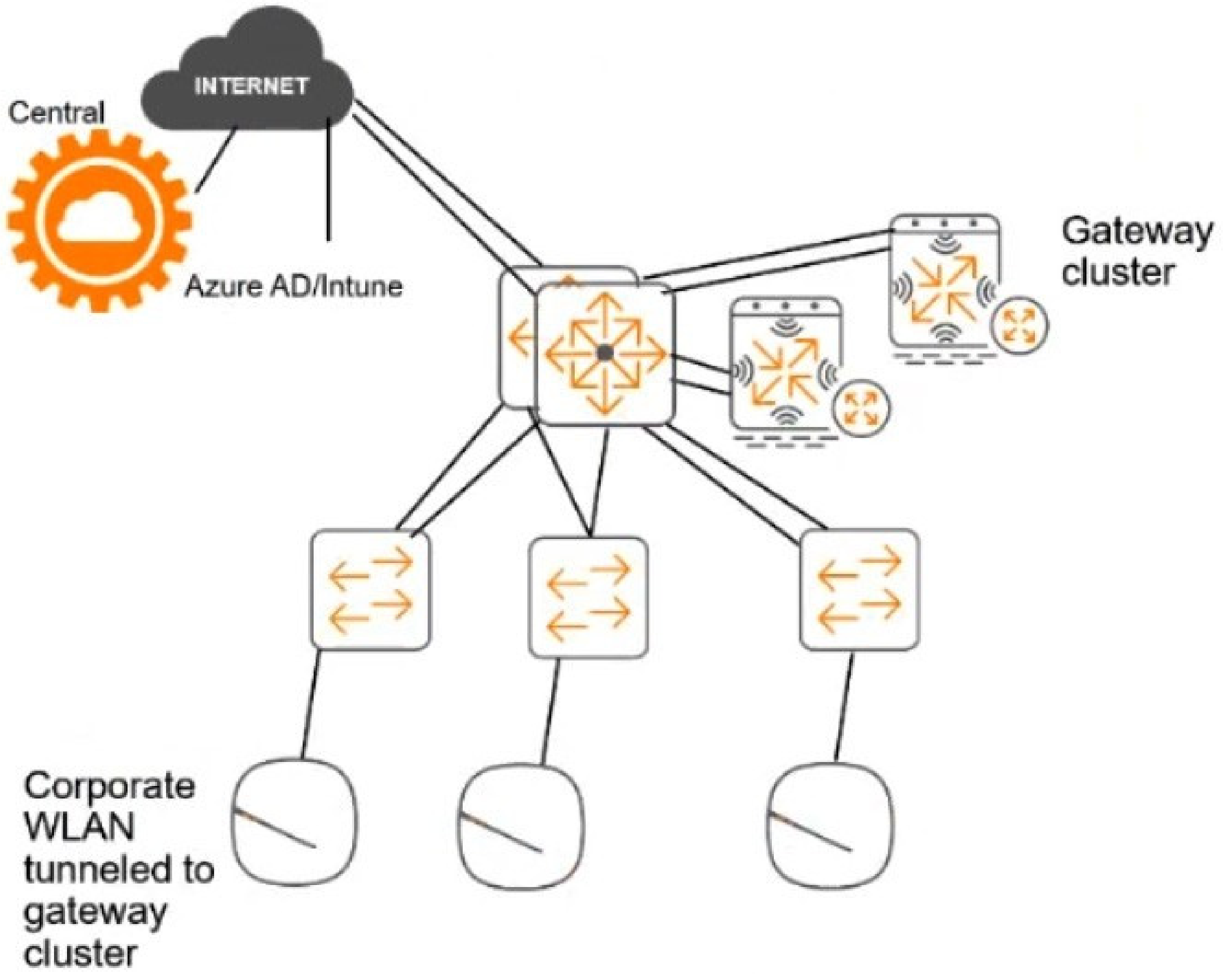
5.

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

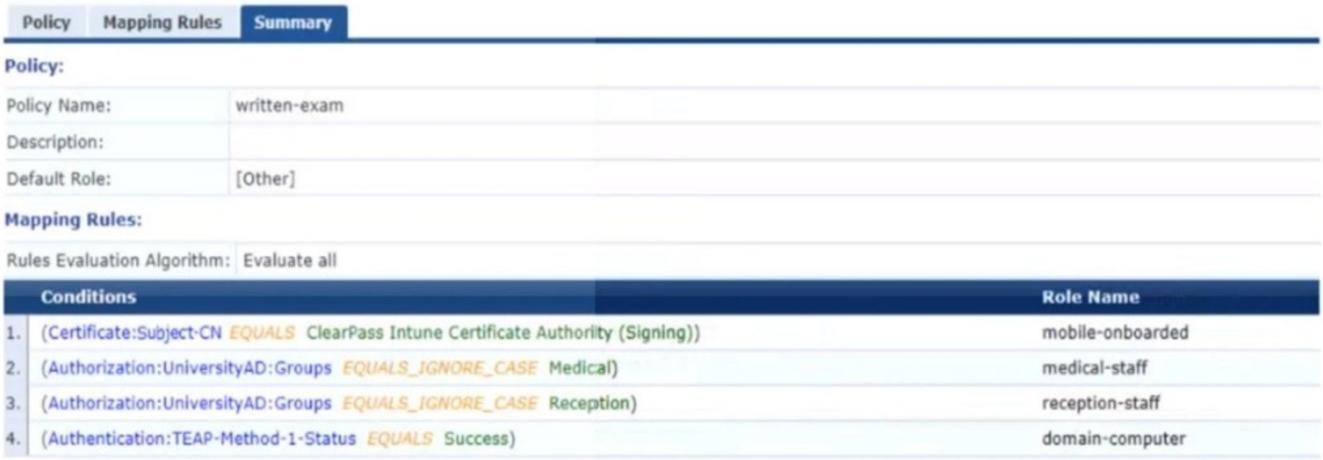
4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

You have created a role mapping policy as shown in the exhibits below.



Policy:

Policy Name:	written-exam
Description:	
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm:	Evaluate all

	Conditions	Role Name
1.	(Certificate:Subject-CN EQUALS ClearPass Intune Certificate Authority (Signing))	mobile-onboarded
2.	(Authorization:UniversityAD:Groups EQUALS_IGNORE_CASE Medical)	medical-staff
3.	(Authorization:UniversityAD:Groups EQUALS_IGNORE_CASE Reception)	reception-staff
4.	(Authentication:TEAP-Method-1-Status EQUALS Success)	domain-computer

What is one change that you need to make to this policy?

A. In rule 1 change Subject-CN to Issuer-CN.

B. Move rules 2 and 3 to the top of the list.

C. Change the rules evaluation mechanism to first applicable.

D. Change the default role to \\'mobile-onboarded*

Correct Answer: A