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

The customer needs a way for users to enroll new wired clients in Intune. The clients should have limited access that only lets them enroll and receive certificates. You plan to set up these rights in an AOS-CX role named "provision."

The customer\\'s security team dictates that you must limit these clients\\' Internet access to only the necessary sites. Your switch software supports IPv4 and IPv6 addresses for the rules applied in the "provision" role.

What should you recommend?

A. Configuring the rules for the "provision" role with IPv6 addresses, which tend to be more stable

B. Enabling tunneling to the MCs on the "provision" role and then setting up the privileges on the MCs

C. Configuring the "provision" role as a downloadable user role (DUR) in CPPM

D. Assigning the "provision" role to a VLAN and then setting up the rules within a Layer 2 access control list (ACL)

Correct Answer: C

This is because a downloadable user role (DUR) is a feature that allows the switch to use a central ClearPass server to download user-roles to the switch for authenticated users12 A DUR can contain various attributes and rules that define the access level and privileges of the user, such as VLAN, ACL, PoE, reauthentication period, etc3 A DUR can also be customized and updated on the ClearPass server without requiring any changes on the switch1 A DUR can be used to create a "provision" role that allows users to enroll new wired clients in Intune. The "provision" role can have limited access that only lets them enroll and receive certificates from the Intune service. The "provision" role can also have rules that restrict the Internet access of the users to only the necessary sites, such as the Intune portal and the certificate authority. The rules can be based on IPv4 or IPv6 addresses, depending on the network configuration and preference2 A. Configuring the rules for the "provision" role with IPv6 addresses, which tend to be more stable. This is not a valid recommendation because it does not address how to create and apply the "provision" role on the switch. Moreover, IPv6 addresses do not necessarily tend to be more stable than IPv4 addresses, as both protocols have their own advantages and disadvantages4

B. Enabling tunneling to the MCs on the "provision" role and then setting up the privileges on the MCs. This is not a valid recommendation because it does not explain how to enable tunneling or what MCs are. Moreover, tunneling is a technique that encapsulates one network protocol within another, which adds complexity and overhead to the network communication5

D. Assigning the "provision" role to a VLAN and then setting up the rules within a Layer 2 access control list (ACL). This is not a valid recommendation because it does not explain how to assign a role to a VLAN or how to create a Layer 2 ACL on the switch. Moreover, a Layer 2 ACL is limited in its filtering capabilities, as it can only match on MAC addresses or Ethernet types, which might not be sufficient for restricting Internet access to specific sites

QUESTION 2

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.

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

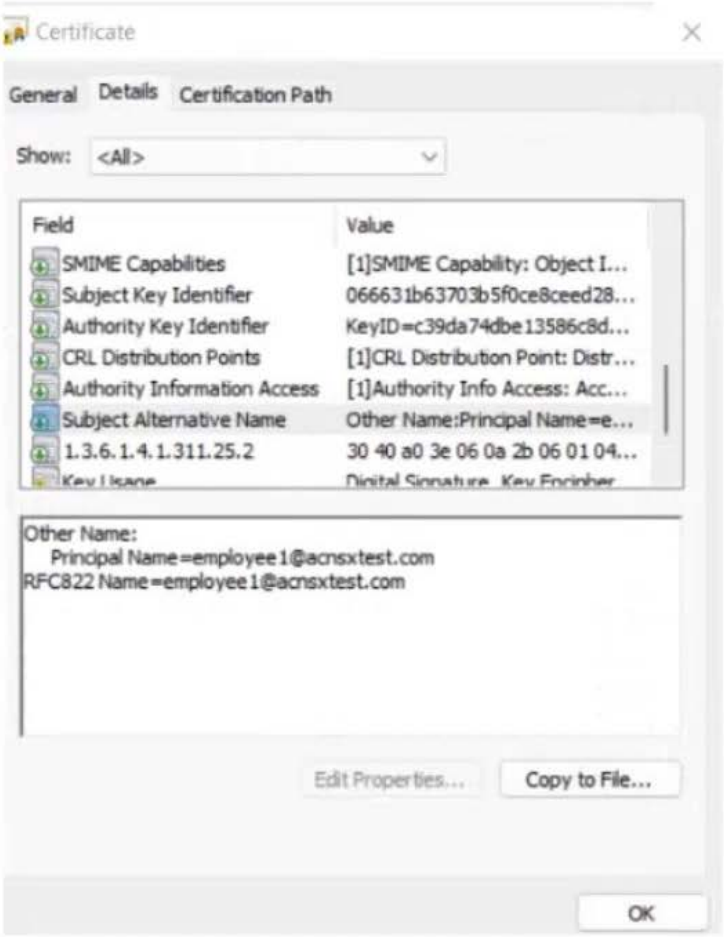
Refer to the scenario.

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
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.

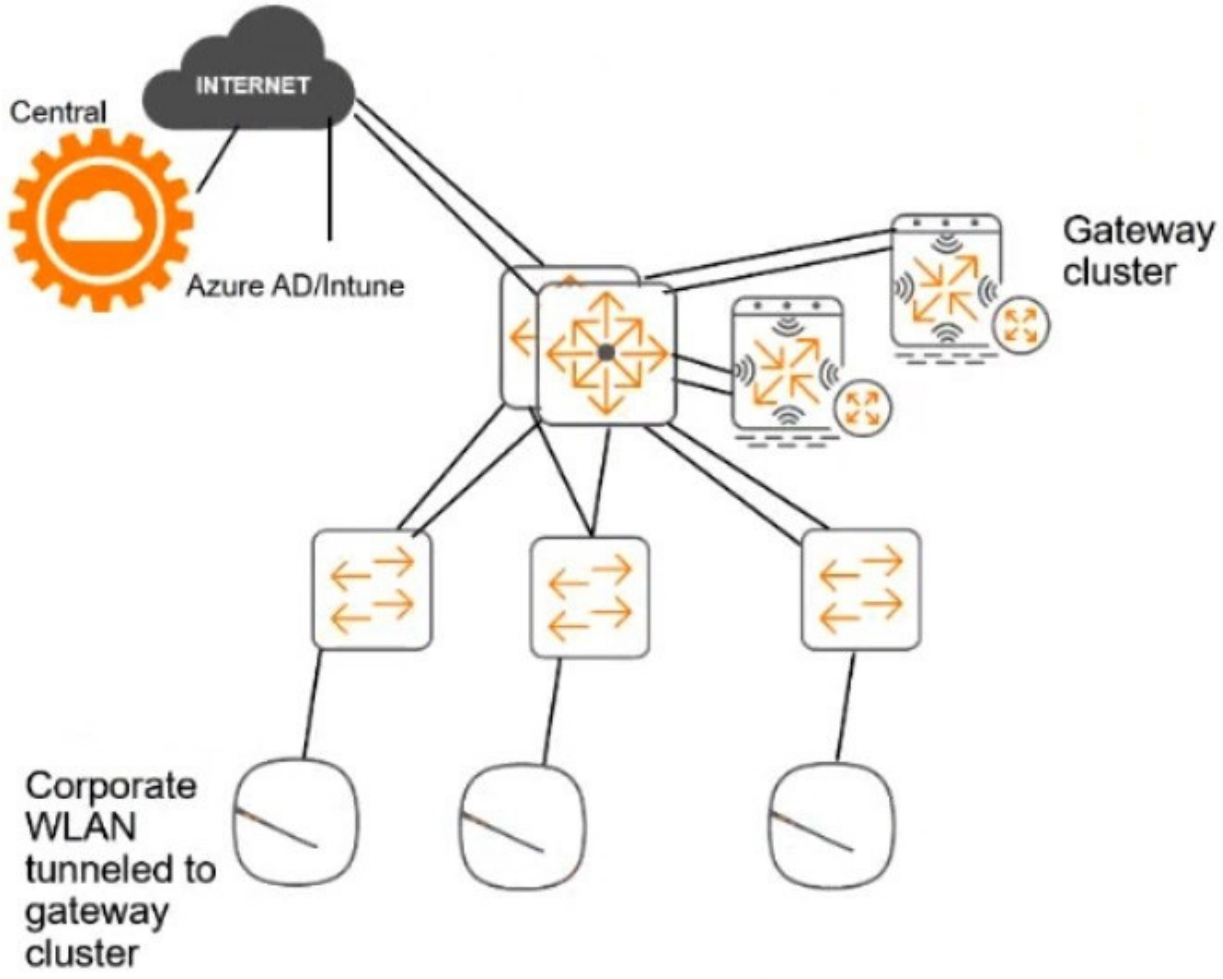
Deny other clients access

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 5

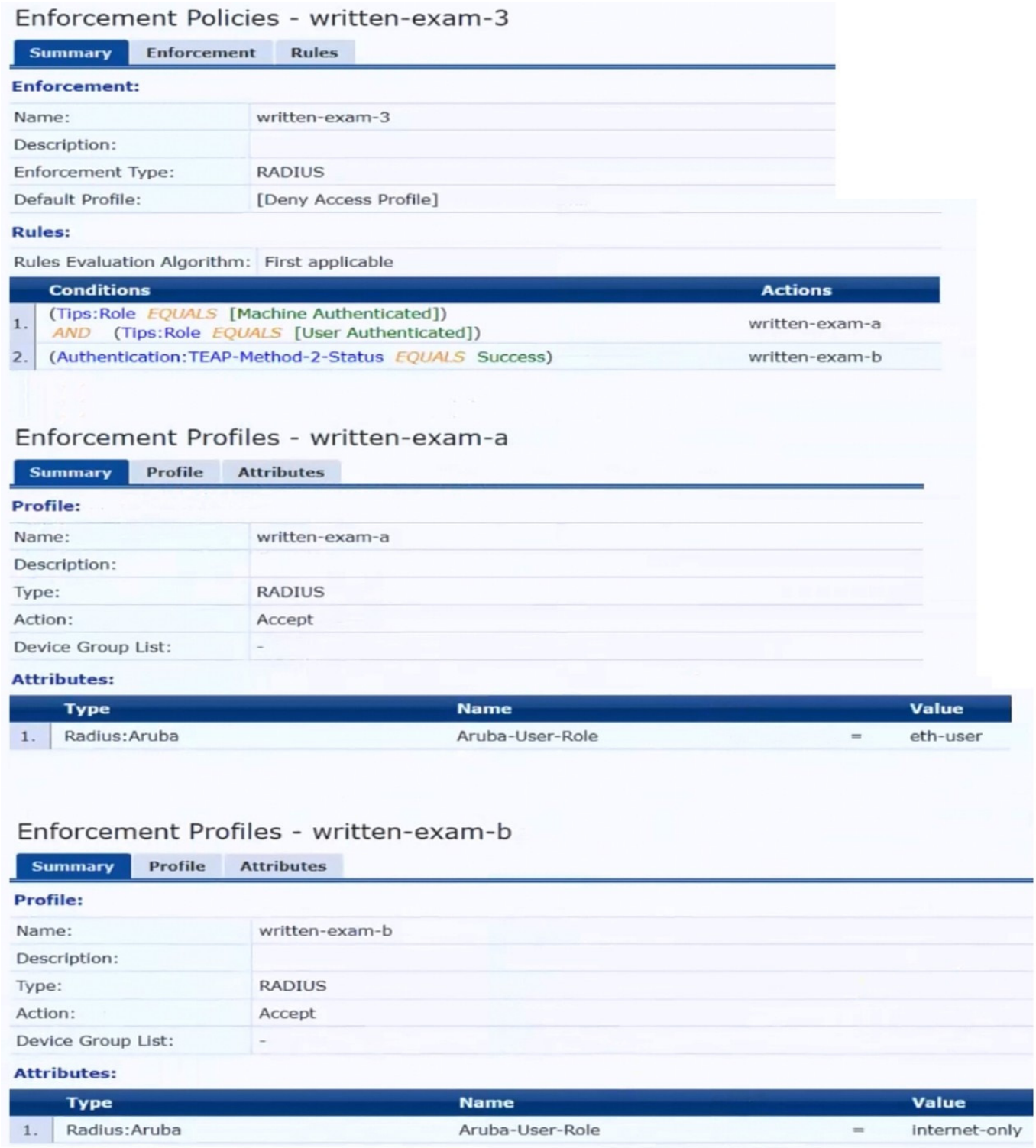
Refer to the scenario.

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: The gateway cluster has two gateways with these IP addresses:



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

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.

You are setting up the UBT zone on an AOS-CX switch.

Which IP addresses should you define in the zone?

A. Primary controller = 10.20.4.21; backup controller = 10.20.4.22

B. [Primary controller = 198.51.100.14; backup controller = 10.20.4.21

C. Primary controller = 10 20 4 21: backup controller not defined

D. Primary controller = 10.20.20.254; backup controller, not defined

Correct Answer: A

To configure user-based tunneling (UBT) on an AOS-CX switch, you need to specify the IP addresses of the mobility gateways that will receive the tunneled traffic from the switch 1. The primary controller is the preferred gateway for the switch to establish a tunnel, and the backup controller is the alternative gateway in case the primary controller fails or becomes unreachable 1. The IP addresses of the gateways should be their system IP addresses, which are used for inter-controller communication and cluster discovery 2. In this scenario, the customer has a gateway cluster with two gateways, each with a system IP address on VLAN 4085. Therefore, the switch should use these system IP addresses as the primary and backup controllers for UBT. The IP addresses of the gateways on VLAN 20 and VLAN 4094 are not relevant for UBT, as they are used for user traffic and WAN connectivity, respectively 2. The VRRP IP address on VLAN 20 is also not applicable for UBT, as it is a virtual IP address that is not associated with any specific gateway 3. Therefore, the best option is to use 10.20.4.21 as the primary controller and 10.20.4.22 as the backup controller for UBT on the switch. This will ensure high availability and cluster discovery for the tunneled traffic from the switch to the gateway cluster.