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

Aruba Certified Network Security Expert Written

Pass HP HPE6-A84 Exam with 100% Guarantee

QUESTION 1

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:

1.

Subject: CN=mc41.site94.example.com

2.

No SANs

3.

Issuer: CN=ca41.example.com

4.

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

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.

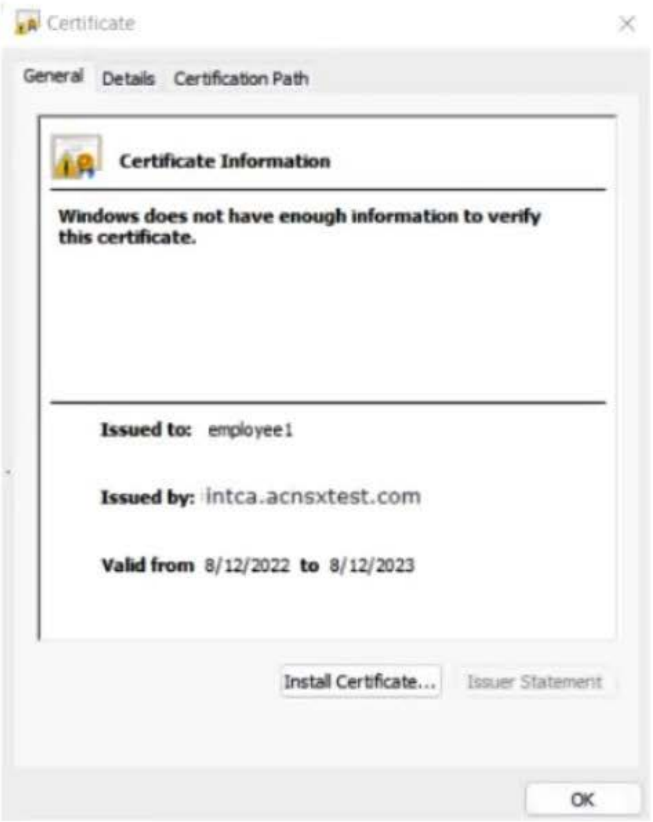
QUESTION 2

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.



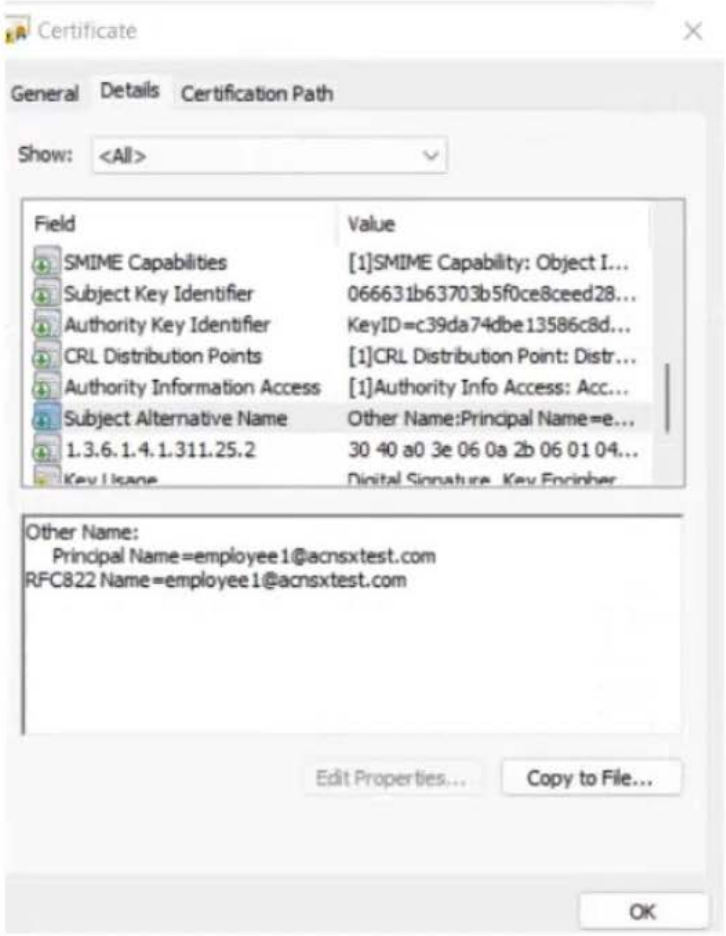
Certificate Information

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.

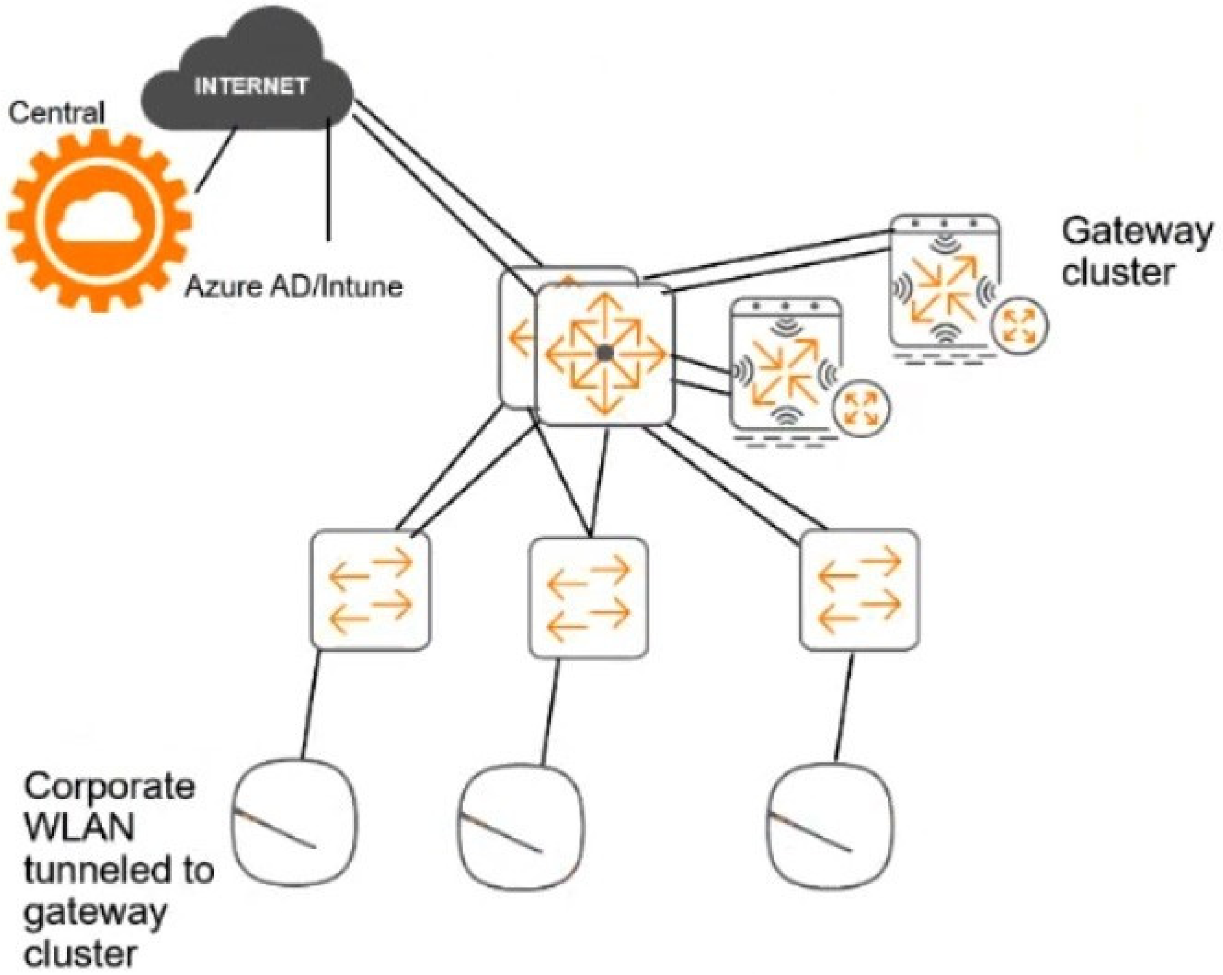
Deny other clients access

# 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

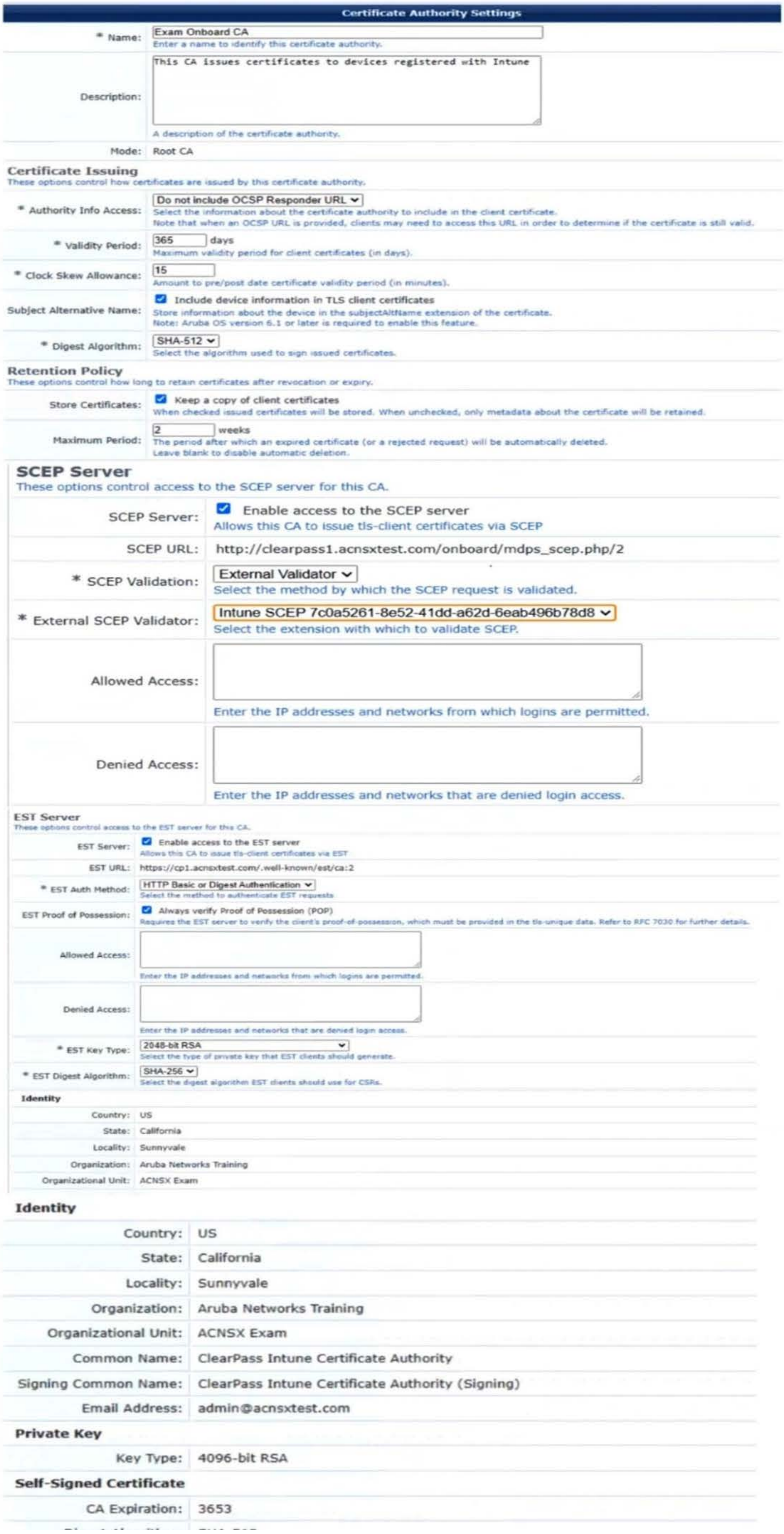
4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

You have 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

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.

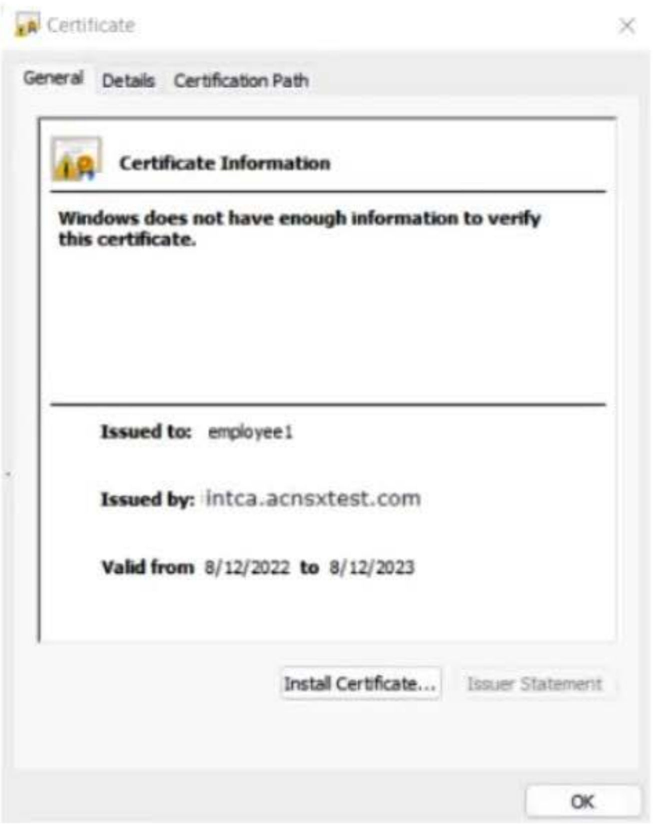
QUESTION 4

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.



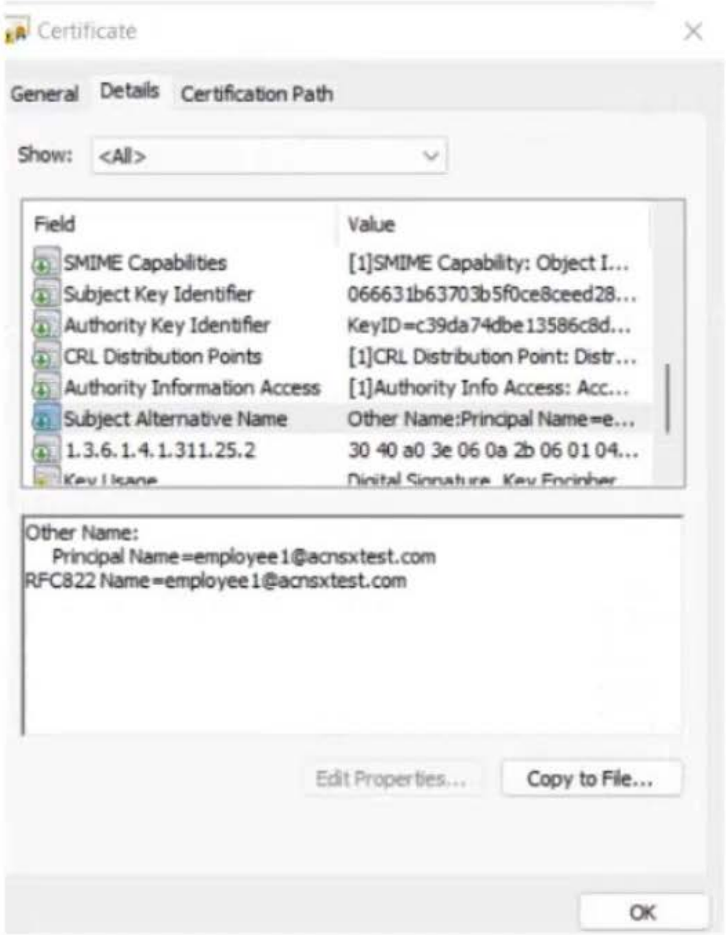
Certificate Information

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

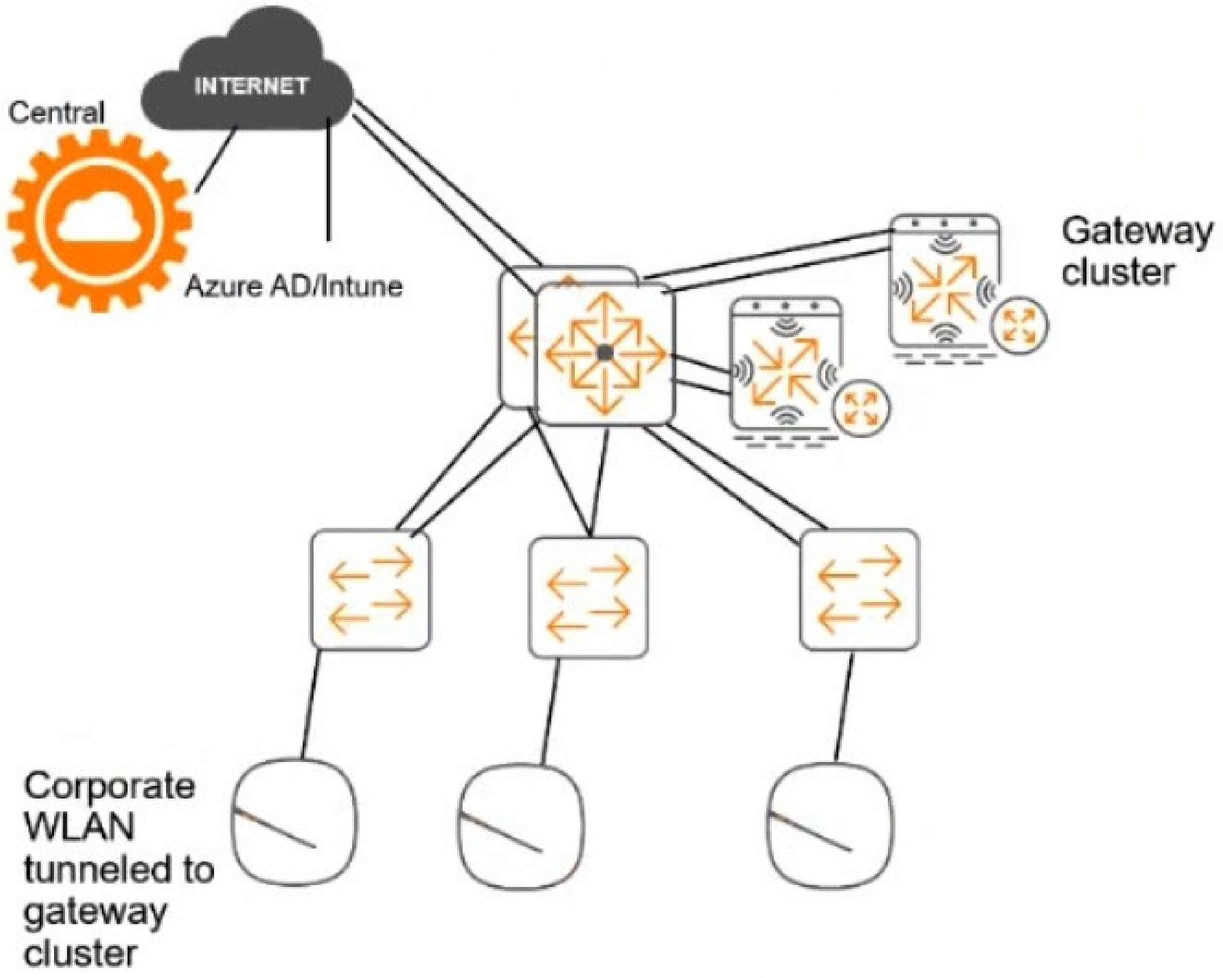
5.

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 cannot see flow attributes for wireless clients. What should you check?

A. Deep packet inspection is enabled on the role to which the Aruba APs assign the wireless clients.

B. Firewall application visibility is enabled on the Aruba gateways, and the gateways have been rebooted.

C. Gateway IDS/IPS is enabled on the Aruba gateways, and the gateways have been rebooted.

D. Deep packet inspection is enabled on the Aruba Aps, and the APs have been rebooted.

Correct Answer: A

QUESTION 5

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.

The developer explains that they plan to define the rule with logic like this:

monitor > value

However, the developer asks you what value to include.

What should you recommend?

A. Checking one of the access switches\\' RADIUS statistics and adding 10 to the number listed for rejects

B. Defining a baseline and referring to it for the value

C. Using 10 (per hour) as a good starting point for the value

D. Defining a parameter and referring to it (self ^ramsfname]) for the value

Correct Answer: D

This is because a parameter is a variable that can be defined and modified by the user or the script, and can be used to customize the behavior and output of the NAE script. A parameter can be referred to by using the syntax self

^ramsfname], where ramsfname is the name of the parameter. By defining a parameter for the value, the developer can make the NAE script more flexible and adaptable to different scenarios and switches. The parameter can be set to a default value, such as 10, but it can also be changed by the user or the script based on the network conditions and requirements. For example, the parameter can be adjusted dynamically based on the average or standard deviation of the number of rejects per hour, or based on the feedback from the user or other admins. This way, the NAE script can trigger an alert only when the number of rejects is truly unusual and not just arbitrary. A. Checking one of the access switches\\' RADIUS statistics and adding 10 to the number listed for rejects. This is not a good recommendation because it does not account for the variability and diversity of the network environment and switches. The number of rejects listed for one switch might not be representative or relevant for another switch, as different switches might have different traffic patterns, client types, RADIUS configurations, etc. Moreover, adding 10 to the number of rejects is an arbitrary and fixed value that might not reflect the actual threshold for triggering an alert. B. Defining a baseline and referring to it for the value. This is not a bad recommendation, but it is not as good as defining a parameter. A baseline is a reference point that represents the normal or expected state of a network metric or performance indicator. A baseline can be used to compare and contrast the current network situation and detect any anomalies or deviations. However, a baseline might not be easy or accurate to define, as it might require historical data, statistical analysis, or expert judgment. Moreover, a baseline might not be stable or constant, as it might change over time due to network growth, evolution, or optimization.

C. Using 10 (per hour) as a good starting point for the value. This is not a good recommendation because it is an arbitrary and fixed value that might not reflect the actual threshold for triggering an alert. Using 10 (per hour) as the value might result in false positives or false negatives, depending on the network conditions and switches. For example, if the normal number of rejects per hour is 5, then using 10 as the value might trigger an alert too frequently and unnecessarily. On the other hand, if the normal number of rejects per hour is 15, then using 10 as the value might miss some important alerts and risks.