



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

Instant Download After Purchase

100% Money Back Guarantee

😳 365 Days Free Update

800,000+ Satisfied Customers





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.



	Information	
Windows does not this certificate.	have enough information	n to verify
Issued to: er	nployee 1	
Issued by: in	tca.acnsxtest.com	
Valid from 8/	12/2022 to 8/12/2023	

	Details Certification Pat	
iow:	<all></all>	v
ield		Value
T SN	IME Capabilities	[1]SMIME Capability: Object I
A SU	bject Key Identifier	066631b63703b5f0ce8ceed28
AL	uthority Key Identifier	KeyID=c39da74dbe13586c8d
a a	RL Distribution Points	[1]CRL Distribution Point: Distr
AL	uthority Information Access	[1]Authority Info Access: Acc
a su	bject Alternative Name	Other Name:Principal Name=e
Long a		
@1	3.6.1.4.1.311.25.2	30 40 a0 3e 06 0a 2b 06 01 04
Other	Name:	Ninital Signature Key Enginher
Other Prin	ev lisane	Dinital Signature Key Enginher



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

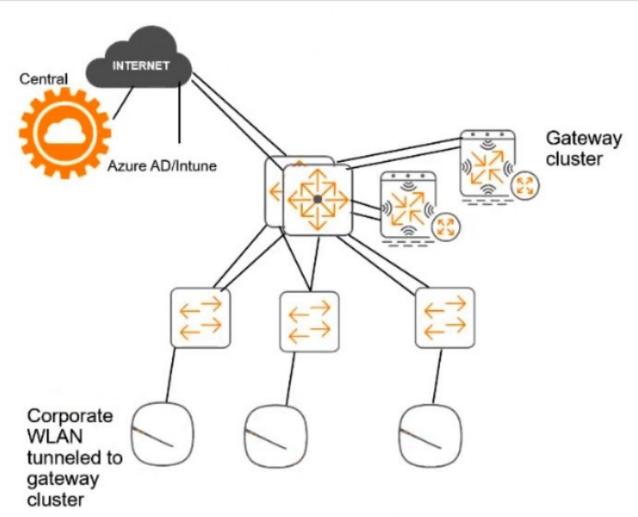
Other requirements

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.
Publ
```

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.



* Name	Exam O	nboard CA	
	Enter a r	ame to identify this certificate authority.	
	This C	issues certificates to devices registered with Intune	
Description			
Description			
	A descrip	tion of the certificate authority.	
Mode	Root CA		
ertificate Issuing	,		
hese options control how o		re issued by this certificate authority.	
# Authority Info Access	Select th	e information about the certificate authority to include in the client certificate.	
	T - contraction of the	t 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	1: 365 Maximur	days n validity period for client certificates (in days).	
Clock Skew Allowance	15		
		to pre/post date certificate validity period (in minutes). ude device information in TLS client certificates	
ubject Alternative Name	Store inf	ormation about the device in the subjectAltName extension of the certificate.	
	COULA E	abe OS version 6.1 or later is required to enable this feature.	
Digest Algorithm		e algorithm used to sign issued certificates.	
etention Policy	one to retain	certificates after revocation or expiry.	
	2 1/10	p a copy of client certificates	
Store Certificates		ecked issued certificates will be stored. When unchecked, only metadata about the certificate will be retained.	
Maximum Period	2	weeks a after which an expired certificate (or a rejected request) will be automatically deleted.	
riskingin Period		id arter which an expired certificate (or a rejected request) will be automatically deleted. Ink to disable automatic deletion.	
SCEP Server			
These options conti	rol access	to the SCEP server for this CA.	
SCE	P Server	Enable access to the SCEP server	
		Allows this CA to issue tls-client certificates via SCEP	
S	CEP URL	: http://clearpass1.acnsxtest.com/onboard/mdps_scep.php/2	
* SCEP V	alidatio	External Validator 🗸	
SUEP V	anuation	Select the method by which the SCEP request is validated.	
* External SCEP	Validates	Intune SCEP 7c0a5261-8e52-41dd-a62d-6eab496b78d8 V	
External SCEP	validator	Select the extension with which to validate SCEP.	
Allouis	d Assass		
Allowe	d Access		
		Enter the IP addresses and networks from which logins are permitted.	
Denie	d Access		
		Enter the IP addresses and networks that are denied login access.	
EST Server		er for the CA.	
These options control access t	and the second second		
These options control access t EST Server:	Enable Allows this C	ccess to the EST server to issue tis-dient certificates via EST	
These options control access t EST Server:	Enable Allows this Control Allows this Control Allows this Control Allows this Control Allows the Control Al	access to the EST server to soul the-dient contributes via EST construct_cont_well+hown/est/ca:2	
These options control access t EST Server:	Enable Allows this Control Allows this Control Allows this Control Allows this Control Allows the Control Al	ccess to the EST server to issue tis-dient certificates via EST	
These options control access t EST Server: EST URL:	Enable i Allows this C https://cp1. HTTP Basic Select the mi Always	In the EST server to sear the -dent continues via EST construct.com/vel/snown/est/ca:2 or Digest Authentication V thod to authenticate EST requests entry. Proof of Possession (POP)	
These options control access t EST Server: EST URL: * EST Auth Method:	Enable i Allows this C https://cp1. HTTP Basic Select the mi Always	to ase the EST server to ase the derificates we EST acrosses.com/.well-known/est/ca:2 or Olgest Authentication => dhod to authenticate EST requests	
These options control access t EST Server: EST URL: * EST Auth Method:	Enable i Allows this C https://cp1. HTTP Basic Select the mi Always	In the EST server to sear the -dent continues via EST construct.com/vel/snown/est/ca:2 or Digest Authentication V thod to authenticate EST requests entry. Proof of Possession (POP)	
These options control eccess t EST Server: EST URL: * EST Auth Method: EST Proof of Possession:	Enable Allows this C https://cp1. HTTP Basis Select the m Always Requires the	In the EST server: to super the-denet continuence we EST construct.com/web/nown/est/ca:2 or Digest Authentication V thod to authenticate EST requests entry. Proof of Possession (POP)	
These sphons control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access:	Enable Allows this C https://cp1. HTTP Basis Select the m Always Requires the	access to the EST server to sould the direct confidence as to EST conclusted.com/.vedl-known/est/ca:2 or Digast Authentication ♥] their to authenticate EST requests. everify Proof of Possession (POP) EST server to verify the citerit's proof-of-possession, which must be provided in the tis-unique data. Refer to RFC 7030 for further details.	
These options control eccess t EST Server: EST URL: * EST Auth Method: EST Proof of Possession:	Enable / Allows this C Allows this C HTTP Bask Select the m Always Requires the Enter the IP	In some the CET server to some the -Centre contributes via EST concluster.com/viat/cat/Cat/Cat/Cat/Cat/Cat/Cat/Cat/Cat/Cat/C	
These options control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access:	Enable / Allows this C Allows this C Https://cp1. Https://cp1. Enter the IP Enter the IP Enter the IP Enter the IP	access to the EST server to make the-direct contributes we EST- soundest.com/, well-known/est/ca:2 or Digest Authentication ♥ their to authentication ♥ their to authenticate EST requests. werfy Proof of Possession (POP) EST server to verify the citerit's proof-of-possession, which must be previded in the tils-unique data. Refer to RFC 7030 for further details. defresses and networks from which logies are permitted. defresses and networks that are denied login access.	
These sphons control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access:	Enable / Allows this C Allows this C https://cpl. HTTP Bask Select the m Always Requires the Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter the IP / Enter	access to the EST server to make the-direct contributes we EST- sonchett.com/.vedl-hnown/est/ca:2 or Digest Authentication ♥ their to authentication ♥ their to authenticate EST requests. everify Proof of Possession (POP) EST server to verify the citerit's proof-of-possession, which must be provided in the tis-unique data. Refer to RFC 7030 for further details. defresses and networks from which logies are permitted. defresses and networks that are denied login access.	
Phese sphons control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access:	Enable Allows the C Allows Select the m Allows Enter the IP C Zet40-bit RS Select the th	access to the EST server to suse the form confidences via EST concluster.com/.vell-known/est/ca:2 or Digast Authentication ♥] their to authentication ♥] their to authenticate EST requests. verify Proof of Possession (POP) EST server to verify the client's proof-of occession, which must be previded in the tis-unique data. Refer to RFC 7030 for further details. EST server to verify the client's proof-of occession, which must be previded in the tis-unique data. Refer to RFC 7030 for further details. detresses and networks from which logins are permitted. estimates and networks that are devied login access. A control of proofs key that EST clients should generate.	
Phese sphons control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type:	Enable Allows the C Allows Select the m Allows Enter the IP C Zet40-bit RS Select the th	Access to the EST server to make the direct contributes we EST conclusted.com/.vedl-hnown/est/ca:2 or Digest Authentication ♥ their to authentication ♥ their to authenticate EST requests. early Proof of Possession (POP) EST server to verify the cient's proof-of-possession, which must be provided in the tis-unique data. Refer to RFC 7030 for further details. EST server to verify the cient's proof-of-possession, which must be provided in the tis-unique data. Refer to RFC 7030 for further details. differences and networks that are denied login access. A of provide kry that EST clients about generate.	
These sphons control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Digest Algorithm:	Enable : Allows the C Allow	access to the EST server to suse the form confidences via EST concluster.com/.vell-known/est/ca:2 or Digast Authentication ♥] their to authentication ♥] their to authenticate EST requests. verify Proof of Possession (POP) EST server to verify the client's proof-of occession, which must be previded in the tis-unique data. Refer to RFC 7030 for further details. EST server to verify the client's proof-of occession, which must be previded in the tis-unique data. Refer to RFC 7030 for further details. detresses and networks from which logins are permitted. estimates and networks that are devied login access. A control of proofs key that EST clients should generate.	
These sphons control access t EST Server: EST URL: * EST Auth Hethod: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Digest Algorithm: Identity Country: State:	C Enable Allows tha C Allows tha C Allows tha C Allows tha C Interpediate the me C Interpediate the me C Inter the IP C Inter	access to the EST server to make the form confidences via EST concluster.com/.vell-known/est/ca:2 or Digast Authentication ♥] their to authentication ♥] their to authenticate EST requests. verify Proof of Possession (POP) EST server to verify the client's proof-of occession, which must be previded in the tis-unique data. Refer to RFC 7030 for further details. defresses and networks from which loging are permitted. defresses and networks that are denied login access. A client key that EST clients should generate.	
These sphons control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST bigest Algorithm: Identity Country: State: Locality:	C Enable Allows the C Allows the C Allows the C Allows the C C Allows C C C C C C C C C C C C C C C C C C C	crosses to the EST server to source the configurate via EST concluster.com/.vell-inoun/est/ca:2 cor Digest Authentication ♥ the to authentication ♥ EST server to verify the cient's proof-of-possession, which must be provided in the tis-unique data. Refer to RFC 7030 for further details. defresses and networks from which logies are permitted. defresses and networks that are denied login access. A C C C C C C C C C C C C	
These sphone control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Digest Algorithm: Identity Country: State: Locality:	Enable Anapy Select the ap Anapy Enter the IP California Sunnyvale Aruba Nethor	Access to the EST server to share the distribution with the site ST: conclusted.com/.vedi-innown(est/ca:2 or Digast Authentication with the distribution and the server and the serve	
These sphore control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST bigest Algorithm: Identity Country: State: Locality:	Enable Anapy Select the ap Anapy Enter the IP California Sunnyvale Aruba Nethor	Access to the EST server to share the distribution with the site ST: conclusted.com/.vedi-innown(est/ca:2 or Digast Authentication with the distribution and the server and the serve	
These sphone control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Nojest Algorithm: Edentity Country: State: Locality: Organizational Unit:	Enable Anapy Select the ap Anapy Enter the IP California Sunnyvale Aruba Nethor	Access to the EST server to share the distribution with the server set of the server set of the server set of the server server to verify the client's provided in the Us-unique data. Refer to BFC 7030 for further details. Refer Proof of Possession (POP) EST server to verify the client's proof-of-possession, which must be provided in the Us-unique data. Refer to BFC 7030 for further details. Indiference and networks from which logies are permitted. Indiference and networks that are denied login access. A v v e of proofset key that EST clients absold generate. Indiference the test denied use for CSRs. Was Training	
These sphore control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Key Type: * EST Digest Algorithm: Identity Country: State: Locality: Organization: Organizational Unit:	California	In some the EST server to some the device vie EST concluster.com/, well-known/est/ca:2 cor Digast Authentication ♥ their to authentication ♥ EST server to verify the cient's proof-of-possession, which must be previded in the tis-unique data. Refer to RFC 7030 for further details. defresses and networks that are denied login access.	
These sphore control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Key Type: * EST Key Type: * EST Digest Algorithm: Identity Country: State: Locality: Organization: Organization: Ucentity	California	crosses to the EST server to source the definition of the defini	
These sphore control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Key Type: * EST Key Type: * EST Digest Algorithm: Identity Country: State: Locality: Organization: Organization: Ucentity	California	In some the EST server to some the device vie EST concluster.com/.vedH-hnown/est/ca:2 cor Digest Authentication ♥ their to authentication ♥ EST server to verify the cient's proof-of-possesson, which must be provided in the tis-unique data. Refer to RFC 7030 for further details. conclusion of the time time time time time time time tim	
These sphere control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Key Type: * EST Key Type: * EST Key Type: * Country: State: Locality: Organizational Unit: Identity	California Sunnyvale California Califo	crosses to the EST server to source the definition of the defini	
These sphere control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Key Type: * EST Digest Algorithm: Identity Country: State: Locality: Organizational Unit: Identity	California Sunnyvale California Califo	In some the EST energy in the EST energy of the source of o	
These sphere control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Digest Algorithm: Identity Country: State: Locality: Organizational Unit: Identity Cu	C Enable Enable Enable Ender the D Ender	In some the LEST energy of the Hest end of the set of t	
These options control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Kay Type: * EST Digest Algorithm: Identity Country: State: Locality: Organization: Organization: Li Organization:	California Sunnyvale California Sunnyvale California Sunnyvale California Ca	In the ST terms	
These options control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Digest Algorithm: Identity Country: State: Locality: Organizational Unit: Identity Country: State: Locality: Organizational Unit:	California Sunnyvale California Sunnyvale California Sunnyvale California Ca	In some the LEST energy of the Hest end of the set of t	
These options control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Kay Type: * EST Digest Algorithm: Identity Country: State: Locality: Organization: Organization: Li Organization:	C Enable Allows this C Allows the C C Inter D Back C C C C C C C C C C C C C C C C C C C	In the ST terms	
These options control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Kay Type: * EST Kay Type:	C Enable Allows this C Intersection C Allows C Allows C C C C C C C C C C C C C C C C C C C	In seve the SST energy to seve the Gott ontificates vie SST server to verify the of of Possession (POP) SST enror to verify the client's proof of Possession, which must be previded in the its unique date. Refer to RFC 7030 for further details addresses and networks from which logies are permitted. addresses and networks that are denied iogin access. A A of provide key that CST clients should generate. ent generate key that CST clients should generate.	
EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Digest Algorithm: Identity Country: State: Locality: Organizational Unit: Identity Corganizational Unit: Identity Corganizational Unit: Identity Corganizational Unit: Editional Unit: Corganizational Unit: Corganizational Unit: Editional Unit: Editional Unit: Editional Unit: Editional Unit: Editional Unit: Corganizational Unit:	C Enable Allows this C Intersection C Allows C Allows C C C C C C C C C C C C C C C C C C C	In seve the SST energy to seve the GST energy is seve the control actes ve SST control to authentication v the dot built authentication v interference of the SST energy SST server to verify the control a proof of possession, which must be previded in the tis-unique data. Refer to RFC 7030 for further details. addresses and networks from which logies are permitted. addresses and networks from which logies are permitted. addresses and networks that are denied login access. A A SUBS California Sunnyvale Aruba Networks Training ACNSX Exam ACNSX Exam	
These options control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Kay Type: * EST Kay Type:	C Enable Allows this C Intersection C Allows C Allows C C C C C C C C C C C C C C C C C C C	In seve the SST energy to seve the Gott ontificates vie SST server to verify the of of Possession (POP) SST enror to verify the client's proof of Possession, which must be previded in the its unique date. Refer to RFC 7030 for further details addresses and networks from which logies are permitted. addresses and networks that are denied iogin access. A A of provide key that CST clients should generate. ent generate key that CST clients should generate.	
These options control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: EST Key Type: * EST Digest Algorithm: Identity Country: State: Country: State: Country: State: Country: State: Country: Country: State: Country: C	California State: cocality: cation: c	In seve the SST energy to seve the Gott ontificates vie SST server to verify the of of Possession (POP) SST enror to verify the client's proof of Possession, which must be previded in the its unique date. Refer to RFC 7030 for further details addresses and networks from which logies are permitted. addresses and networks that are denied iogin access. A A of provide key that CST clients should generate. ent generate key that CST clients should generate.	
These sphere control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: * EST Rey Type: * EST Digest Algorithm: Zdentity Country: State: Country: Country: State: Country: Country: Country: Country: Country: State: Country: Country: Country: State: Country: Country: State: Country: Country: State: Country: State: Country: Country: State: Country: Country: State: Country: Country: Country: Country: State: Country: State: Country: State: Country: State: Country: Country: Country: Country: Country: Country: Country: Country: Country: State: Country: Country: State: Country: Country: State: Country: Country: State: Country: Country: State: Country: Country: State: Country: Country: State: Country: Country: State: Country: State: Country: State: Country: State: Country: State: Country: State: Country: State: Country: State: Country: State: Country: State: State: Country: State: S	California State: california	In seve the SST server to seve the destream of the several set of the several set of the several set of the several set of the several	
These options control access t EST Server: EST URL: * EST Auth Method: EST Proof of Possession: Allowed Access: Denied Access: * EST Key Type: * EST Rey Type:	California State: california	In seve the SST server to seve the destream of the several set of the several set of the several set of the several set of the several	



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.



	· Information
Windows does no this certificate.	ot have enough information to verify
Issued to:	employee 1
Issued by: i	ntca.acnsxtest.com
	ntca.acnsxtest.com 8/12/2022 to 8/12/2023

erai	Details Certification Pat	n
now:	<ali></ali>	~
Field		Value
T SN	IME Capabilities	[1]SMIME Capability: Object I
A SU	bject Key Identifier	066631b63703b5f0ce8ceed28
AL	uthority Key Identifier	KeyID=c39da74dbe13586c8d
a a	RL Distribution Points	[1]CRL Distribution Point: Distr
AL	uthority Information Access	[1]Authority Info Access: Acc
a su	bject 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
Ke	3.6.1.4.1.311.25.2 ev lisane	30 40 a0 3e 06 0a 2b 06 01 04 Ninital Sinnature Kev Enrinher
Other Prin	ev lisane	Dinital Signature Key Enginher



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.

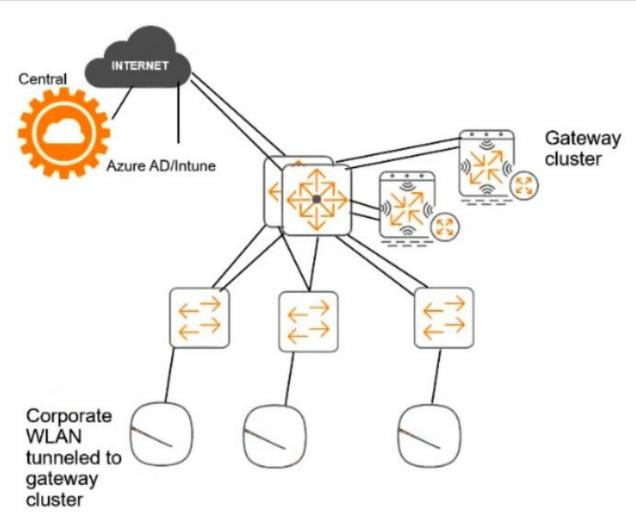
All domain computers with no valid user logged in to the "computer-only" firewall role

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.

HPE6-A84 PDF Dumps

HPE6-A84 VCE Dumps

HPE6-A84 Study Guide