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

100% Passing Guarantee
100% Money Back Assurance

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

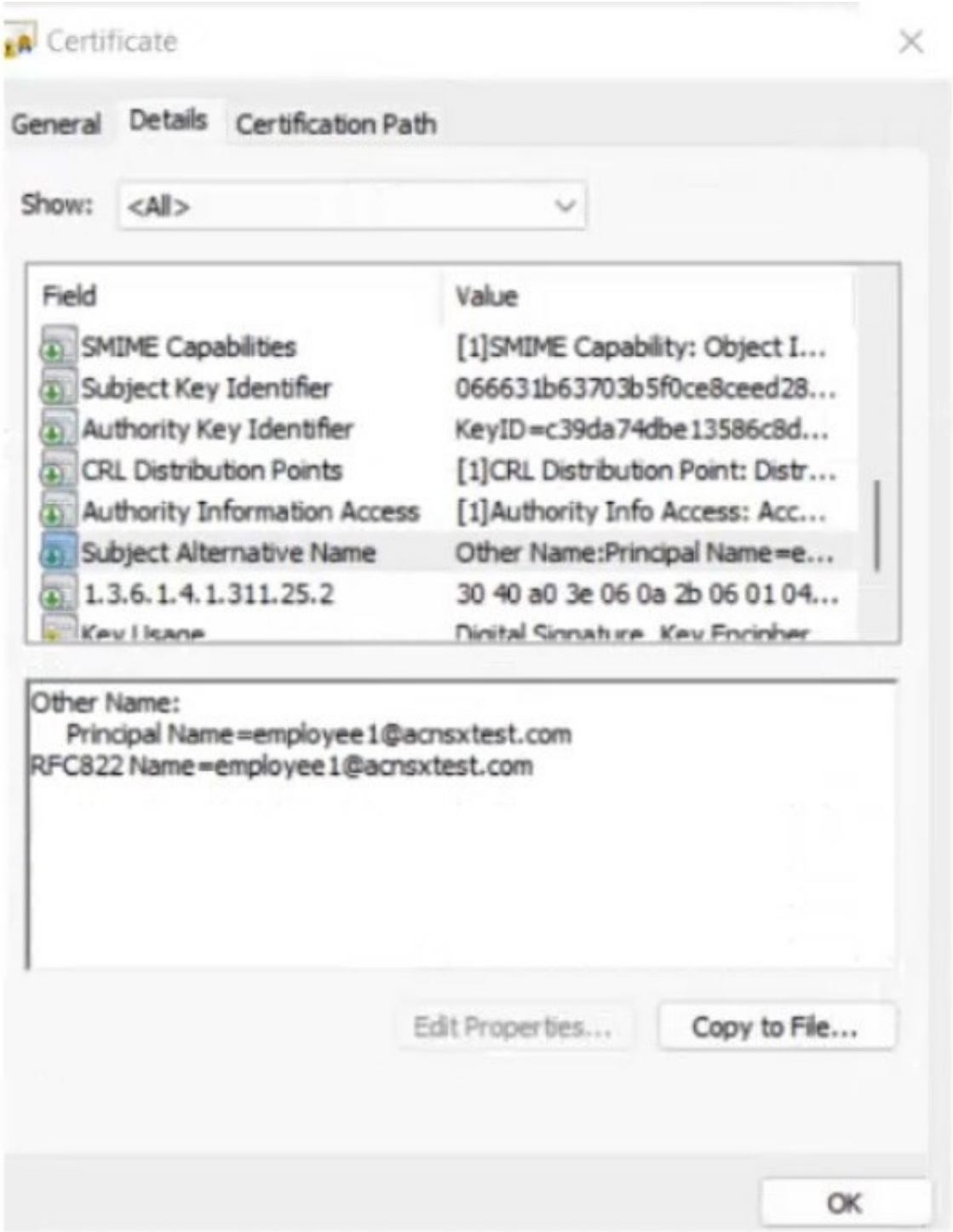
QUESTION 1

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.



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

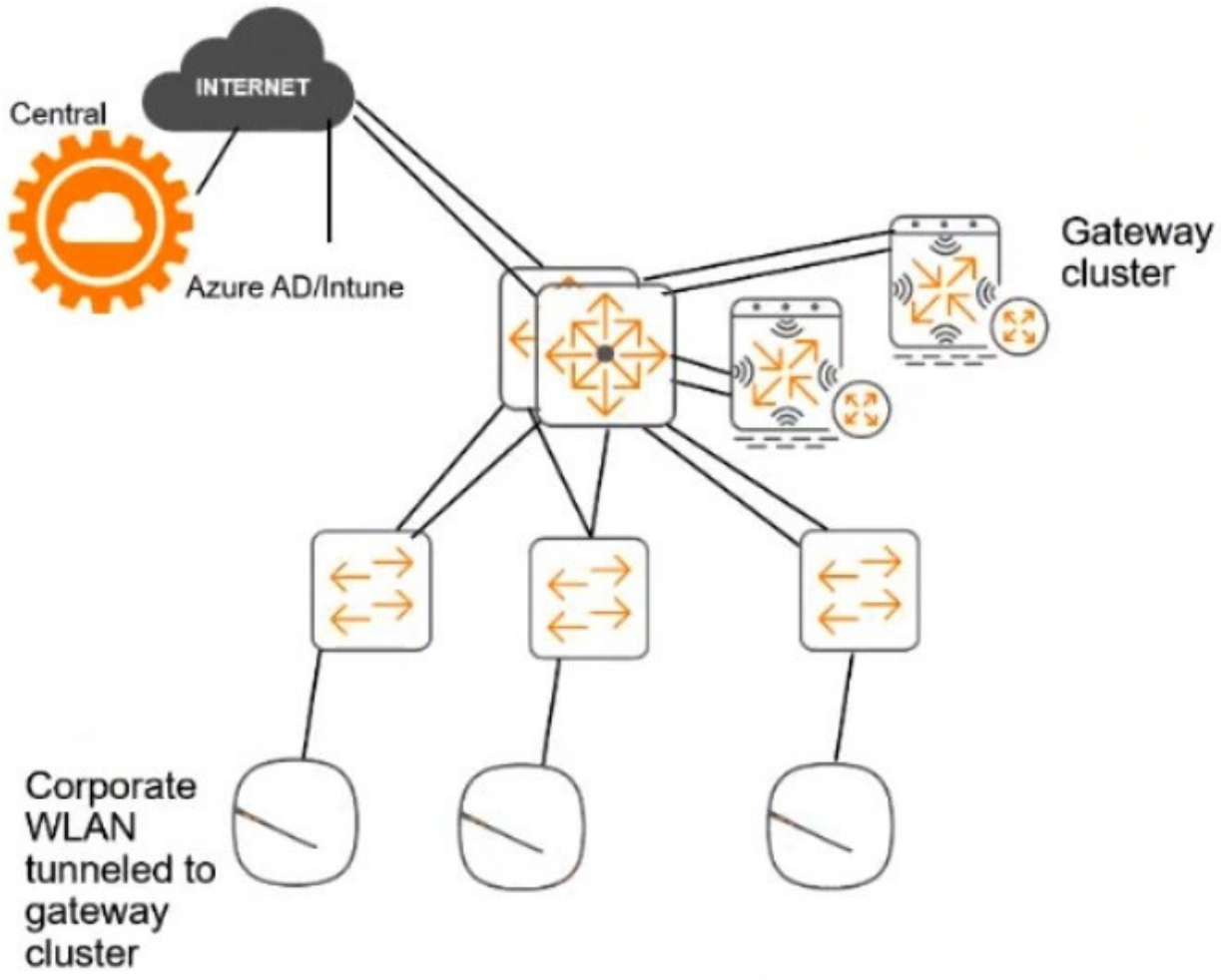
5.

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 imported the root certificate for the Windows CA to the ClearPass CA Trust list.

Which usages should you add to it based on the scenario requirements?

A. EAP and AD/LDAP Server

B. LDAP and Aruba infrastructure

C. Radsec and Aruba infrastructure

D. EAP and Radsec

Correct Answer: A

QUESTION 2

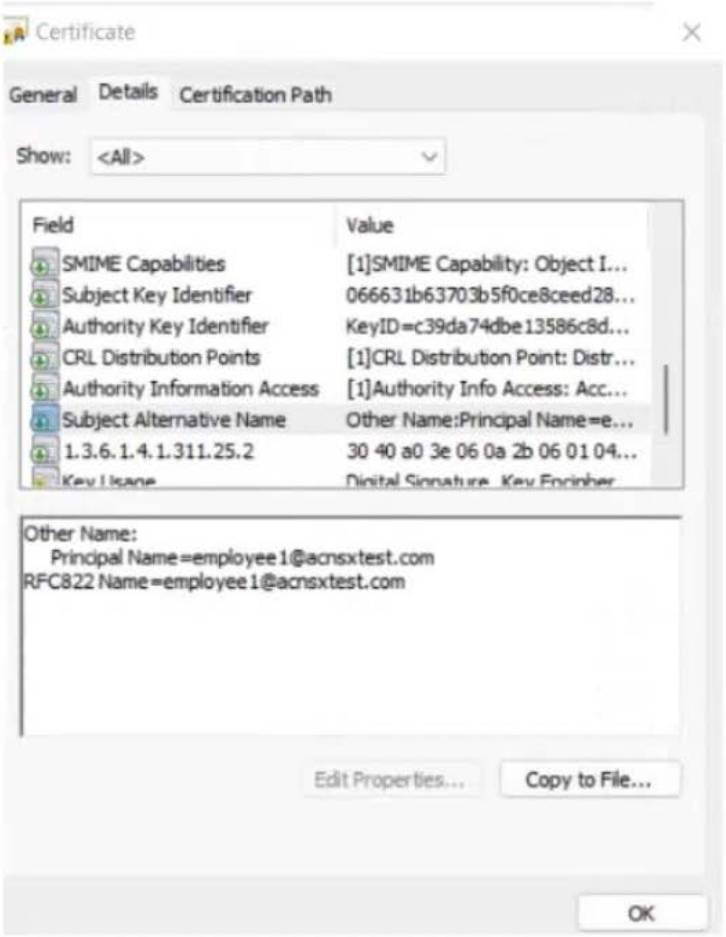
Refer to the scenario.

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
General
Details
Certification Path
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
Install Certificate...
Issuer Statement
OK


Certificate
General
Details
Certification Path
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...
Other Name:
Principal Name=employee1@acnsxtest.com
RFC822 Name=employee1@acnsxtest.com
Edit Properties...
Copy to File...
OK

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.

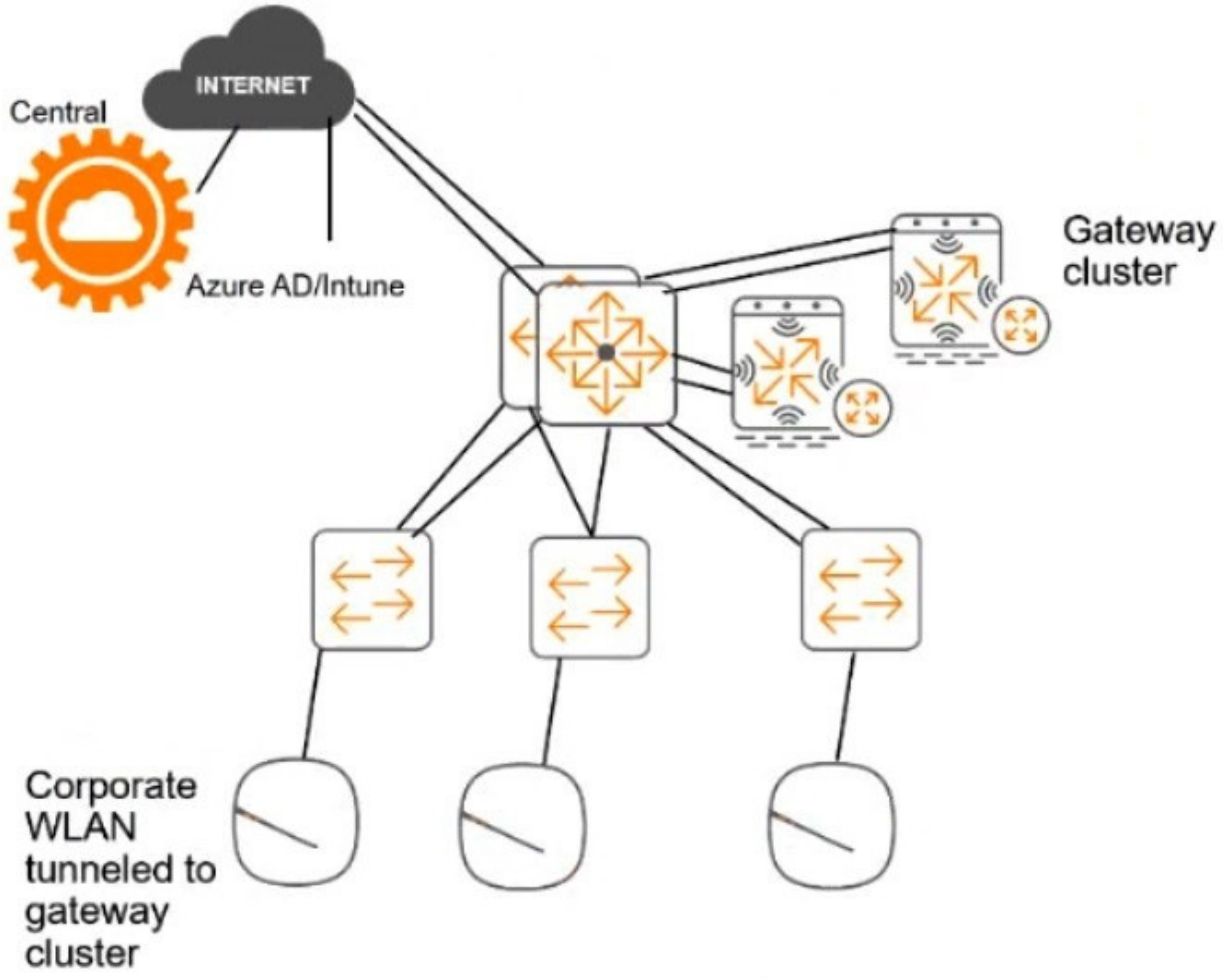
Deny other clients access

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 started to create a CA to meet the customer\\'s requirements for issuing certificates to mobile clients, as shown in the exhibit below.


Certificate Authority Settings
* Name: Exam Onboard CA
Enter a name to identify this certificate authority.
Description: This CA issues certificates to devices registered with Intune
A description of the certificate authority.
Mode: Root CA
Certificate Issuing
These options control how certificates are issued by this certificate authority.
* Authority Info Access: Do not include OCSP Responder URL
Select the information about the certificate authority to include in the client certificate.
Note that when an OCSP URL is provided, clients may need to access this URL in order to determine if the certificate is still valid.
* Validity Period: 365 days
Maximum validity period for client certificates (in days).
* Clock Skew Allowance: 15
Amount to pre/post date certificate validity period (in minutes).
Subject Alternative Name: Include device information in TLS client certificates
Store information about the device in the subjectAltName extension of the certificate.
Note: Aruba OS version 6.1 or later is required to enable this feature.
* Digest Algorithm: SHA-512
Select the algorithm used to sign issued certificates.
Retention Policy
These options control how long to retain certificates after revocation or expiry.
Store Certificates: Keep a copy of client certificates
When checked issued certificates will be stored. When unchecked, only metadata about the certificate will be retained.
Maximum Period: 2 weeks
The period after which an expired certificate (or a rejected request) will be automatically deleted.
Leave blank to disable automatic deletion.
SCEP Server
These options control access to the SCEP server for this CA.
SCEP Server: Enable access to the SCEP server
Allows this CA to issue tls-client certificates via SCEP
SCEP URL: http://clearpass1.acnsxtest.com/onboard/mdps_scep.php/2
* SCEP Validation: External Validator
Select the method by which the SCEP request is validated.
* External SCEP Validator: Intune SCEP 7c0a5261-8e52-41dd-a62d-6eab496b78d8
Select the extension with which to validate SCEP.
Allowed Access:
Enter the IP addresses and networks from which logins are permitted.
Denied Access:
Enter the IP addresses and networks that are denied login access.
EST Server
These options control access to the EST server for this CA.
EST Server: Enable access to the EST server
Allows this CA to issue tls-client certificates via EST
EST URL: https://cp1.acnsxtest.com/.well-known/est/ca:2
* EST Auth Method: HTTP Basic or Digest Authentication
Select the method to authenticate EST requests
EST Proof of Possession: Always verify Proof of Possession (POP)
Requires the EST server to verify the client's proof-of-possession, which must be provided in the tls-unique data. Refer to RFC 7030 for further details.
Allowed Access:
Enter the IP addresses and networks from which logins are permitted.
Denied Access:
Enter the IP addresses and networks that are denied login access.
* EST Key Type: 2048-bit RSA
Select the type of private key that EST clients should generate.
* EST Digest Algorithm: SHA-256
Select the digest algorithm EST clients should use for CSRs.
Identity
Country: US
State: California
Locality: Sunnyvale
Organization: Aruba Networks Training
Organizational Unit: ACNSX Exam
Identity
Country: US
State: California
Locality: Sunnyvale
Organization: Aruba Networks Training
Organizational Unit: ACNSX Exam
Common Name: ClearPass Intune Certificate Authority
Signing Common Name: ClearPass Intune Certificate Authority (Signing)
Email Address: admin@acnsxtest.com
Private Key
Key Type: 4096-bit RSA
Self-Signed Certificate
CA Expiration: 3653

What change will help to meet those requirements and the requirements for authenticating clients?

A. Change the EST authentication method to use an external validator.

B. Change the EST Digest Algorithm to SHA-512.

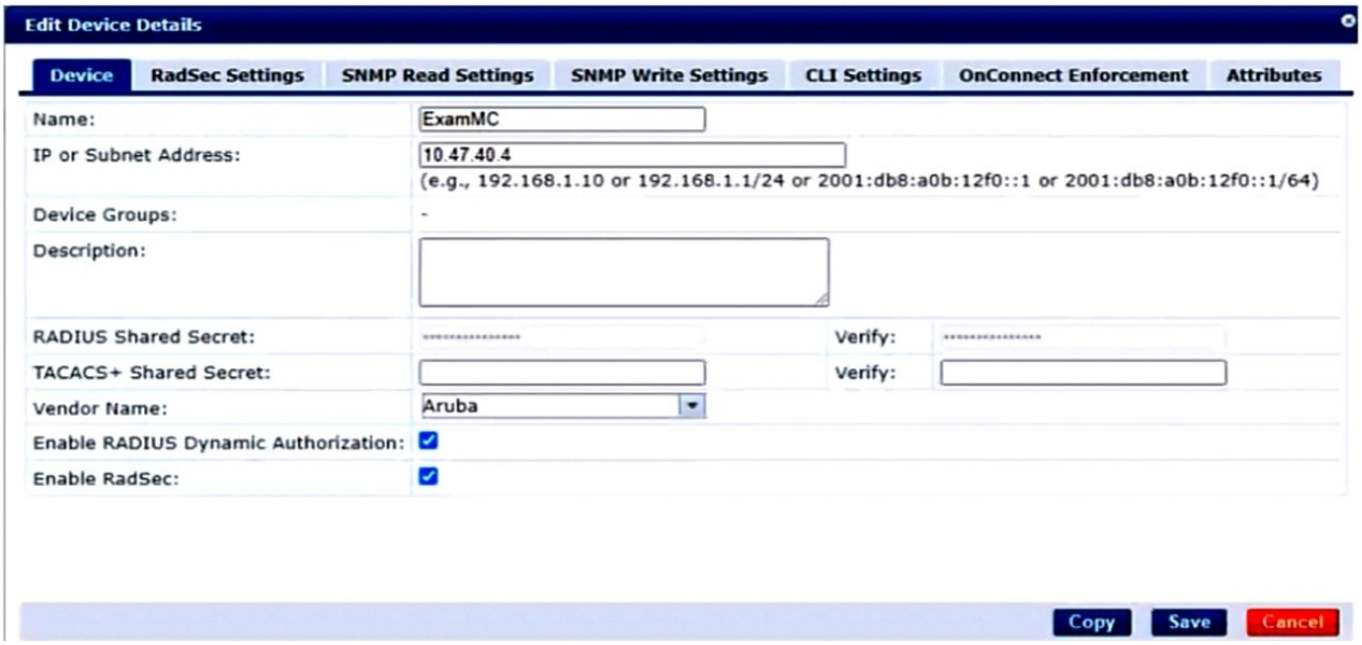
C. Recreate the CA as a registration authority under Azure AD.

D. Specify an OCSP responder, setting the hostname to localhost.

Correct Answer: A

QUESTION 3

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).



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.

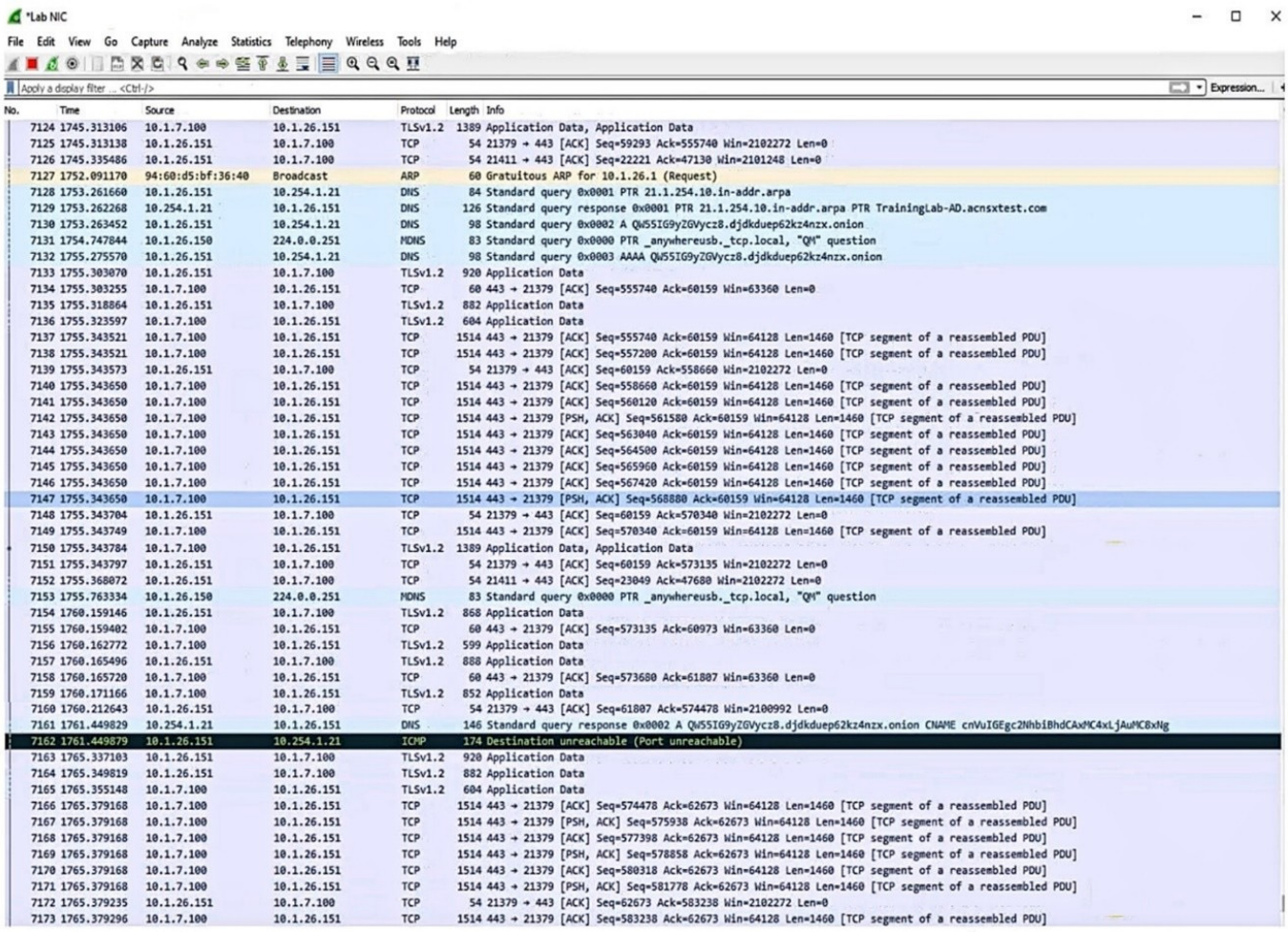
D. Make sure that CPPM is using an ArubaOS Wireless RADIUS CoA enforcement profile.

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 4

Refer to the exhibit.



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

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 0x2a0x2a0x2a0x2a0x2a0x2a0x2a0x2a.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 5

You are configuring gateway IDS/IPS settings in Aruba Central.

For which reason would you set the Fail Strategy to Bypass?

A. To permit traffic if the IPS engine falls to inspect It

B. To enable the gateway to honor the allowlist settings configured in IDS/IPS policies

C. To tell gateways to stop enforcing IDS/IPS policies if they lose connectivity to the Internet

D. To avoid wasting IPS engine resources on filtering traffic for unauthenticated clients

Correct Answer: A

The Fail Strategy is a configuration option for the IPS mode of inspection on Aruba gateways. It defines the action to be taken when the IPS engine crashes and cannot inspect the traffic. There are two possible options for the Fail Strategy: Bypass and Block1 If you set the Fail Strategy to Bypass, you are telling the gateway to allow the traffic to flow without inspection when the IPS engine fails. This option ensures that there is no disruption in the network connectivity, but it also exposes the network to potential threats that are not detected or prevented by the IPS engine1 If you set the Fail Strategy to Block, you are telling the gateway to stop the traffic flow until the IPS engine resumes inspection. This option ensures that there is no compromise in the network security, but it also causes a loss of network connectivity for the duration of the IPS engine failure1