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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the scenario.

A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

Switches are using local port-access policies.

The customer wants to start tunneling wired clients that pass user authentication only to an Aruba gateway cluster. The gateway cluster should assign these clients to the "eth- internet" role. The gateway should also handle assigning clients

to their VLAN, which is VLAN 20.

The plan for the enforcement policy and profiles is shown below:

Enforcement Policies - written-exam-3

Summary | Enforcement | Rules

Enforcement:

Name:	written-exam-3
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS [Machine Authenticated]) AND (Tips:Role EQUALS [User Authenticated])	written-exam-a
2.	(Authentication:TEAP-Method-2-Status EQUALS Success)	written-exam-b

Enforcement Profiles - written-exam-a

Summary | Profile | Attributes

Profile:

Name:	written-exam-a
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	eth-user

Enforcement Profiles - written-exam-b

Summary | Profile | Attributes

Profile:

Name:	written-exam-b
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	internet-only

The gateway cluster has two gateways with these IP addresses:

Gateway 1

1.

VLAN 4085 (system IP) = 10.20.4.21

2.

VLAN 20 (users) = 10.20.20.1

3.

VLAN 4094 (WAN) = 198.51.100.14

Gateway 2

1.

VLAN 4085 (system IP) = 10.20.4.22

2.

VLAN 20 (users) = 10.20.20.2

3.

VLAN 4094 (WAN) = 198.51.100.12

VRRP on VLAN 20 = 10.20.20.254

The customer requires high availability for the tunnels between the switches and the gateway cluster. If one gateway falls, the other gateway should take over its tunnels. Also, the switch should be able to discover the gateway cluster regardless of whether one of the gateways is in the cluster.

Assume that you have configured the correct UBT zone and port-access role settings. However, the solution is not working.

What else should you make sure to do?

A. Assign VLAN 20 as the access VLAN on any edge ports to which tunneled clients might connect.

B. Create a new VLAN on the AOS-CX switch and configure that VLAN as the UBT client VLAN.

C. Assign sufficient VIA licenses to the gateways based on the number of wired clients that will connect.

D. Change the port-access auth-mode mode to client-mode on any edge ports to which tunneled clients might connect.

Correct Answer: B

The correct answer is B. Create a new VLAN on the AOS-CX switch and configure that VLAN as the UBT client VLAN.

User-based tunneling (UBT) is a feature that allows the AOS-CX switches to tunnel the traffic from wired clients to a mobility gateway cluster, where they can be assigned a role and a VLAN based on their authentication and authorization 1.

To enable UBT, the switches need to have a UBT zone configured with the IP addresses of the gateways, and a UBT client VLAN configured with the ubt-client-vlan command 2. The UBT client VLAN is a special VLAN that is used to

encapsulate the traffic from the tunneled clients before sending it to the gateways. The UBT client VLAN must be different from any other VLANs used on the switch or the network, and it must not be assigned to any ports or interfaces on the

switch 2. The UBT client VLAN is only used internally by the switch for UBT, and it is not visible to the clients or the gateways. In this scenario, the customer wants to tunnel the clients that pass user authentication to the gateway cluster,

where they will be assigned to VLAN 20. Therefore, the switch must have a UBT client VLAN configured that is different from VLAN 20 or any other VLANs on the network. For example, the switch can use VLAN 4000 as the UBT client VLAN,

as shown in one of the web search results 3. The switch must also have a UBT zone configured with the system IP addresses of the gateways as the primary and backup controllers, as explained in question 3.

The other options are not correct or relevant for this issue:

Option A is not correct because assigning VLAN 20 as the access VLAN on any edge ports to which tunneled clients might connect would conflict with UBT. The access VLAN is the VLAN that is assigned to untagged traffic on a port, and it is

used for local switching on the switch 4. If VLAN 20 is assigned as the access VLAN, then the traffic from the clients will not be tunneled to the gateways, but rather switched locally on VLAN 20. This would defeat the purpose of UBT and

cause inconsistency in role and VLAN assignment.

Option C is not correct because VIA licenses are not required for UBT. VIA licenses are required for enabling VPN services on Aruba Mobility Controllers for remote access clients using Aruba Virtual Intranet Access (VIA) software . VIA

licenses are not related to UBT or wired clients.

Option D is not correct because changing the port-access auth-mode mode to client-mode on any edge ports to which tunneled clients might connect would not affect UBT. The port-access auth-mode mode determines how a port handles

authentication requests from multiple clients connected to a single port . Client- mode is the default mode that allows only one client per port, while multi-client- mode allows multiple clients per port. The port-access auth-mode mode does not

affect how UBT works or how traffic is tunneled from a port.

QUESTION 2

Refer to the scenario.

A customer has an AOS10 architecture that is managed by Aruba Central. Aruba infrastructure devices authenticate clients to an Aruba ClearPass cluster.

In Aruba Central, you are examining network traffic flows on a wireless IoT device that is categorized as "Raspberry Pi" clients. You see SSH traffic. You then check several more wireless IoT clients and see that they are sending SSH also.

You want a relatively easy way to communicate the information that an IoT client has used SSH to Aruba CPPM.

What is one prerequisite?

A. Enable event processing on subscribers in the ClearPass cluster.

B. In CPPM\\'s CA trust list, add the Aruba Infrastructure usage to the DigiCert certificate.

C. Obtain a data collector token from Central\\'s platform integration settings.

D. Create an API application and token within the REST API settings.

Correct Answer: C

QUESTION 3

Refer to the scenario.

A customer is migrating from on-prem AD to Azure AD as its sole domain solution. The customer also manages both wired and wireless devices with Microsoft Endpoint Manager (Intune).

The customer wants to improve security for the network edge. You are helping the customer design a ClearPass deployment for this purpose. Aruba network devices will authenticate wireless and wired clients to an Aruba ClearPass Policy Manager (CPPM) cluster (which uses version 6.10).

The customer has several requirements for authentication. The clients should only pass EAP-TLS authentication if a query to Azure AD shows that they have accounts in Azure AD. To further refine the clients\\' privileges, ClearPass also should use information collected by Intune to make access control decisions.

You are planning to use Azure AD as the authentication source in 802.1X services.

What should you make sure that the customer understands is required?

A. An app registration on Azure AD that references the CPPM\\'s FQDN

B. Windows 365 subscriptions

C. CPPM\\'s RADIUS certificate was imported as trusted in the Azure AD directory

D. Azure AD Domain Services

Correct Answer: A

To use Azure AD as the authentication source in 802.1X services, you need to configure CPPM as a SAML service provider and Azure AD as a SAML identity provider. This allows CPPM to use Azure AD for user authentication and role mapping. To do this, you need to create an app registration on Azure AD that references the CPPM\\'s FQDN as the reply URL and the entity ID. You also need to grant the app registration the required permissions to access user information from Azure AD1

QUESTION 4

Refer to the scenario.

A customer has asked you to review their AOS-CX switches for potential vulnerabilities. The configuration for these switches is shown below:

```
hostname Access-Switch-$$

ntp authentication-key 1 sha1 ciphertext
AQBapYn45h7mDzxcLhAYWBH6biegegFASS1kvTQPPgICEfaLCAAAAMIb48QNRhSg
ntp trusted-key 1
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst key-id 1
ntp enable
ntp authentication
!
radius-server host rad.example.com tls
!
tacacs-server host rad.example.com
!
aaa authentication login ssh group tacacs local
aaa authentication login telnet group tacacs local
!
aaa accounting port-access start-stop interim group radius
!
radius dyn-authorization enable
!
radius dyn-authorization client rad.example.com tls
ssh server vrf default
ssh server vrf mgmt
telnet server vrf default
telnet server vrf mgmt
crypto pki application radsec-client certificate device-identity
crypto pki ta-profile privateca
ta-certificate
      -----BEGIN CERTIFICATE-----
      MIIGAzCCA+ugAwIBAgIUEVfsxopuixT2QHZDJ/UYAAbYsdowDQYJKoZIhvcNAQEL
      BQAwgYgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQH
      DAlTdW5ueXZhbGUxHDAaBgNVBAoME0FydWJhIFRyYWluaW5nIExhYnMxEzARBgNV
      BAsMCkFDTlNYIFRlc3QxHTAbBgNVBAMMFHJvb3RjYS5hY25zeHRlc3QuY29tMB4X
      DTIyMTEyMjIwNTQxOFoXDTMyMTExOTIwNTQxOFowgYgxCzAJBgNVBAYTAlVTMRMw
      EQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUxHDAaBgNVBAoM
      E0FydWJhIFRyYWluaW5nIExhYnMxEzARBgNVBAsMCkFDTlNYIFRlc3QxHTAbBgNV
      BAMMFHJvb3RjYS5hY25zeHRlc3QuY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
      MIICCgKCAgEAsiUzsBkJcUgcdsbRyoLd0ZNqpcXfphk2VsSzZngP1LCu3lea3OHU
      V9GchhJXOQaI3HDUTcLp4b5If63z4nKzA36T6tyWXOe0PSgUjy+61XXMA9Rp5DKc
      CyoY9F8spVJiEo2n2hqL4m/DLFYlhxo5Z2UKav/08DMfzD/yVUzGNiQKDP/L7ivk
      CWF+15WIGSrH10i/rgIM/+W20n58aDx5f1AWaH9DYdRTWFMuk1UXQ/I8+7+9PXju
      B95Mt4b77RaWWj6CkW9k8WhmyjE7MMPSHtuJ4t3evh7jd/lTkm5ZOg/V8kvNTtW5
      fif7lkWLevmlLlvcxYnj+S3CWhAFdaR7S33a6xwdZxCDOLfPB6L1oOnKe0VM4mO2
      lOZtJNPFueBt16BRolR+IMANQkj3B2lB0whSLHF6JmLr0L6y/edV8XhIUhMxOfIp
      JKeSw38TDm3t1k98PBCOaLj5s4tYJRxcZLDnrg7Oz1e37sxENYoBtgRp77cdfePr
      cP/sp8U66gti2F0ijkU6k37moL3sMs2uHgC0YWpfRyFI09BWCRbxmy81UePiSlsW
      0goOaPDr35W/0443I/z6A+q/ciwVrALS+zEfHbMDFxo4VMygJttaiWZ05GAQQSHj
      redQmQEQPMwkgbzaELtAgYOWGkB56T/XifRLVxneYU8woAEZwmscI3kCAwEAAaNj
      MGEwHQYDVR0OBBYEFGXCH/z475pdNKIHhjDxFCfjz8khMB8GA1UdIwQYMBaAFGXC
      H/z475pdNKIHhjDxFCfjz8khMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
      AgGGMA0GCSqGSIb3DQEBCwUAA4ICAQB5TGIspaamHQXtsnWgmux6PANdEdPZ0Ele
      wDnpUxkVbeSPr9wl8luRJMptRO25rwVwEtrM8t5JD4jAK+d0usr4TDKwWqPPqFi0
      F5svFK9aEJ59ceD+eDWl4LAJJi3zjb9ZBuBa3LkaP7kyTlSnI0+opN+vdV43LNXh
      T23xEmLC9OUolq3bb8zpkWXieeFwSo2BafFMscPdf75DVY+x+Qo1SgpjbWBAS80B
      jRdZHrKmsqcrIG+37bixqaFj9nMzWpX0n2HfKCVcl6uk2pDNbiYVbU3k9b/ZWQmW
      DRYkAuR8dFBN3lKDyQo86T/chT/DY77FoStfg0gDZEj3EqaM76rf8S2z1GCsrfkp
      Crp5oKP6jiOCi2EcidkZSsmbzAHWKXNaF7vWRj0OivpqEFRkIVu/kce9O2KaxNYd
      sIKlNh7gG4pcQqhFfDddFD9vXvjOwKnXKkKppUpN6w+Quc+jhqFpP8GVPOy7ayZo
      z5cz5yEaVXtbfXRhVSg9oooq7xImBT14SK1pyrHSj8sD67Og3zgnNot/v8fHhI3O
      zUtBe4UPGWfraO4gkHH3mbb1qYeJnxKpMz56A0APBkKV9icY0uTQOsHk6bA9lG+Q
      sjqyWwKApf7RB4lHjF+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 recommendation to make?

A. Let the RADIUS server confiqure VLANs on LAG 1 dynamically.

B. Use MDS instead of SHA1 for the NTP authentication key.

C. Encrypt the certificate in the TA-profile.

D. Create a control plane ACL to limit the sources that can access the switch with SSH.

Correct Answer: D

According to the AOS-CX Switches Multiple Vulnerabilities1, one of the vulnerabilities (CVE-2021-41000) affects the SSH service on AOS-CX switches. This vulnerability allows an unauthenticated remote attacker to cause a denial-of-service condition on the switch by sending specially crafted SSH packets. The impact of this vulnerability is high, as it could result in a loss of management access and network disruption. Therefore, one recommendation to make is to create a control plane ACL to limit the sources that can access the switch with SSH. This way, the switch can filter out unwanted or malicious SSH traffic and reduce the risk of exploitation.

QUESTION 5

Refer to the scenario.

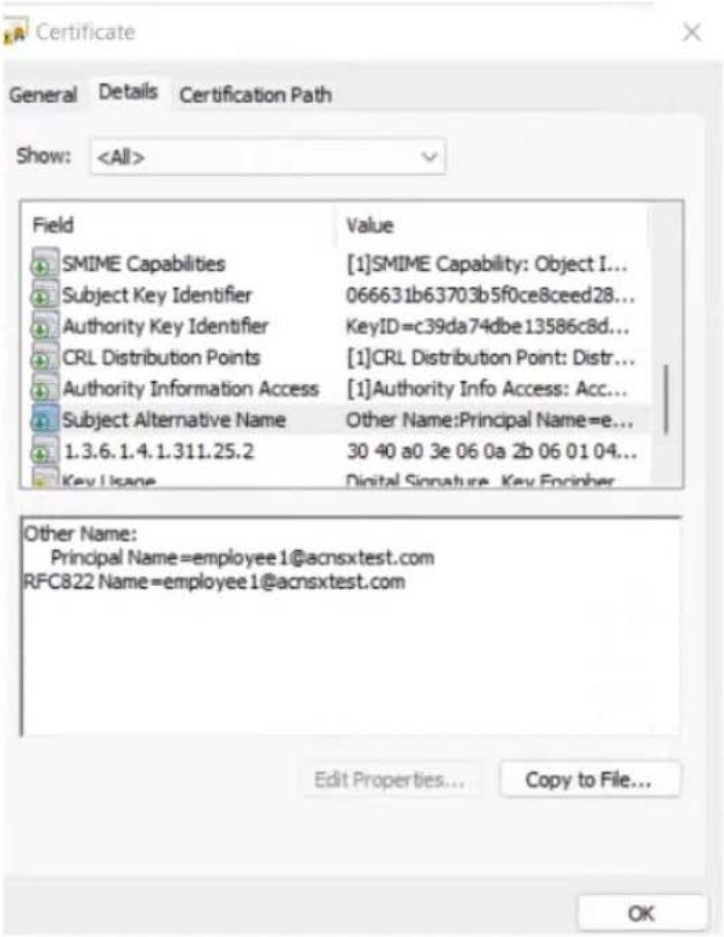
Introduction to the customer

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
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

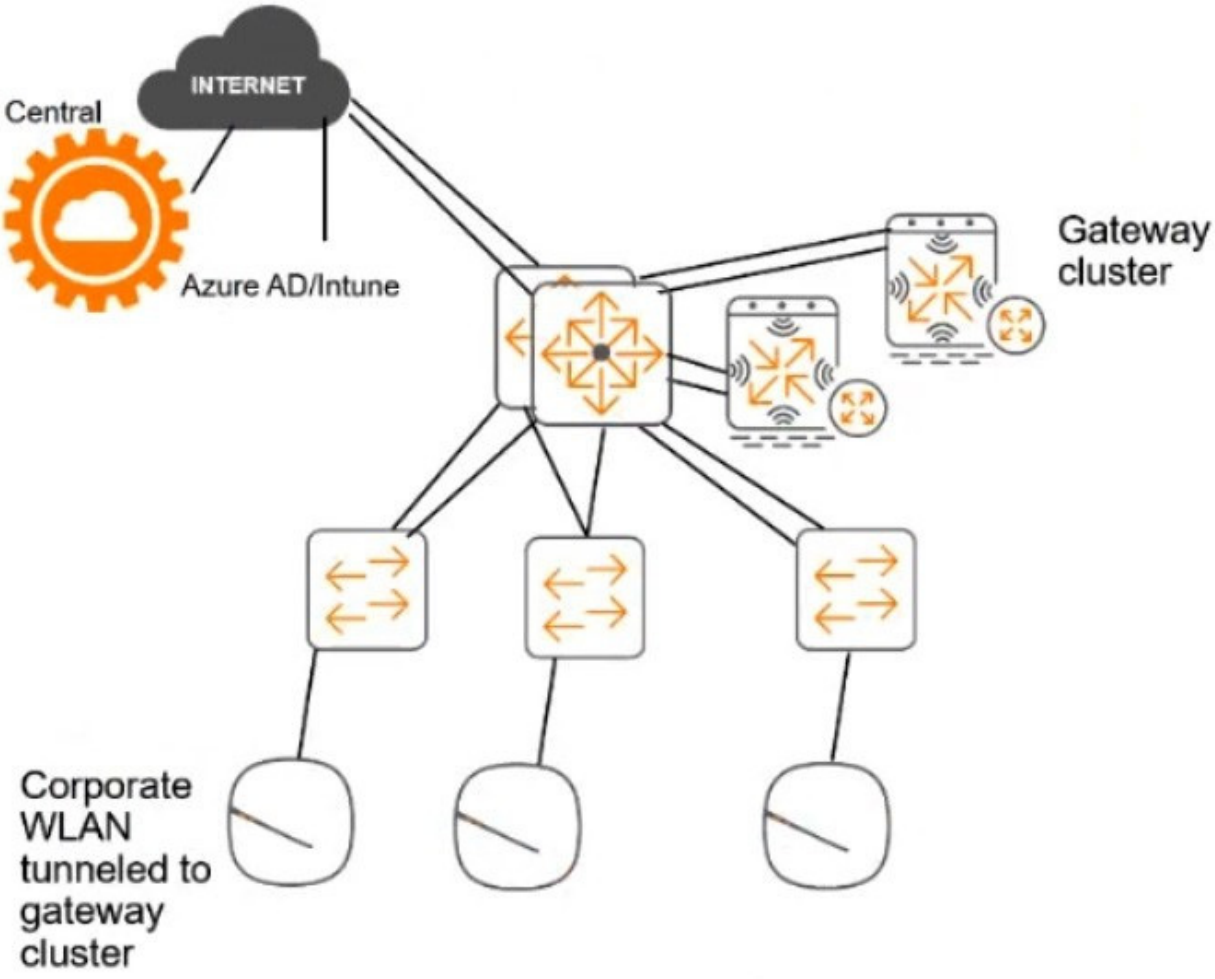
5.

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

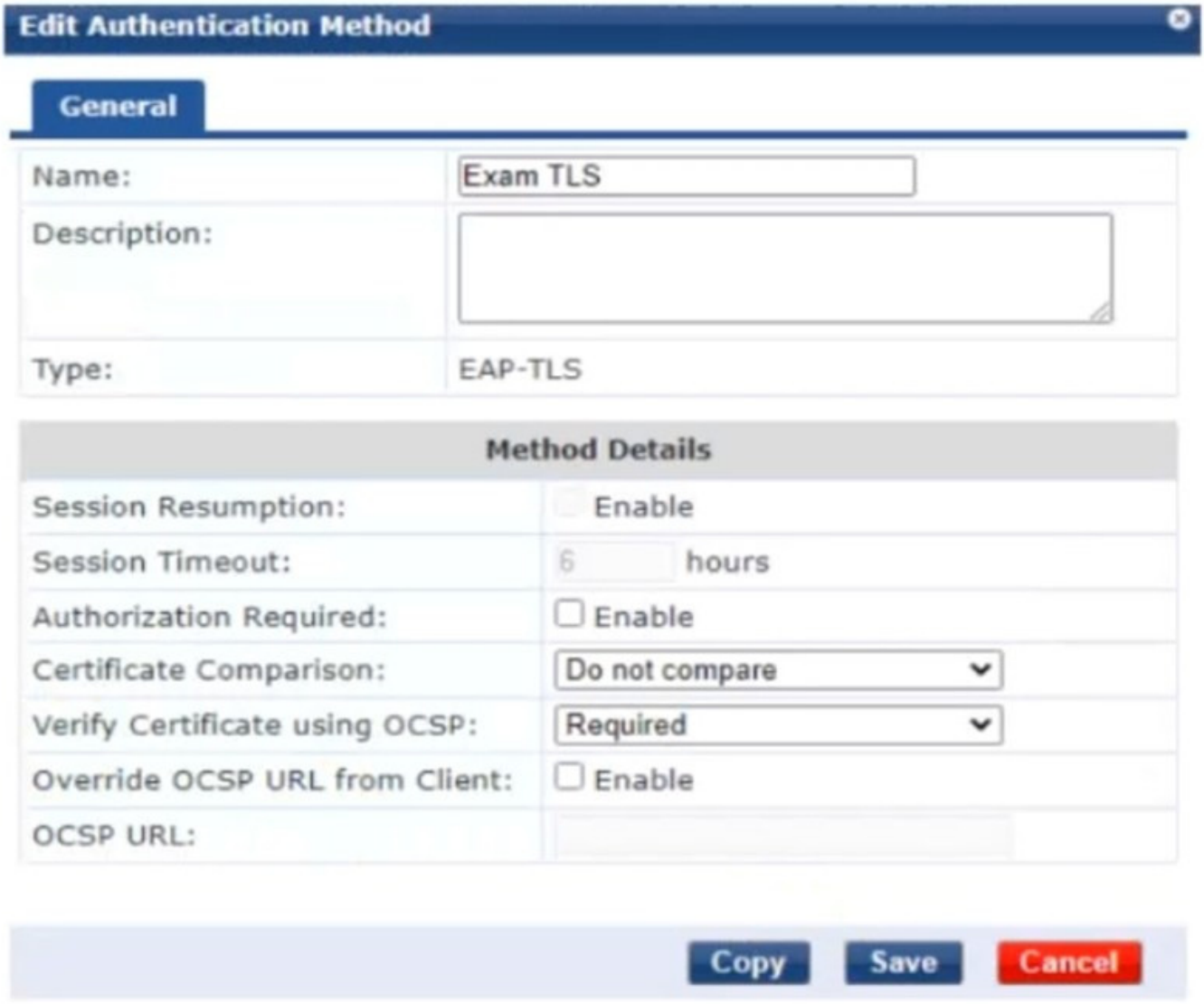
4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

On CPPM, you are creating the authentication method shown in the exhibit below:



You will use the method for standalone EAP-TLS and for inner methods in TEAP. What should you do?

A. Configure OCSP override and set the OCSP URL to localhost/onboard/mdps ocspphp/2

B. Enable certificate comparison.

C. Enable authorization.

D. Configure OCSP override and leave the OCSP URL blank.

Correct Answer: A