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

Aruba Certified Network Security Expert Written

QUESTION 1

Refer to the scenario.

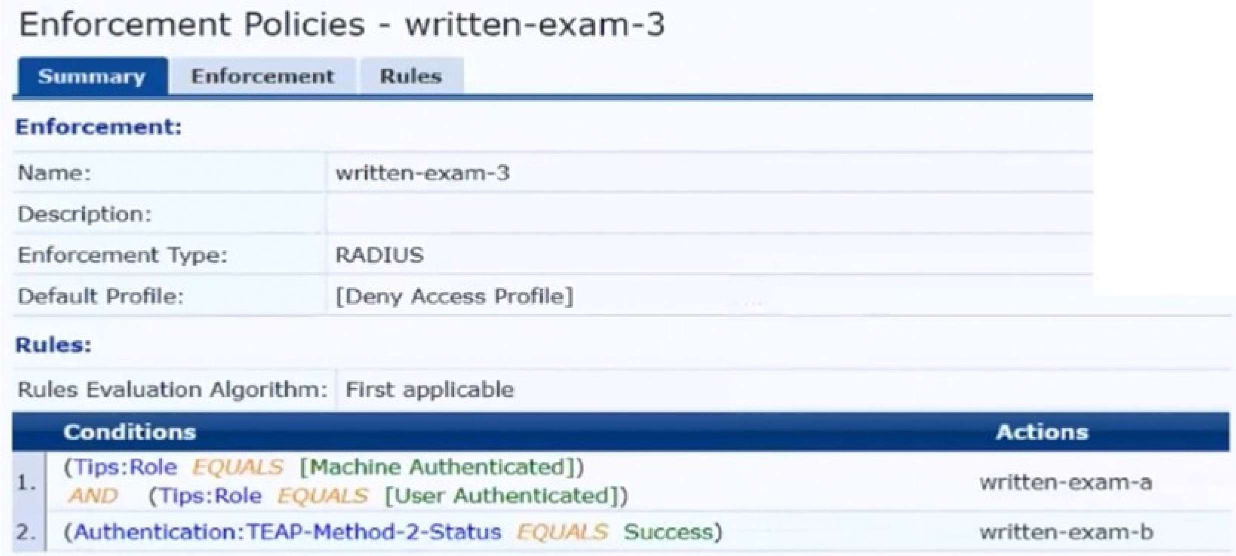
A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

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

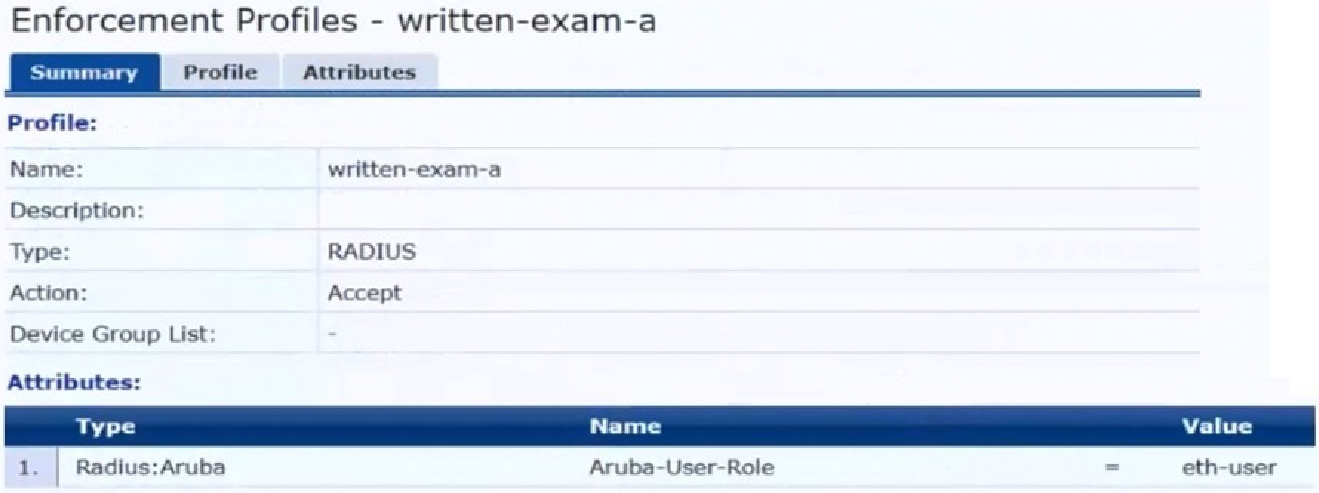
Enforcement:

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



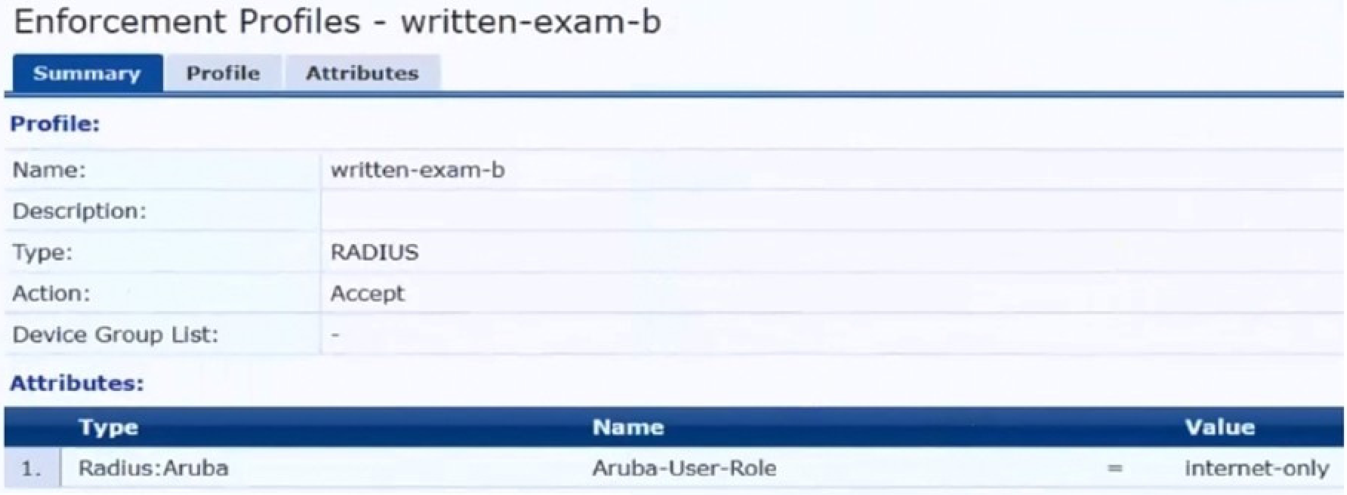
Enforcement Profiles - written-exam-a

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

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 are using the "myzone" name for the UBT zone.

Which is a valid minimal configuration for the AOS-CX port-access roles?

A. port-access role eth-internet gateway-zone zone myzone gateway-role eth-user

B. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet

C. port-access role eth-internet gateway-zone zone myzone gateway-role eth-internet vlan access 20

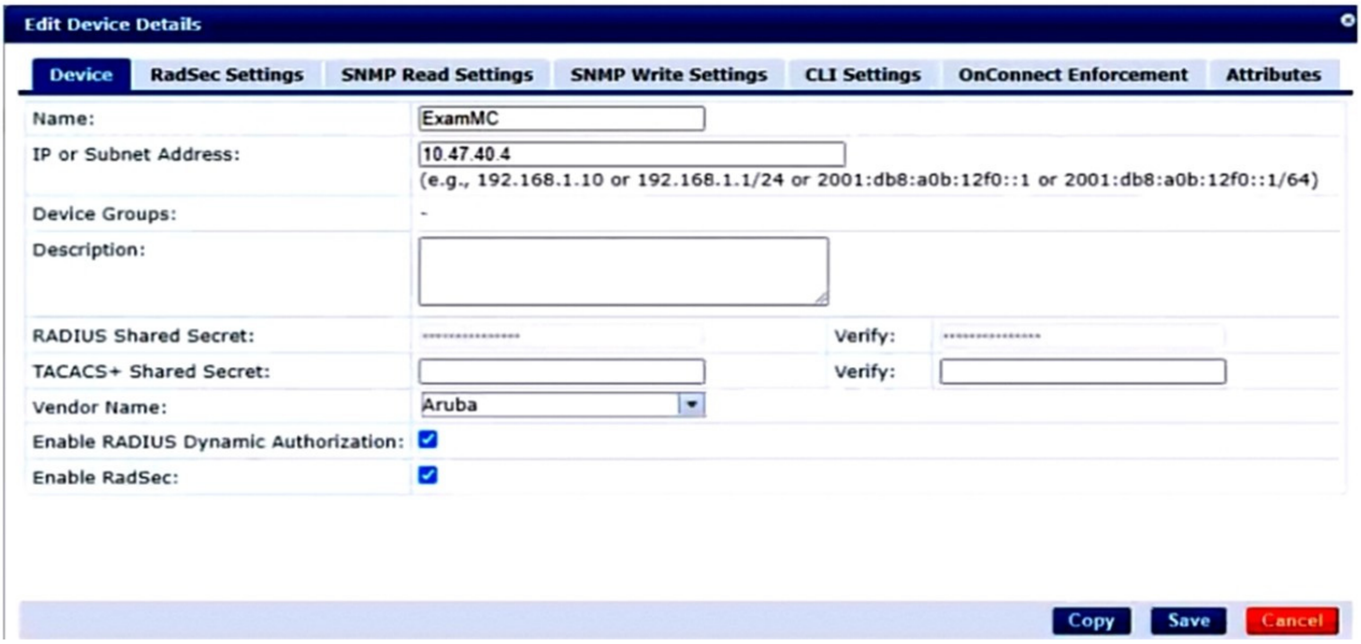
D. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet vlan access 20

Correct Answer: B

The UBT solution requires that the edge ports on the switches are configured in VLAN trunk mode, not access mode. This is because the UBT solution uses a special VLAN (VLAN 4095 by default) to encapsulate the user traffic and tunnel it to the gateway. The edge ports need to allow this VLAN as well as any other VLANs that are used for management or control traffic. Therefore, the edge ports should be configured as VLAN trunk ports and allow the necessary VLANs

QUESTION 2

A company has an Aruba ClearPass server at 10.47.47.8, FQDN radius.acnsxtest.local. This exhibit shows ClearPass Policy Manager\\'s (CPPM\\'s) settings for an Aruba Mobility Controller (MC).

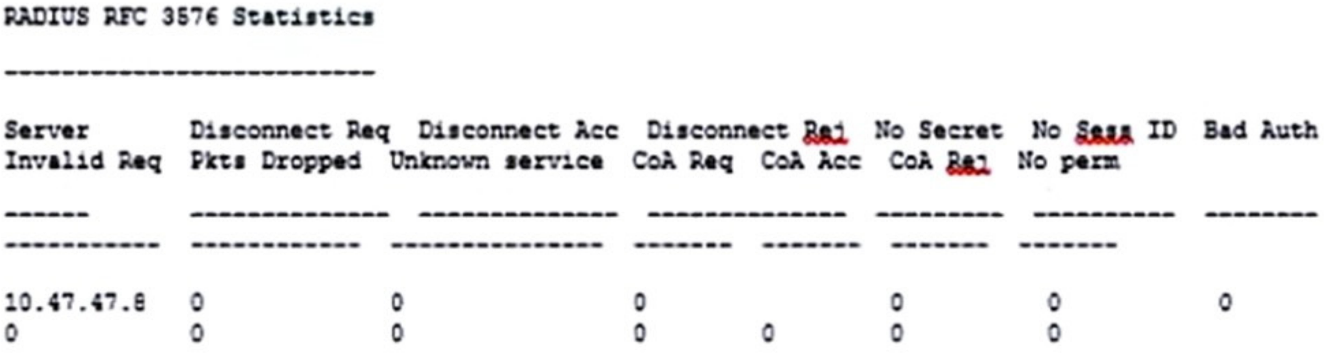


Name:	ExamMC		
IP or Subnet Address:	10.47.40.4 (e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)		
Device Groups:	-		
Description:			
RADIUS Shared Secret:	················	Verify:	················
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Aruba		
Enable RADIUS Dynamic Authorization:	☑		
Enable RadSec:	☑		

The MC is already configured with RADIUS authentication settings for CPPM, and RADIUS requests between the MC and CPPM are working. A network admin enters and commits this command to enable dynamic authorization on the MC:

aaa rfc-3576-server 10.47.47.8

But when CPPM sends CoA requests to the MC, they are not working. This exhibit shows the RFC 3576 server statistics on the MC:



```
RADIUS RFC 3576 Statistics
--------------------------

Server        Disconnect Req  Disconnect Acc  Disconnect Rej  No Secret  No Sess ID  Bad Auth
Invalid Req   Pkts Dropped   Unknown service   CoA Req   CoA Acc   CoA Rej   No perm

------        --------------  --------------  --------------  ---------  ----------  ---------
-----------   ------------   ---------------   -------   -------   -------   -------

10.47.47.8    0               0                0                         0          0           0
0             0               0                0         0         0         0
```

How could you fix this issue?

A. Change the UDP port in the MCs\\' RFC 3576 server config to 3799.

B. Enable RadSec on the MCs\\' RFC 3676 server config.

C. Configure the MC to obtain the time from a valid NTP server.

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

Correct Answer: A

Dynamic authorization is a feature that allows CPPM to send change of authorization (CoA) or disconnect messages to the MC to modify or terminate a user session based on certain conditions or events 1. Dynamic authorization uses the RFC 3576 protocol, which is an extension of the RADIUS protocol 2. To enable dynamic authorization on the MC, you need to configure the IP address and UDP port of the CPPM server as the RFC 3576 server on the MC 3. The default UDP port for RFC 3576 is 3799, but it can be changed on the CPPM server . The MC and CPPM must use the same UDP port for dynamic authorization to work properly 3. In this scenario, the MC is configured with the IP address of the CPPM server (10.47.47.8) as the RFC 3576 server, but it is using the default UDP port of 3799. However, according to the exhibit, the CPPM server is using a different UDP port of 1700 for dynamic authorization . This mismatch causes the CoA requests from CPPM to fail on the MC, as shown by the statistics . To fix this issue, you need to change the UDP port in the MCs\\' RFC 3576 server config to match the UDP port used by CPPM, which is 1700 in this case. Alternatively, you can change the UDP port in CPPM to match the default UDP port of 3799 on the MC. Either way, you need to ensure that both devices use the same UDP port for dynamic authorization .

QUESTION 3

Refer to the scenario.

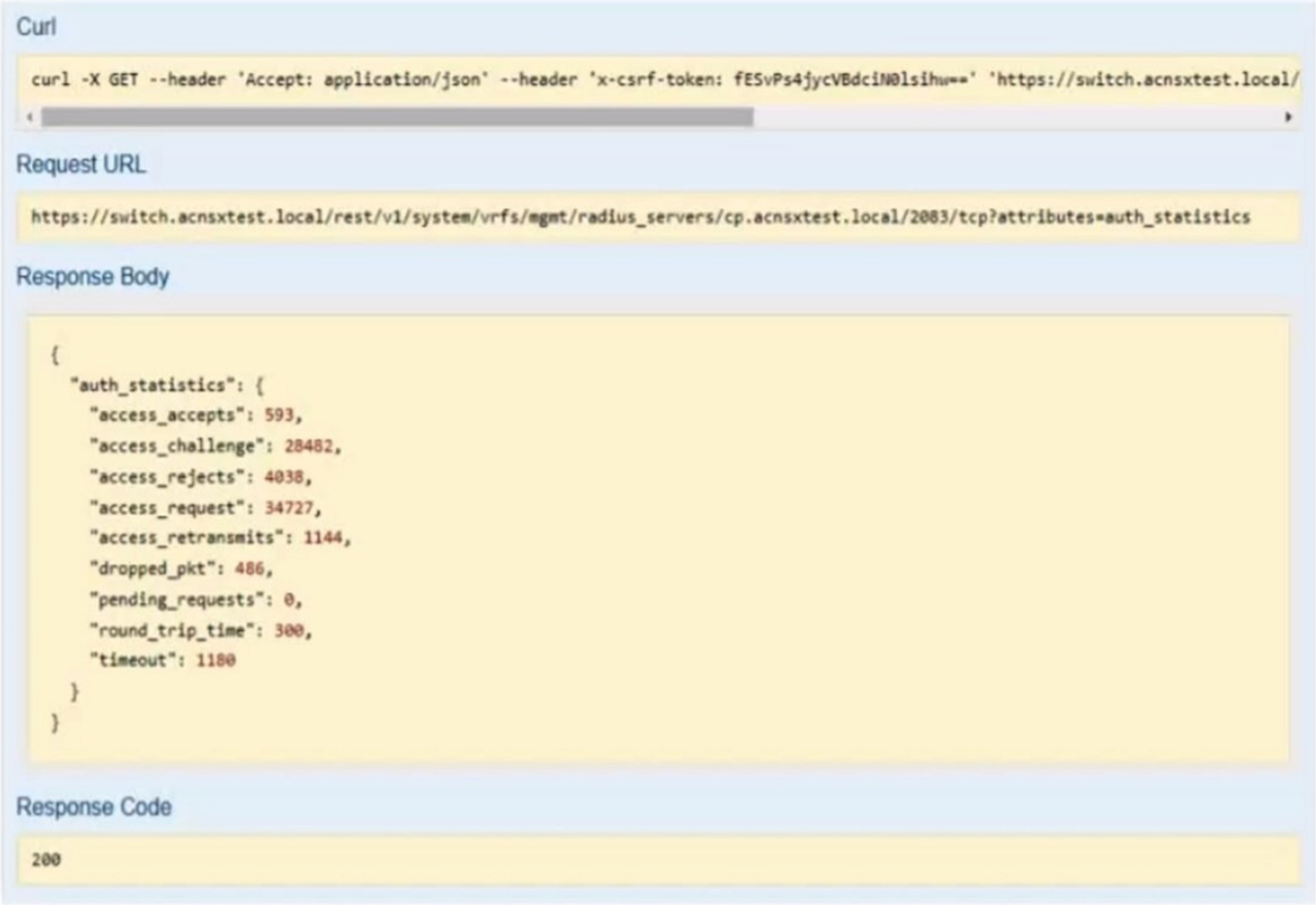
An organization wants the AOS-CX switch to trigger an alert if its RADIUS server (cp.acnsxtest.local) rejects an unusual number of client authentication requests per hour. After some discussions with other Aruba admins, you are still not sure

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.

You are helping the developer find the right URI for the monitor.

Refer to the exhibit.



Curl

```
curl -X GET --header 'Accept: application/json' --header 'x-csrf-token: fESvPs4jycVBdciN0lsihw==' 'https://switch.acnsxtest.local/
```

Request URL

```
https://switch.acnsxtest.local/rest/v1/system/vrfs/mgmt/radius_servers/cp.acnsxtest.local/2083/tcp?attributes=auth_statistics
```

Response Body

```
{
  "auth_statistics": {
    "access_accepts": 593,
    "access_challenge": 28482,
    "access_rejects": 4038,
    "access_request": 34727,
    "access_retransmits": 1144,
    "dropped_pkt": 486,
    "pending_requests": 0,
    "round_trip_time": 300,
    "timeout": 1180
  }
}
```

Response Code

```
200
```

You have used the REST API reference interface to submit a test call. The results are shown in the exhibit.

Which URI should you give to the developer?

A. /rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs

B. /rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs?attributes=access_rejects

C. /rest/v1/system/vrfs/mgmt/radius/_servers/cp.acnsxtest.local/2083/tcp

D. /rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs.access_rejects

Correct Answer: D

This is because this URI specifies the exact attribute that contains the number of access rejects from the RADIUS server, which is the information that the NAE script needs to monitor and trigger an alert.

A.

/rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatisti cs. This is not the correct URI because it returns the entire authstatistics object, which contains more information than the access rejects, such as

access accepts, challenges, timeouts, etc. This might make the NAE script more complex and inefficient to parse and process the data.

B.

/rest/v1/system/vrfs/mgmt/radius/servers/cp.acnsxtest.local/2083/tcp?attributes=authstatistics?attributes=access_rejects. This is not a valid URI because it has two question marks, which is a syntax error. The question mark is used to

indicate the start of the query string, which can have one or more parameters separated by ampersands. The correct way to specify multiple attributes is to use a comma-separated list after the question mark, such as ?

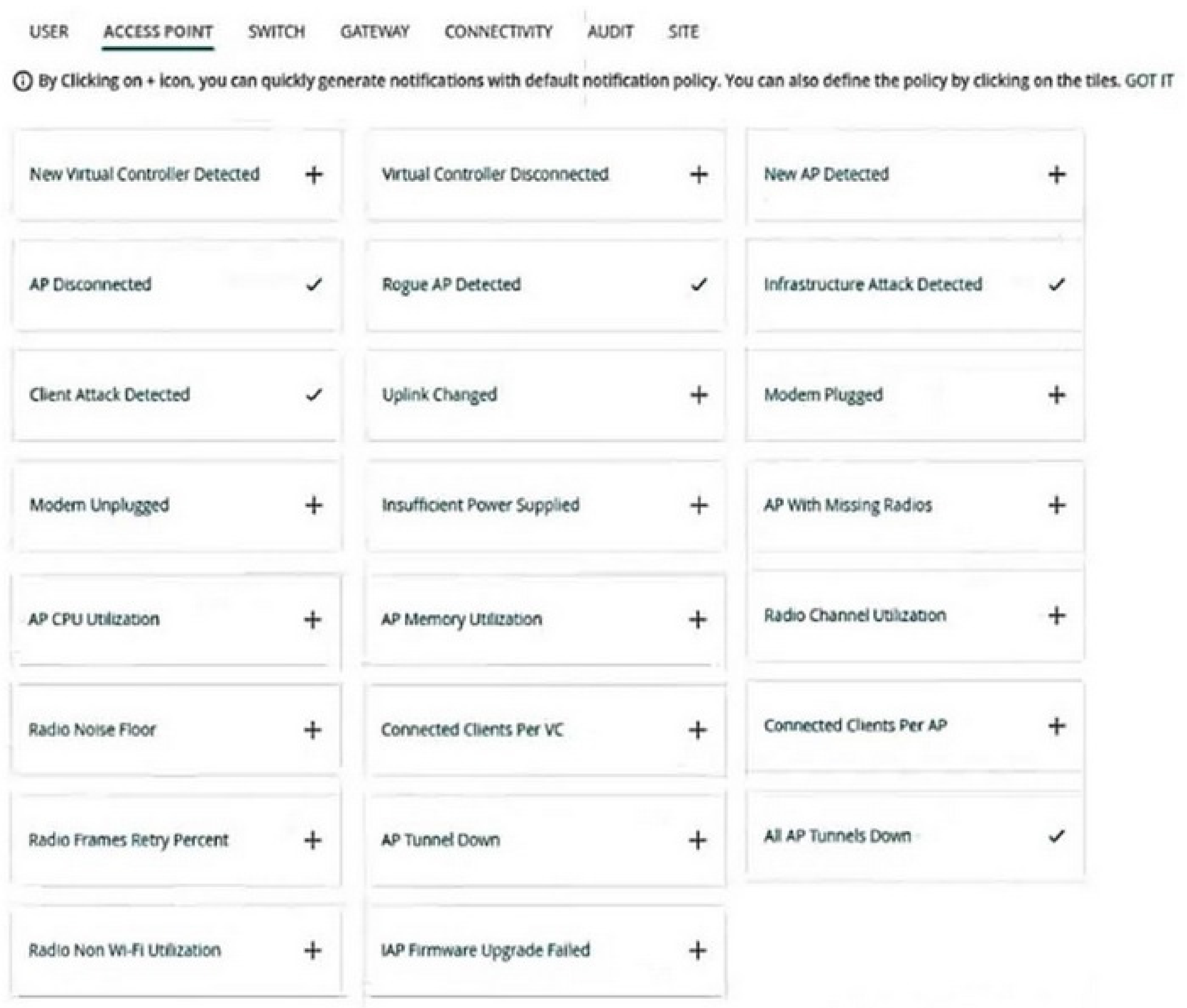
attributes=attr1,attr2,attr3.

C. /rest/v1/system/vrfs/mgmt/radius/_servers/cp.acnsxtest.local/2083/tcp. This is not a valid URI because it has an extra underscore before servers, which is a typo. The correct resource name is servers, not _servers. Moreover, this URI does

not specify any attributes, which means it will return the default attributes of the RADIUS server object, such as name, port, protocol, etc., but not the authstatistics or access_rejects.

QUESTION 4

A customer has an AOS 10 architecture, which includes Aruba APs. Admins have recently enabled WIDS at the high level. They also enabled alerts and email notifications for several events, as shown in the exhibit.



USER | ACCESS POINT | SWITCH | GATEWAY | CONNECTIVITY | AUDIT | SITE

ⓘ By Clicking on + icon, you can quickly generate notifications with default notification policy. You can also define the policy by clicking on the tiles. GOT IT

New Virtual Controller Detected +	Virtual Controller Disconnected +	New AP Detected +
AP Disconnected ✓	Rogue AP Detected ✓	Infrastructure Attack Detected ✓
Client Attack Detected ✓	Uplink Changed +	Modem Plugged +
Modem Unplugged +	Insufficient Power Supplied +	AP With Missing Radios +
AP CPU Utilization +	AP Memory Utilization +	Radio Channel Utilization +
Radio Noise Floor +	Connected Clients Per VC +	Connected Clients Per AP +
Radio Frames Retry Percent +	AP Tunnel Down +	All AP Tunnels Down ✓
Radio Non Wi-Fi Utilization +	IAP Firmware Upgrade Failed +	

Admins are complaining that they are getting so many emails that they have to ignore them, so they are going to turn off all notifications.

What is one step you could recommend trying first?

A. Send the email notifications directly to a specific folder, and only check the folder once a week.

B. Disable email notifications for Roque AP, but leave the Infrastructure Attack Detected and Client Attack Detected notifications on.

C. Change the WIDS level to custom, and enable only the checks most likely to indicate real threats.

D. Disable just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert.

Correct Answer: C

According to the AOS 10 documentation1, WIDS is a feature that monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. WIDS can be configured at different levels, such as low, medium, high, or custom. The higher the level, the more checks are enabled and the more alerts are generated. However, not all checks are equally relevant or indicative of real threats. Some checks may generate false positives or unnecessary alerts that can overwhelm the administrators and reduce the effectiveness of WIDS. Therefore, one step that could be recommended to reduce the number of email notifications is to change the WIDS level to custom, and enable only the checks most likely to indicate real threats. This way, the administrators can fine-tune the WIDS settings to suit their network environment and security needs, and avoid getting flooded with irrelevant or redundant alerts. Option C is the correct answer. Option A is incorrect because sending the email notifications directly to a specific folder and only checking the folder once a week is not a good practice for security management. This could lead to missing or ignoring important alerts that require immediate attention or action. Moreover, this does not solve the problem of getting too many emails in the first place. Option B is incorrect because disabling email notifications for Rogue AP, but leaving the Infrastructure Attack Detected and Client Attack Detected notifications on, is not a sufficient solution. Rogue APs are unauthorized access points that can pose a serious security risk to the network, as they can be used to intercept or steal sensitive data, launch attacks, or compromise network performance. Therefore, disabling email notifications for Rogue APs could result in missing critical alerts that need to be addressed. Option D is incorrect because disabling just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert, is not a valid assumption. The Infrastructure Attack Detected alert covers a broad range of attacks that target the network infrastructure, such as deauthentication attacks, spoofing attacks, denial-of-service attacks, etc. The Rogue AP and Client Attack Detected alerts are more specific and focus on detecting and classifying rogue devices and clients that may be involved in such attacks. Therefore, disabling these alerts could result in losing valuable information about the source and nature of the attacks.

QUESTION 5

A company has Aruba gateways and wants to start implementing gateway IDS/IPS. The customer has selected Block for the Fail Strategy.

What might you recommend to help minimize unexpected outages caused by using this particular fall strategy?

A. Configuring a relatively high threshold for the gateway threat count alerts

B. Making sure that the gateways have formed a cluster and operate in default gateway mode

C. Setting the IDS or IPS policy to the least restrictive option, Lenient

D. Enabling alerts and email notifications for events related to gateway IPS engine utilization and errors

Correct Answer: D

The correct answer is D. Enabling alerts and email notifications for events related to gateway IPS engine utilization and errors. Gateway IDS/IPS is a feature that allows the Aruba gateways to monitor and block malicious or unwanted traffic based on predefined or custom rules 1. The Fail Strategy is a setting that determines how the gateways handle traffic when the IPS engine fails or crashes 2. The Block option means that the gateways will stop forwarding traffic until the IPS engine recovers, while the Bypass option means that the gateways will continue forwarding traffic without inspection 2. The Block option provides more security, but it also increases the risk of network outages if the IPS engine fails frequently or for a long time 2. To minimize this risk, it is recommended to enable alerts and email notifications for events related to gateway IPS engine utilization and errors 3. This way, the network administrators can be informed of any issues with the IPS engine and take appropriate actions to restore or troubleshoot it 3. The other options are not correct or relevant for this issue: Option A is not correct because configuring a relatively high threshold for the gateway threat count alerts would not help minimize unexpected outages caused by using the Block option. The gateway threat count alerts are used to notify the network administrators of the number of threats detected by the IPS engine, but they do not affect how the gateways handle traffic when the IPS engine fails 4. Option B is not correct because making sure that the gateways have formed a cluster and operate in default gateway mode would not help minimize unexpected outages caused by using the Block option. The gateway cluster mode is used to provide high availability and load balancing for the gateways, but it does not affect how the gateways handle traffic when the IPS engine fails . The default gateway mode is used to enable routing and NAT functions on the gateways, but it does not affect how the gateways handle traffic when the IPS engine fails . Option C is not correct because setting the IDS or IPS policy to the least restrictive option, Lenient, would not help minimize unexpected outages caused by using the Block option. The IDS or IPS policy is used to define what rules are applied by the IPS engine to inspect and block traffic, but it does not affect how the gateways handle traffic when the IPS engine fails 2. The Lenient option contains fewer and older rules than the Moderate or Strict options, which means that it

provides less security and more false negatives .