HPE2-W05.VCEplus.premium.exam.115q

Number: HPE2-W05
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

HPE2-W05

Implementing Aruba IntroSpect

Version 1.0

Exam A

QUESTION 1
You are troubleshooting ClearPass with IntroSpect, and you notice that in Access Tracker the IntroSpect Logon Logoff actions profile is executing. However, the ClearPass Log Source on the IntroSpect Analyzer is showing dropped entries.

Would this be a good troubleshooting step? (Confirm that the ClearPass context action is sending the User name, MAC Address, Entity Type, and User Role)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
You are troubleshooting ClearPass with IntroSpect, and you notice that in Access Tracker the IntroSpect Logon Logoff actions profile is executing. However, the ClearPass Log Source on the IntroSpect Analyzer is showing dropped entries.

Would this be a good troubleshooting step? (Confirm that the ClearPass context action is sending the User name, IP Address, Entity Type, and User Role)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
You are troubleshooting ClearPass with IntroSpect, and you notice that in Access Tracker the IntroSpect Logon Logoff actions profile is executing. However, the ClearPass Log Source on the IntroSpect Analyzer is showing dropped entries.

Would this be a good troubleshooting step? (Confirm that the ClearPass context action is sending the User name, MAC Address, IP Address, and Time Stamp)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
While troubleshooting integration between ClearPass and IntroSpect, you notice that there are no log events for either THROUGHPUT or ERROR in the ClearPass log source on the IntroSpect Analyzer. You are planning your troubleshooting actions.

Is this something you should check? (Under Cluster-Wide Parameters on the ClearPass Publisher, make sure Post-Auth v2 is enabled.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
While troubleshooting integration between ClearPass and IntroSpect, you notice that there are no log events for either THROUGHPUT or ERROR in the ClearPass log source on the IntroSpect Analyzer. You are planning your troubleshooting actions.

Is this something you should check? (Check the authentication service being used in ClearPass for the Login – Logout enforcement policy.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
While looking at the conversation page you notice some strange network behavior, such as DNS requests coming inbound from external DNS servers. Could this be the reason why? (One of your Packet Processors may be over subscribed and is dropping packets.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.hpe.com/t5/Comware-Based/Meaning-of-FFP-in-packet-drop/td-p/6071115#.XIH4nOdR2kw

QUESTION 7
While looking at the conversation page you notice some strange network behavior, such as DNS requests coming inbound from external DNS servers. Could this be the reason why? (You have your network tap positioned wrong, and you are just getting outside data.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
While validating the data sources in a new IntroSpect installation, you have confirmed that the network tap data is correct and there are AMON log sources for both firewall and DNS. When you lock in the Entity360, you see the usernames from Active Directory.

However, when you look under E360 > activity > for any user accounts there is no information under “Activity Card” and “Authentication” for any user. When you filter the Entity360 for IP address and look at the Activity screen you do see activity on the “Activity Card”.

Could this be a reason why you do not see the information but do not see activity? (The log broker could be configured incorrectly and not sending authentication logs to IntroSpect.)

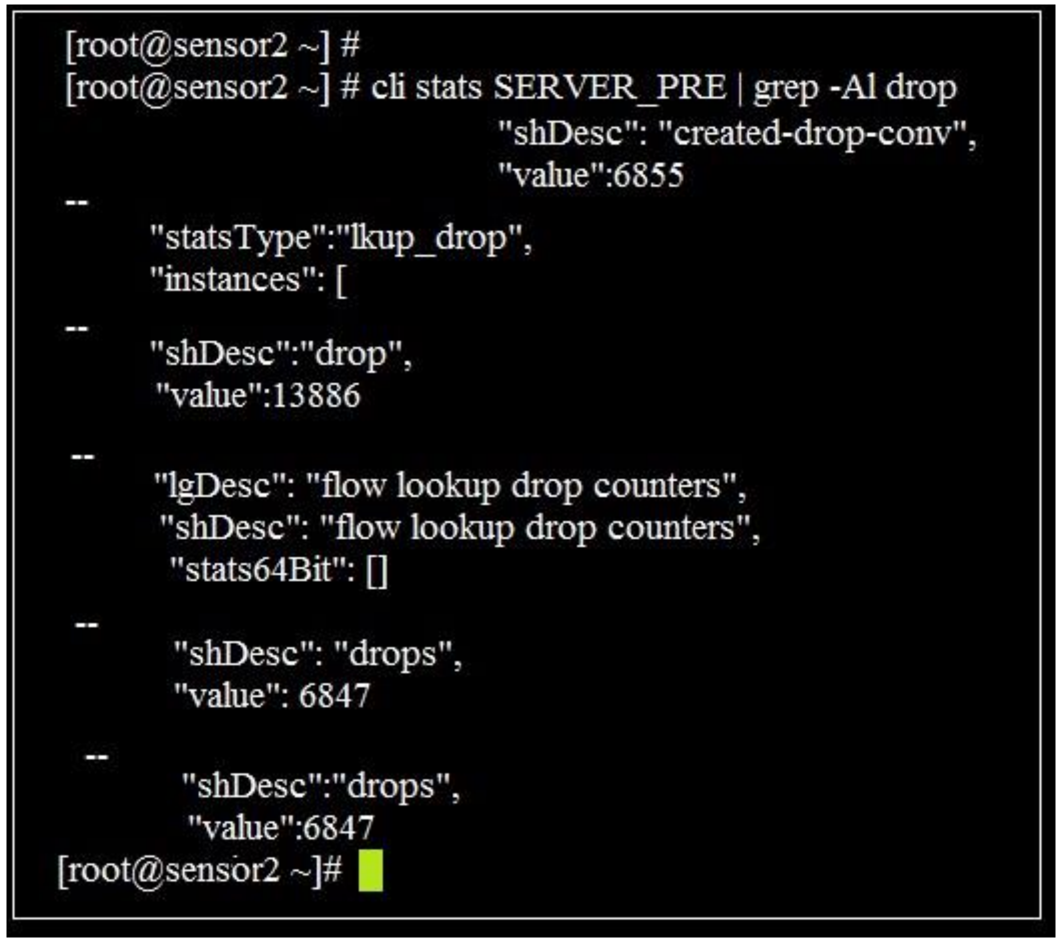
A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9

Refer to the exhibit.



```
[root@sensor2 ~] #
[root@sensor2 ~] # cli stats SERVER_PRE | grep -Al drop
                                        "shDesc": "created-drop-conv",
                                        "value":6855
--
        "statsType":"lkup_drop",
        "instances": [
--
        "shDesc":"drop",
         "value":13886

 --
        "lgDesc": "flow lookup drop counters",
         "shDesc": "flow lookup drop counters",
          "stats64Bit": []
 --
          "shDesc": "drops",
          "value": 6847
  --
           "shDesc":"drops",
            "value":6847
[root@sensor2 ~]#
```

You are monitoring a new virtual packet processor with a network tap. You run the command “cli stats SERVER_PRE | gre-a1 drop” and then return an hour later and run the same command, but notice there is a significant increase in the number dropped packets.

Could this be a reason for the increase? (The Packet Processor may not be allocated the proper number of memory allocated on the VM server for the size of the TAP.)

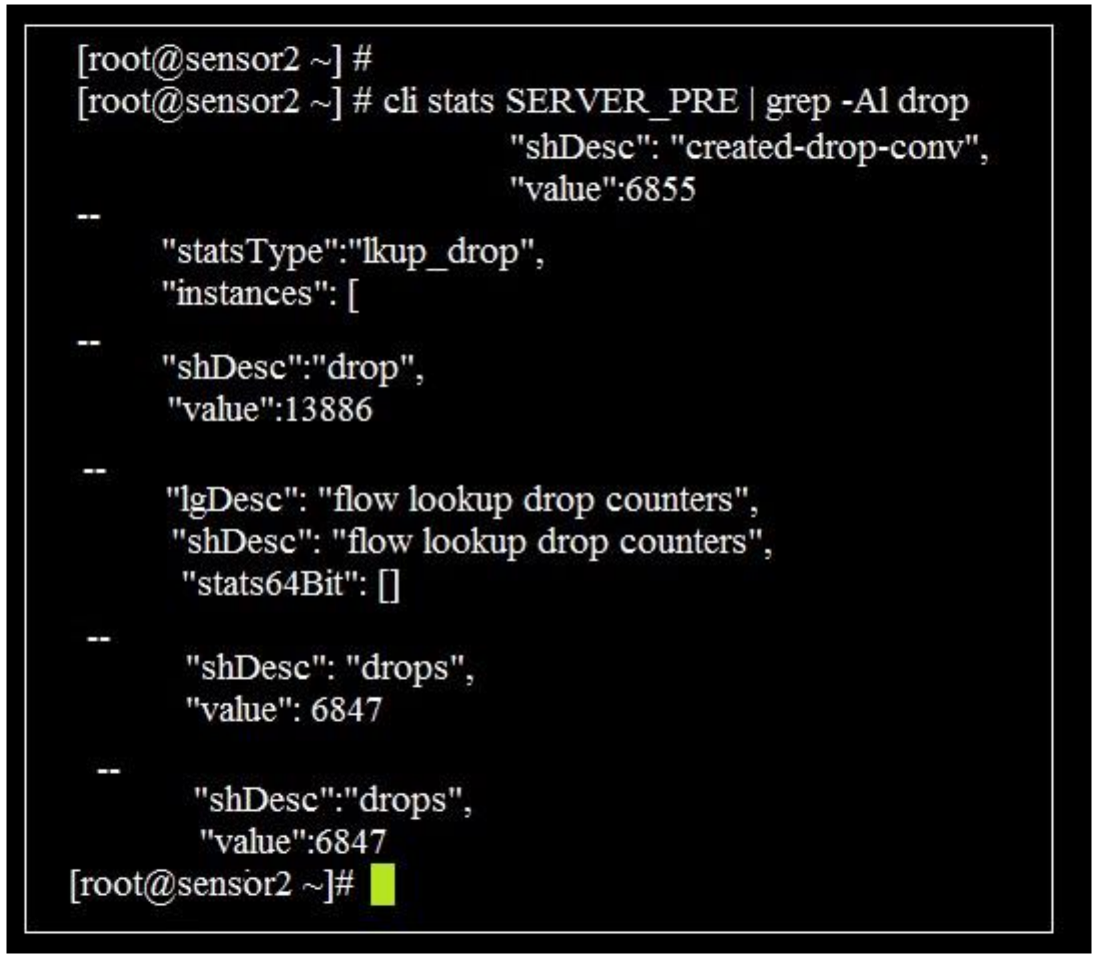
A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

Refer to the exhibit.



```
[root@sensor2 ~] #
[root@sensor2 ~] # cli stats SERVER_PRE | grep -A1 drop
                                   "shDesc": "created-drop-conv",
                                   "value":6855
--
       "statsType":"lkup_drop",
       "instances": [
--
       "shDesc":"drop",
        "value":13886

 --
        "lgDesc": "flow lookup drop counters",
         "shDesc": "flow lookup drop counters",
          "stats64Bit": []

 --
          "shDesc": "drops",
          "value": 6847

  --
           "shDesc":"drops",
            "value":6847
[root@sensor2 ~]# █
```

You are monitoring a new virtual packet processor with a network tap. You run the command “cli stats SERVER_PRE | gre-a1 drop’ and then return an hour later and run the same command, but notice there is a significant increase in the number dropped packets.

Could this be a reason for the increase? (The Packet Processor may not be allocated the proper number of CPUs allocated on the VM server for the size of the TAP.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

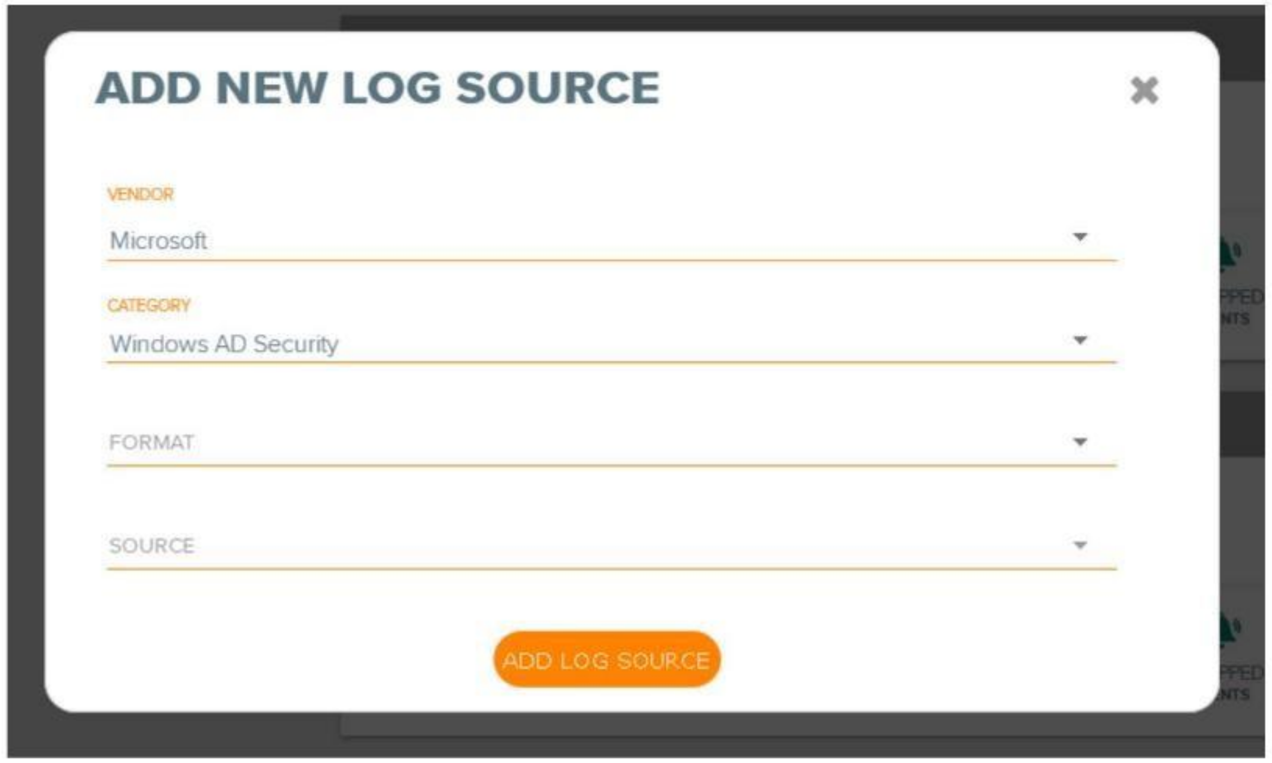
QUESTION 11
When IntroSpect ingests logs from different sources, it standardizes and catalogs the information. When it stores log data, it currently categorizes it into one of four standard schemas. Are these the four standard schemas? (VPN access data, email data, network data, and authentication data.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 12

Refer to the exhibit.



ADD NEW LOG SOURCE

VENDOR
Microsoft

CATEGORY
Windows AD Security

FORMAT

SOURCE

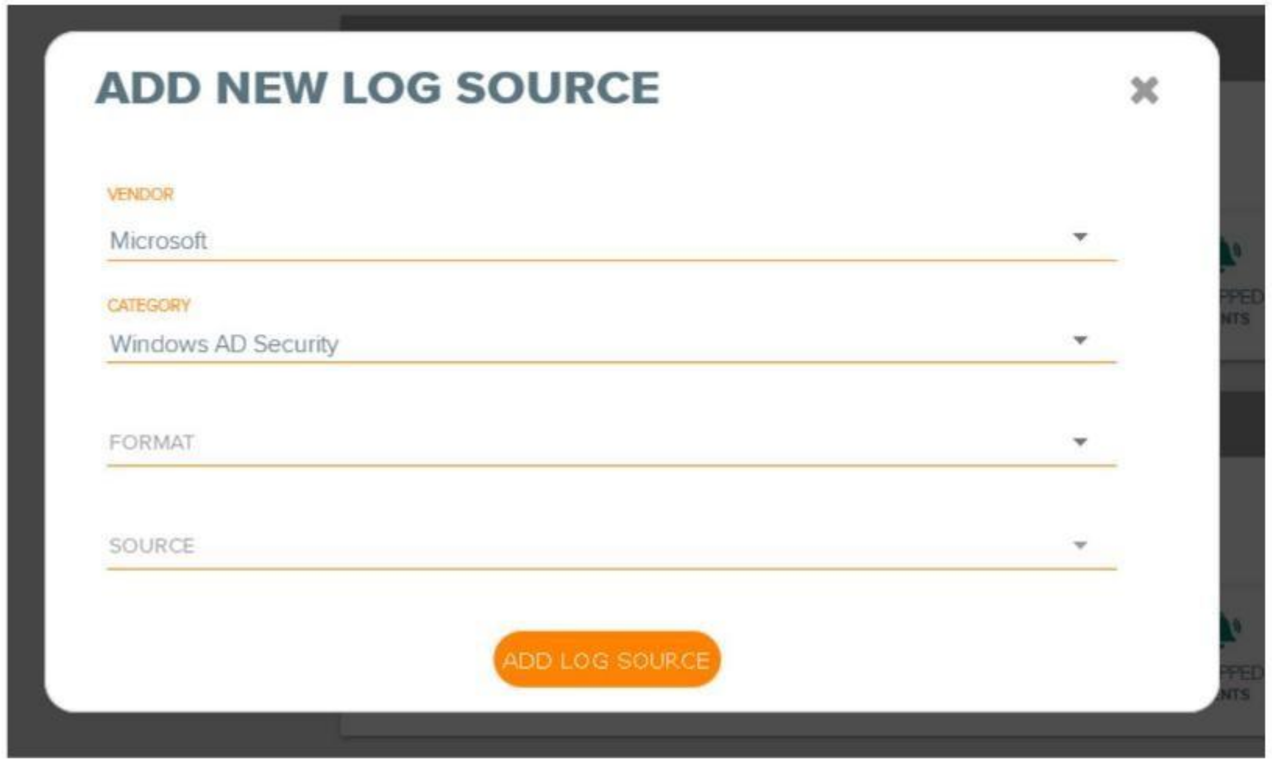
An IntroSpect admin is configuring an Aruba IntroSpect Packet Processor to add Microsoft AD server as a log source for analyzing the AD server logs. Are these correct Format and Source options? (Format = Snare, and Source Type = Syslog.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Refer to the exhibit.



ADD NEW LOG SOURCE

VENDOR
Microsoft

CATEGORY
Windows AD Security

FORMAT

SOURCE

An IntroSpect admin is configuring an Aruba IntroSpect Packet Processor to add Microsoft AD server as a log source for analyzing the AD server logs. Are these correct Format and Source options? (Format = Standard, and Source Type = Syslog.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
You receive an email alert that a Packet Processor forwarding AMON data at a remote site to a cloud-based Analyzer has stopped communicating.
Is this a valid step to try to fix the issue? (Log into the Packet Processor and check the Alerts page to make sure that the alert is still valid.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
You receive an email alert that a Packet Processor forwarding AMON data at a remote site to a cloud-based Analyzer has stopped communicating.
Is this a valid step to try to fix the issue? (Contact the firewall administrator from the site and see if any rules have changed that may be blocking TCP port 389.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
You are configuring a ClearPass Cluster to send endpoint context to an IntroSpect Analyzer for the wireless network. You want to test the setup after you have installed the XML file with the enforcement profiles and actions. Can this method be used to test that the setup is functioning correctly?

(Connect to the wireless network, and send a test authentication from a test device/user in the network. Observe the results in Access Tracker.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
You are one of the system administrators in your company, and you are assigned to monitor the IntroSpect system for alarms. Is this a correct statement about alarms? (The alarm bell icon on the header bar indicates active alarms, and clicking on it will take you to the Alerts>page.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
You are one of the system administrators in your company, and you are assigned to monitor the IntroSpect system for alarms. Is this a correct statement about alarms? (You must navigate to the IntroSpect Analyzer Menu>Alerts page to see if there are any alarms.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/26587/Default.aspx

QUESTION 19
You are one of the system administrators in your company, and you are assigned to monitor the IntroSpect system for alarms. Is this a correct statement about alarms? (To see the alarms, navigate to the IntroSpect Analyzer Menu> System Status>Alerts> page.)

A. Yes
B. No

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/26587/Default.aspx

QUESTION 20
You are one of the system administrators in your company, and you are assigned to monitor the IntroSpect system for alarms. Is this a correct statement about alarms? (A memory_full alarm will fire when there is less than 1 GB of free memory for more than thirty minutes.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=27259
(2.4 user guide)

QUESTION 21
An IntroSpect installation has been up for a day. While validating the log sources, you see an Aruba Firewall log source configured on a Packet Processor that has shown up on the interface in the analyzer.

While evaluating conversation data you notice there is no eflow data from AMON. You log into the controller and confirm there is user activity in the dashboard. Would this be a correct statement about this situation? (The log source on the Packet Processor may not be pointed to the analyzer IP address.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=27259

QUESTION 22
An IntroSpect installation has been up for a day. While validating the log sources, you see an Aruba Firewall log source configured on a Packet Processor that has shown up on the interface in the analyzer.

While evaluating conversation data you notice there is no eflow data from AMON. You log into the controller and confirm there is user activity in the dashboard.
Would this be a correct statement about this situation? (The Packet Processor has been configured correctly.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
A customer with approximately 200 users in Active Directory, is running Aruba Mobility Controllers, Palo Alto firewalls, and Pulse Secure VPN and InfoBlox DNS on their network. They would like to implement the 2RU Fixed Configuration Analyzer Standard Edition.

Would this be a good response to the customer? (The Standard Edition will work for this customer as long as they do not want to capture the InfoBlox DNS logs.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A customer with approximately 200 users in Active Directory, is running Aruba Mobility Controllers, Palo Alto firewalls, and Pulse Secure VPN and InfoBlox DNS on their network. They would like to implement the 2RU Fixed Configuration Analyzer Standard Edition.

Would this be a good response to the customer? (The 2RU Fixed Configuration Analyzer should work for this smaller customer. However, they will need the Advanced Edition to monitor the DNS server.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
You need to deploy IntroSpect Analyzer in your existing network. You are planning to configure logs from multiple systems around your network. Can this 3rd-party tool collect the logs and push them to Analyzer? (IBM QRadar SIEM will push logs to IntroSpect.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: IBM QRadar SIEM will push logs to IntroSpect

QUESTION 26
You need to deploy IntroSpect Analyzer in your existing network. You are planning to configure logs from multiple systems around your network. Can this 3rd-party tool collect the logs and push them to Analyzer? (Splunk Enterprise will allow push notifications.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
In a meeting with a customer that runs a fully automated manufacturing facility that is connected to the business and corporate offices, the operations manager asks why they need IntroSpect to monitor the manufacturing network. Is this a reason they should monitor the manufacturing network security? (Because the controllers and sensors do not store customer data or corporate intellectual property, even if the automation network was to be breached it would not expose anything valuable.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

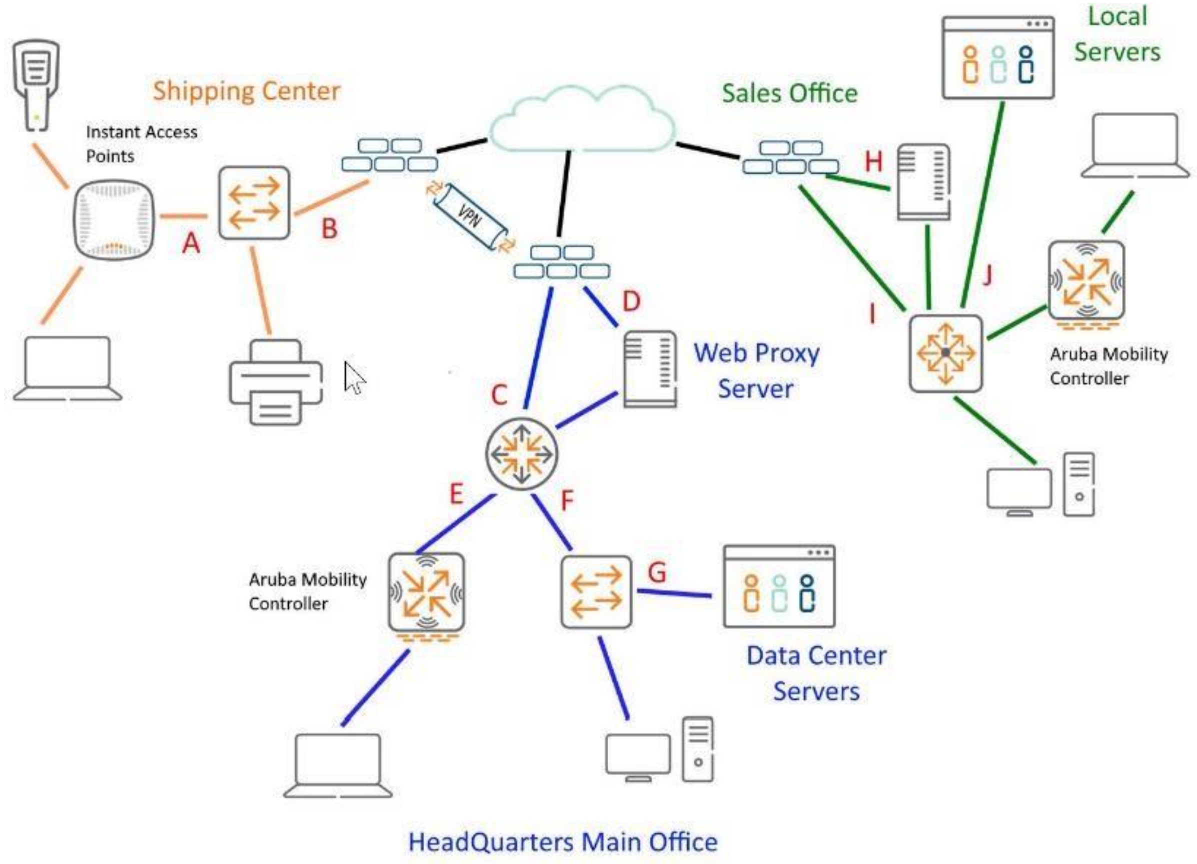
QUESTION 28
In a meeting with a customer that runs a fully automated manufacturing facility that is connected to the business and corporate offices, the operations manager asks why they need IntroSpect to monitor the manufacturing network. Is this a reason they should monitor the manufacturing network security? (The devices on the automation network are vulnerable to attack because they are highly functional and could be weaponized by an attacker and used to attack the corporate network.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.arubanetworks.com/assets/ds/DS_IntroSpect.pdf

QUESTION 29
Refer to the exhibit.



Given the network diagram, would this be a proper location for a network tap? (Port G at the Head Quarters Site would expose all East/West traffic bound for the data center.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
You deploy IntroSpect Analyzer in your existing network. You want to monitor email for suspect malware activity. Would this action be supported by IntroSpect? (Deploy a supported DNP like Proofpoint Email Protection, and integrate with The IntroSpect Analyzer.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 You deploy IntroSpect Analyzer in your existing network. You want to monitor email for suspect malware activity. Would this action be supported by IntroSpect? (Deploy Splunk SIEM to gather logs from the email servers.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 You are planning to configure ClearPass to send endpoint context to IntroSpect. You need to create a checklist of functions that must be enabled in ClearPass to support this. Is this an option that is required? (System Monitor Service.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33 You are planning to configure ClearPass to send endpoint context to IntroSpect. You need to create a checklist of functions that must be enabled in ClearPass to support this. Is this an option that is required? (Ingress Event Processing.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
You are planning to configure ClearPass to send endpoint context to IntroSpect. You need to create a checklist of functions that must be enabled in ClearPass to support this. Is this an option that is required? (Time Source Now as part of the authorization in the service.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiBra-C-_HgAhWLsKQKHQ4yDkkQFjABegQICBAC&url=http%3A%2F%2Fsupport.arubanetworks.com%2FDocumentation%2Ftabid%2F77%2FDMXModule%2F512%2FCommand%2FCore_Download%2FMethod%2Fattachment%2FDefault.aspx%3FEntryId%3D33268&usg=AOvVaw3plzLBTQalED4qNGbdU1Dx

QUESTION 35
You are a security analyst for a company where an Aruba infrastructure, such as Controllers, ClearPass, and Airwave, has been deployed. The company has recently deployed Aruba IntroSpect for security analytics. You are trying to understand the functionality of three components: Analyzer, Compute Node(CN), and Packet Processor of the IntroSpect system. Is this a good description of the functions of the Analyzer Node in the system? (The Analyzer Node is the center of the system, providing all of the control and interface to the other components.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A company wants to integrate ClearPass with the IntroSpect. Is this a supported version? (ClearPass 6.7.4.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A company wants to integrate ClearPass with the IntroSpect. Is this a supported version? (ClearPass 6.7.3.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
While discussing network security with an associate, the associate asks why a company would need internal monitoring when they have firewalls and Wireless Intrusion Protection configured. Is this an appropriate response? (You point out that while these security measures are required, there are other attack vectors in a network that are simply not protected by these.)

A. Yes

B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
While reviving the logs at a customer site you notice that one particular device is accessing multiple servers in the environment, using a number of different user accounts. When you question the IT admin, they tell you that the computer is a JumpBox and running software used to monitor all of the servers in the environment.
Would this be a logical next step? (You can safely ignore this activity as this is normal behavior for a JumpBox.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

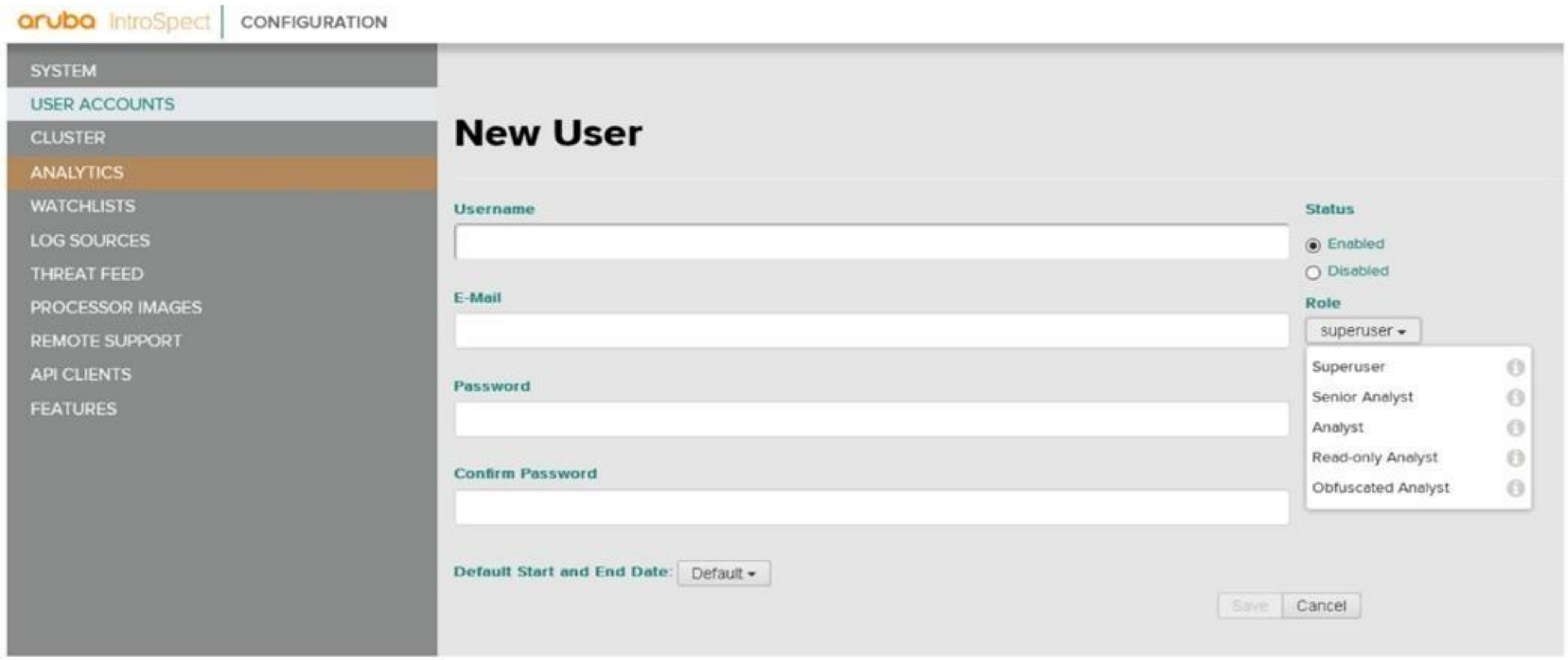
QUESTION 40
While reviving the logs at a customer site you notice that one particular device is accessing multiple servers in the environment, using a number of different user accounts. When you question the IT admin, they tell you that the computer is a JumpBox and running software used to monitor all of the servers in the environment.
Would this be a logical next step? (As a next step, you should audit all of the accounts that are being used on the JumpBox to determine if the JumpBox is being accessed by unauthorized accounts.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Refer to the exhibit.



New User

Username

E-Mail

Password

Confirm Password

Default Start and End Date: Default ▾

Status

● Enabled

○ Disabled

Role

superuser ▾

- Superuser
- Senior Analyst
- Analyst
- Read-only Analyst
- Obfuscated Analyst

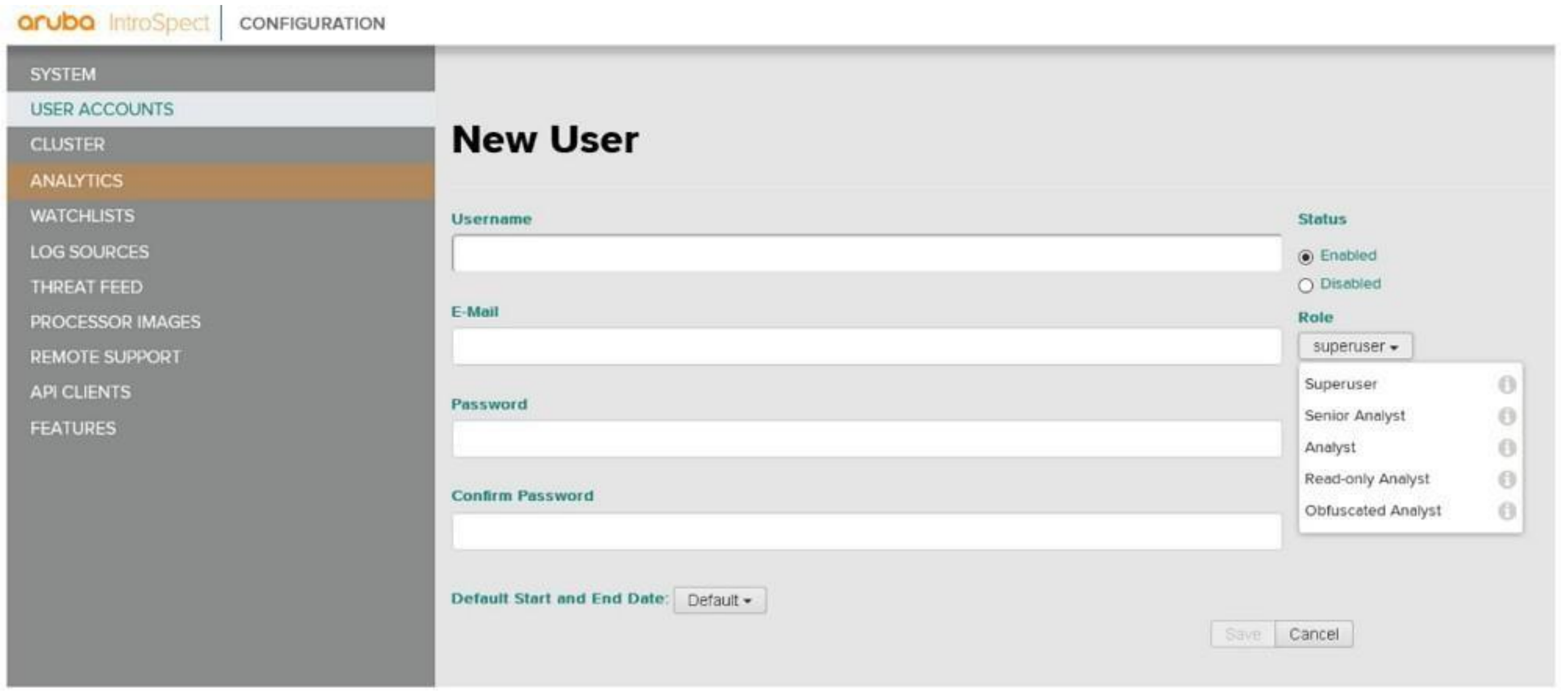
Would this be a correct option when configuring a user account for a ClearPass to use to communicate with IntroSpect? (The username and email address must match.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=27259

QUESTION 42
Refer to the exhibit.



New User

Username

E-Mail

Password

Confirm Password

Default Start and End Date: Default ▾

Status

● Enabled

○ Disabled

Role

superuser ▾

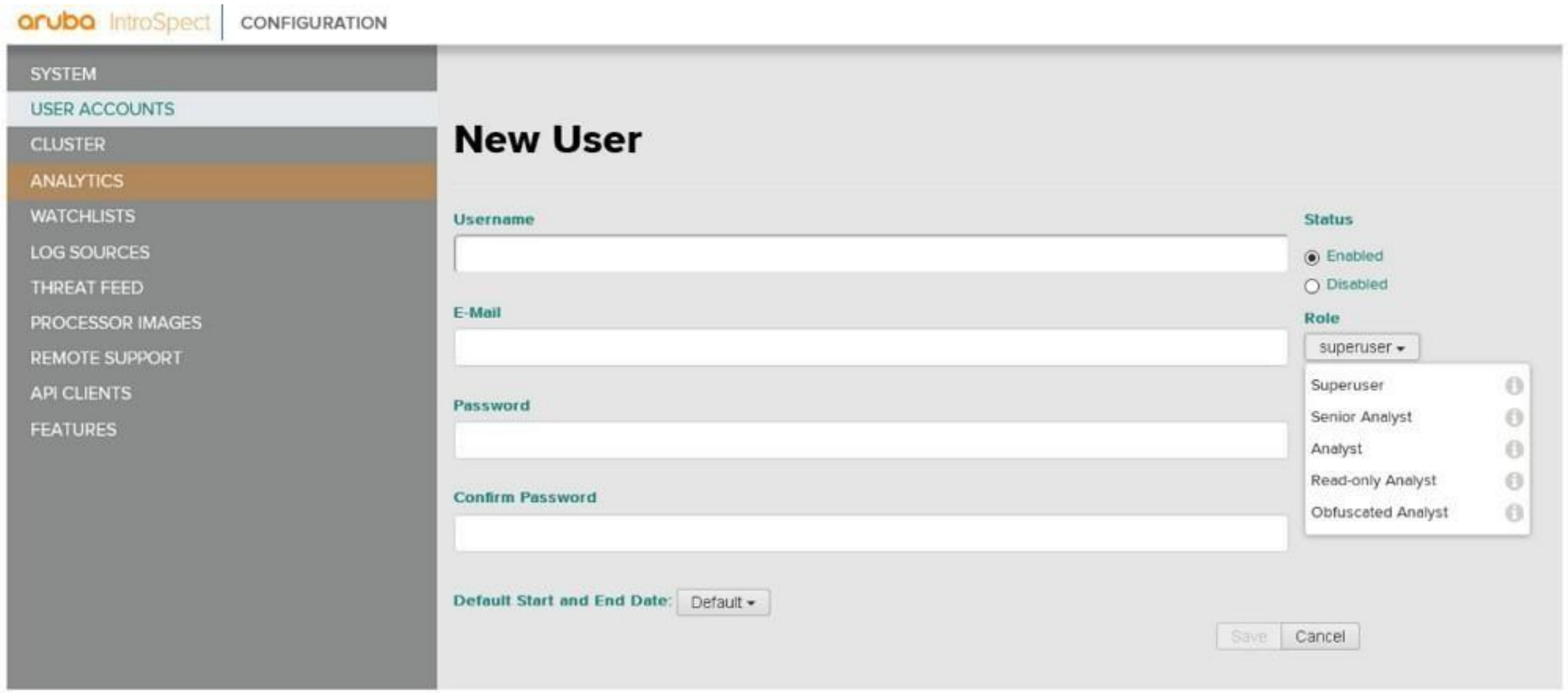
Would this be a correct option when configuring a user account for a ClearPass to use to communicate with IntroSpect? (The email address needs to match the username used in ClearPass.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Refer to the exhibit.



New User

Username

E-Mail

Password

Confirm Password

Default Start and End Date: Default ▾

Status

● Enabled

○ Disabled

Role

superuser ▾

Would this be a correct option when configuring a user account for a ClearPass to use to communicate with IntroSpect? (The username must be the host name of the ClearPass server, and the email address needs to be the username on the ClearPass server.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
During a discovery at a large company, the customer asks if they can run IntroSpect on a segment of the network and only monitor a small group of users and servers as a trial. As their IT staff becomes familiar with the analytics, they want to expand the installation to the entire enterprise. Would this be a valid option for the customer? (It is easy to support growth with the Scale-out Analyzer appliance, as Analyzer Nodes may be added over time to support the larger demand from the full environment.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
During a discovery at a large company, the customer asks if they can run IntroSpect on a segment of the network and only monitor a small group of users and servers as a trial. As their IT staff becomes familiar with the analytics, they want to expand the installation to the entire enterprise. Would this be a valid option for the customer? (The customer can deploy the analyzer at the first site and use whitelist/blacklist functions to contain the scope of the analytics to the smaller site.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
You have been asked to provide a Bill of Materials (BoM) for a mature small business with two sites. The IT Director prefers all hardware to be on-premise but is open to cloud-based solution. In conversations with the IT staff, you determine that the main site has approximately 550 network devices and 400 users. All users are in Active Directory. Eighty of the users use a Pulse Secure VPN to work remotely.

The second site is a warehouse operation with approximately 40 users and another 10 users that use Pulse Secure VPN. All wireless is using Aruba Networks Instant APs. There are Active Directory servers at both sites. All logs are currently being gathered into Splunk. The team feels that they can properly monitor the corporate site network with a single tap port on a central switch at the main office. There will be a network tap at the remote site.

Is this a suggestion you would make to the customer? (The customer should purchase the Scale-Out option for their data center, with a Packet Processor at the remote site.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 47

You have been asked to provide a Bill of Materials (BoM) for a mature small business with two sites. The IT Director prefers all hardware to be on-premise but is open to cloud-based solution. In conversations with the IT staff, you determine that the main site has approximately 550 network devices and 400 users. All users are in Active Directory. Eighty of the users use a Pulse Secure VPN to work remotely.

The second site is a warehouse operation with approximately 40 users and another 10 users that use Pulse Secure VPN. All wireless is using Aruba Networks Instant APs. There are Active Directory servers at both sites. All logs are currently being gathered into Splunk. The team feels that they can properly monitor the corporate site network with a single tap port on a central switch at the main office. There will be a network tap at the remote site.
Is this a suggestion you would make to the customer? (The customer should install the Fixed Configuration Analyzer in the data center to manage the tap and Splunk logs for the main site and a single Packet Processor at the warehouse site.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48

You have been asked to provide a Bill of Materials (BoM) for a mature small business with two sites. The IT Director prefers all hardware to be on-premise but is open to cloud-based solution. In conversations with the IT staff, you determine that the main site has approximately 550 network devices and 400 users. All users are in Active Directory. Eighty of the users use a Pulse Secure VPN to work remotely.

The second site is a warehouse operation with approximately 40 users and another 10 users that use Pulse Secure VPN. All wireless is using Aruba Networks Instant APs. There are Active Directory servers at both sites. All logs are currently being gathered into Splunk. The team feels that they can properly monitor the corporate site network with a single tap port on a central switch at the main office. There will be a network tap at the remote site.
Is this a suggestion you would make to the customer? (The customer should install the Fixed Configuration Analyzer at the main site, along with a Packet Processor in the data center and a single Packet Processor at the warehouse site.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49

During a conversation with one of your colleagues, they bring up the subject of small business security and ask you to explain why a small business would be interested in a product like IntroSpect. Is this a reason they would purchase IntroSpect? (Most small business that suffer a data breach will go out of business as a result of the breach.

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50

You are deploying a new IntroSpect Packet Processor in your data center. It is not communicating with the analyzer in the same data center. You think that you have entered the host name of the analyzer incorrectly while bootstrapping the packet processor. Would this be a logical next step? (Just restart the system by executing “shutdown –r now” command during the reboot; when prompted, select the option for “reset processor”.)

A. Yes
B. No

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
You are deploying a new IntroSpect Packet Processor in your data center. It is not communicating with the analyzer in the same data center. You think that you have entered the host name of the analyzer incorrectly while bootstrapping the packet processor. Would this be a logical next step? (Clear out the bootstrap data and restart the system. After the restart, rerun the bootstrap.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
You are deploying a new IntroSpect Packet Processor in your data center. It is not communicating with the analyzer in the same data center. You think that you have entered the host name of the analyzer incorrectly while bootstrapping the packet processor. Would this be a logical next step? (Enter a new host name with the command #>/opt/niara/analyzer/lib/hadoop/rename-an-node {analyzer FQDN} in the CLI.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=27256

QUESTION 53
While a customer site you are asked to explain the advantages and limits of collecting AMON from the Aruba Mobility Controllers. Would this be a correct statement? (AMON is an easy way to monitor a network where the primary access method is through Aruba Mobility Controllers.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
A customer is asking you to explain the difference between a data breach and a data leak. Does this explain the difference? (In both cases, data has left your network for the outside. A data breach is executed by an outside attacker, while a data leak is executed either deliberately or accidentally by an inside actor.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 55
You were called into a customer site to do an evaluation of installing IntroSpect for a small business. During the discovery process, the customer asks you to explain when they would need to deploy a Packet Processor. Does this explain the function of the Packet Processor? (They always need the Packet Processor to process AMON data from the Aruba Networks Mobility Controller.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
You were called into a customer site to do an evaluation of installing IntroSpect for a small business. During the discovery process, the customer asks you to explain when they would need to deploy a Packet Processor. Does this explain the function of the Packet Processor? (The packet Processor helps if they are using the analyzer deployed in the cloud by forwarding log data over HTTPS.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
You are administering an IntroSpect Installation. While monitoring the load on the IntroSpect Packet Processors, you think that one Packet Processor is overloaded. Is this a correct statement about the possible overload? (As a general rule, the data rate should be below 9000 event/sec.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
You are administering an IntroSpect Installation. While monitoring the load on the IntroSpect Packet Processors, you think that one Packet Processor is overloaded. Is this a correct statement about the possible overload? (As a general rule, the data rate should be below 5000 event/sec.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
You are a system admin with a company where Aruba infrastructure, such as Controllers, ClearPass, and Airwave, have been deployed. The company has integrated an Aruba Introspect 2-RU appliance in the Network Infrastructure. Recently, you are seeing overload issues with the IntroSpect system. So, you want to add five more Compute Nodes to meet the requirements.
Is this a correct solution for adding more Compute Nodes? (2-RU is a single appliance that does not scale, and you cannot add any more Compute Nodes to it.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
You are a system admin with a company where Aruba infrastructure, such as Controllers, ClearPass, and Airwave, have been deployed. The company has integrated an Aruba Introspect 2-RU appliance in the Network Infrastructure. Recently, you are seeing overload issues with the IntroSpect system. So, you want to add five more Compute Nodes to meet the requirements.
Is this a correct solution for adding more Compute Nodes? (With a 2-RU system, you can add a maximum 4 Compute Nodes.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A network administrator is looking for an option to set the maximum data retention period to 180 days in the IntroSpect Analyzer. Is this a correct statement about data retention in IntroSpect? (The data retention period cannot exceed 90 days.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A network administrator is looking for an option to set the maximum data retention period to 180 days in the IntroSpect Analyzer. Is this a correct statement about data retention in IntroSpect? (The default data retention period is set at 30 days, and this cannot be changed.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
You are an administrator who made a few configuration changes in the IntroSpect Packet Processor, and a restart is required after those changes. Is this a valid method to restart the Packet Processor? (SSH into the Packet Processor, and log in as “admin” and issue the command #> shutdown –s now.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
You are an administrator who made a few configuration changes in the IntroSpect Packet Processor, and a restart is required after those changes. Is this a valid method to restart the Packet Processor? (Issue the command #>shutdown –r now from the CLI of the Packet Processor.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
You are an administrator who made a few configuration changes in the IntroSpect Packet Processor, and a restart is required after those changes. Is this a valid method to restart the Packet Processor? (SSH into the Packet Processor, and log in as “admin” and issue the command #>shutdown –r now.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
An administrator scheduled a maintenance window for upgrading an IntroSpect system. Is this a true statement about upgrading the IntroSpect system? (All Packer Processors should be upgraded first, then the IntroSpect Analyzer should be upgraded.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
You are working on an IntroSpect Analyzer to fix an issue, and a restart is required after fixing the issue. Is this the correct procedure to restart? (From the Analyzer Menu navigate to Configuration ->System->Cluster Start/Stop->Restart Cluster.)

A. Yes

B. No

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
You are working on an IntroSpect Analyzer to fix an issue, and a restart is required after fixing the issue. Is this the correct procedure to restart? (From the Analyzer Menu navigate to Configuration ->Cluster->Cluster Start/Stop->Restart Cluster.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
You are working on an IntroSpect Analyzer to fix an issue, and a restart is required after fixing the issue. Is this the correct procedure to restart? (From the Analyzer Menu navigate to Maintenance ->System->Cluster Start/Stop->Restart Cluster.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70 An analyst notices that a disabled user account has been enabled. Is this an action that the analyst should take? (Put the user account on a watchlist to keep an eye on it.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71 An analyst notices that a disabled user account has been enabled. Is this an action that the analyst should take? (Allow the system to run for 15 days to establish a historical baseline, and determine if this account is a threat.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 72
While investigating alerts you notice an entity has triggered a peer alert for visiting recruiting websites. Two days later the same user accessed the office for the first time in the late evening. You also noticed that they downloaded more data than their peers through the VPN session. Based on these conditions, is this a possible cause? (This user has just become a flight risk, and is now sending data off the network to use in their next job.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
While investigating alerts you notice an entity has triggered a peer alert for visiting recruiting websites. Two days later the same user accessed the office for the first time in the late evening. You also noticed that they downloaded more data than their peers through the VPN session. Based on these conditions, is this a possible cause? (The user's account could have been compromised and is now being used by an attacker to exfiltrate company information.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
While looking in the IntroSpect Analyzer Conversations screen you see there are a large number of DNS sessions coming from one IP address on the data center network VLAN. Would this be a logical next step? (The device at the IP address could be infected with malware seeking Command and Control. You should audit the device.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

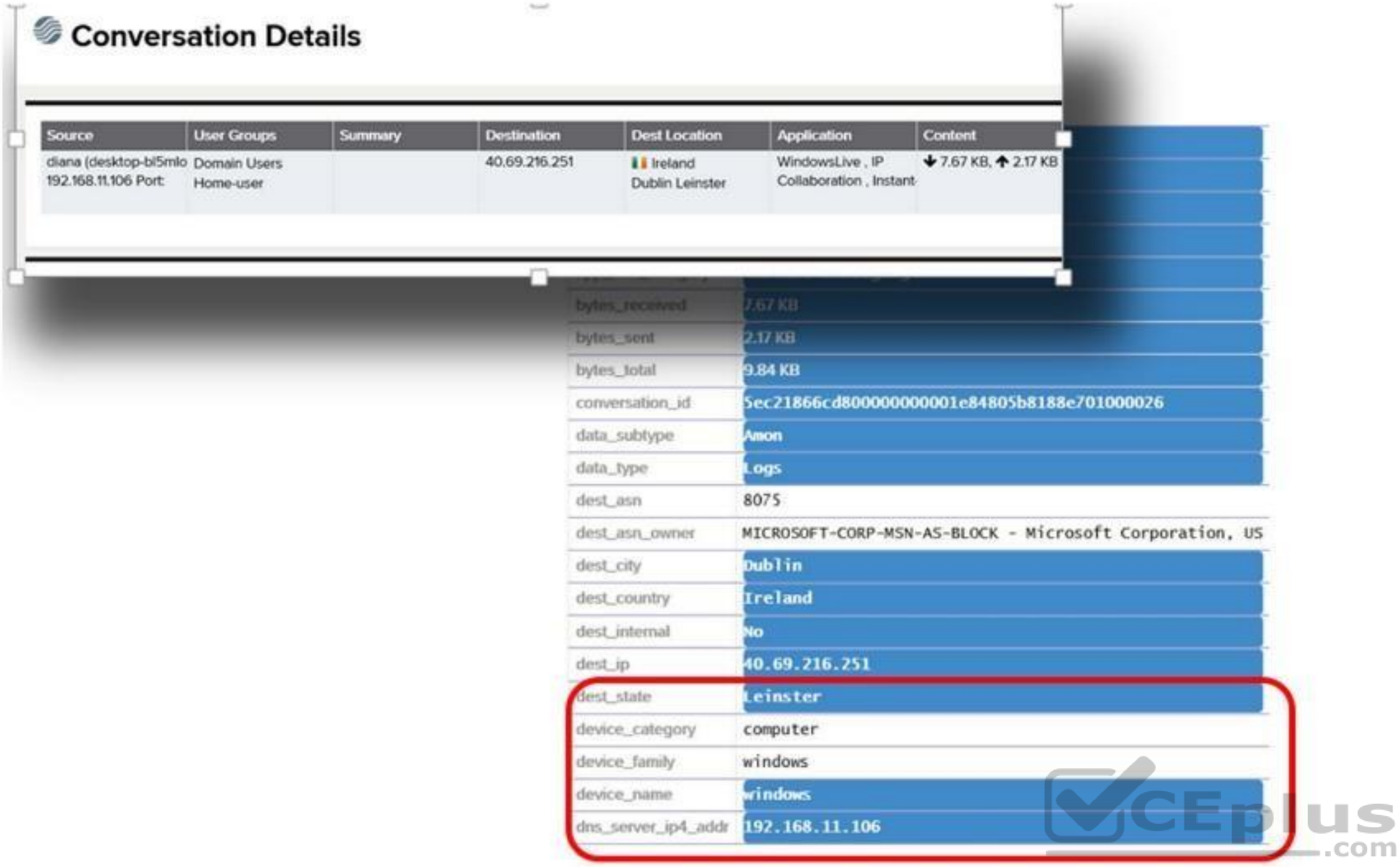
QUESTION 75
While looking in the IntroSpect Analyzer Conversations screen you see there are a large number of DNS sessions coming from one IP address on the data center network VLAN. Would this be a logical next step? (Add the IP address to the DNS Server under Configuration>System>in the analyzer so the Analyzer will ignore the DNS traffic from the IP address.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Refer to the exhibit.



Conversation Details

Source	User Groups	Summary	Destination	Dest Location	Application	Content
diana (desktop-bi5mlo 192.168.11.106 Port:	Domain Users Home-user		40.69.216.251	Ireland Dublin Leinster	WindowsLive , IP Collaboration , Instant	↓ 7.67 KB, ↑ 2.17 KB

bytes_received	7.67 KB
bytes_sent	2.17 KB
bytes_total	9.84 KB
conversation_id	5ec21866cd800000000001e84805b8188e701000026
data_subtype	Amon
data_type	Logs
dest_asn	8075
dest_asn_owner	MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US
dest_city	Dublin
dest_country	Ireland
dest_internal	No
dest_ip	40.69.216.251
dest_state	Leinster
device_category	computer
device_family	windows
device_name	windows
dns_server_ip4_addr	192.168.11.106

You are a security analyst for a company that has deployed an Aruba infrastructure, such as Mobility Controllers, ClearPass, and Airwave. Recently they have deployed Aruba IntroSpect for security analytics. You are looking at the conversation details of an entity. Is this statement correct about the details highlighted? (These details came from the ClearPass server and it has been integrated as a context server in the IntroSpect.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You are looking in the conversation page on the IntroSpect Analyzer. Is this a valid method for determining which source the conversation data come from? (Click on the different options under Applications to filter for application types like DNS and HTTP.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 78
While investigating alerts in the Analyzer you notice a host desktop with a low risk score has been sending regular emails from an internal account to the same external account. Upon investigation you see that the emails all have attachments. Would this be correct assessment of the situation? (The user on this host spends way too much time sending email, but should not be considered a risk until the risk score climbs above 60.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
While investigating alerts in the Analyzer you notice a host desktop with a low risk score has been sending regular emails from an internal account to the same external account. Upon investigation you see that the emails all have attachments. Would this be correct assessment of the situation? (This desktop should be added to a watch list and audited for a time to determine if this is real threat activity.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

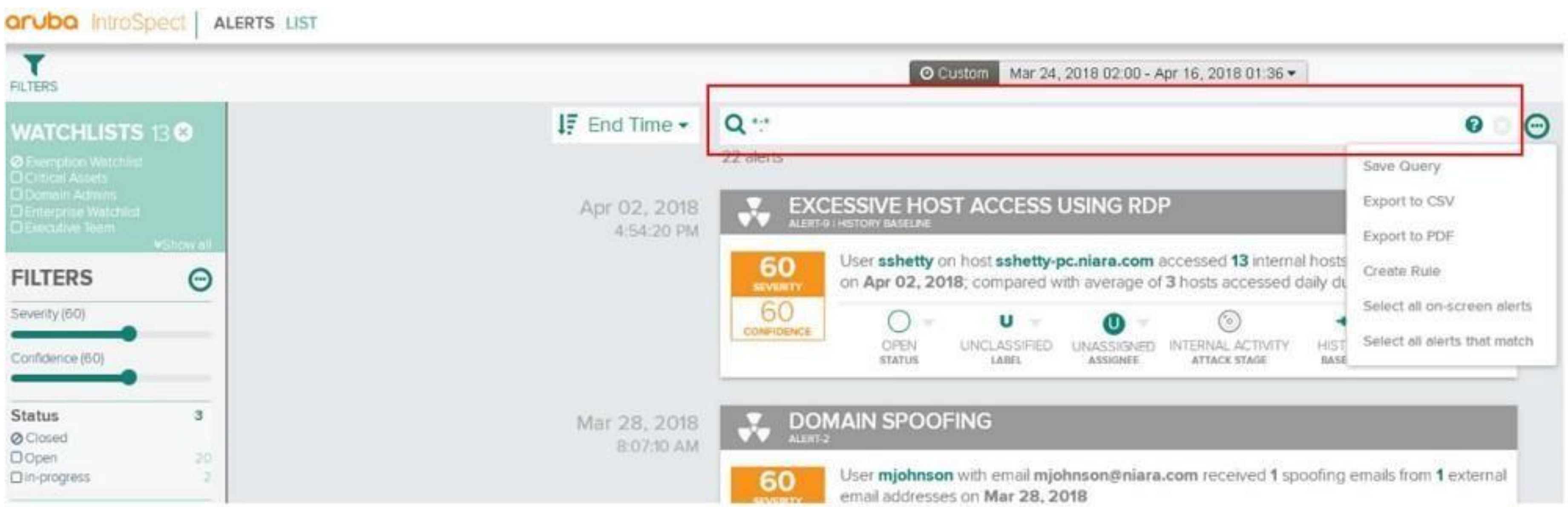
QUESTION 80
While investigating alerts in the Analyzer you notice a host desktop with a low risk score has been sending regular emails from an internal account to the same external account. Upon investigation you see that the emails all have attachments. Would this be correct assessment of the situation? (Your next step should be to find what user account logs into this desktop, and look at activity of their devices this user has access to.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Refer to the exhibit.



User sshetty on host sshetty-pc.niara.com accessed 13 internal hosts on Apr 02, 2018; compared with average of 3 hosts accessed daily du

User mjohnson with email mjohnson@niara.com received 1 spoofing emails from 1 external email addresses on Mar 28, 2018

You are logged into the IntroSpect and have navigated to the Alerts list. You are trying to filter the alerts to show all malware alerts for users. Is this a correct search query? (alertcategory:malware* AND username:any)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
An alert goes off for the internal DNS server, and while investigating the logs you notice that the hostnames in the queries are random alphanumeric characters. Is this a logical investigation step? (Contact the DNS admin and request that they enable root hints in the DNS server.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

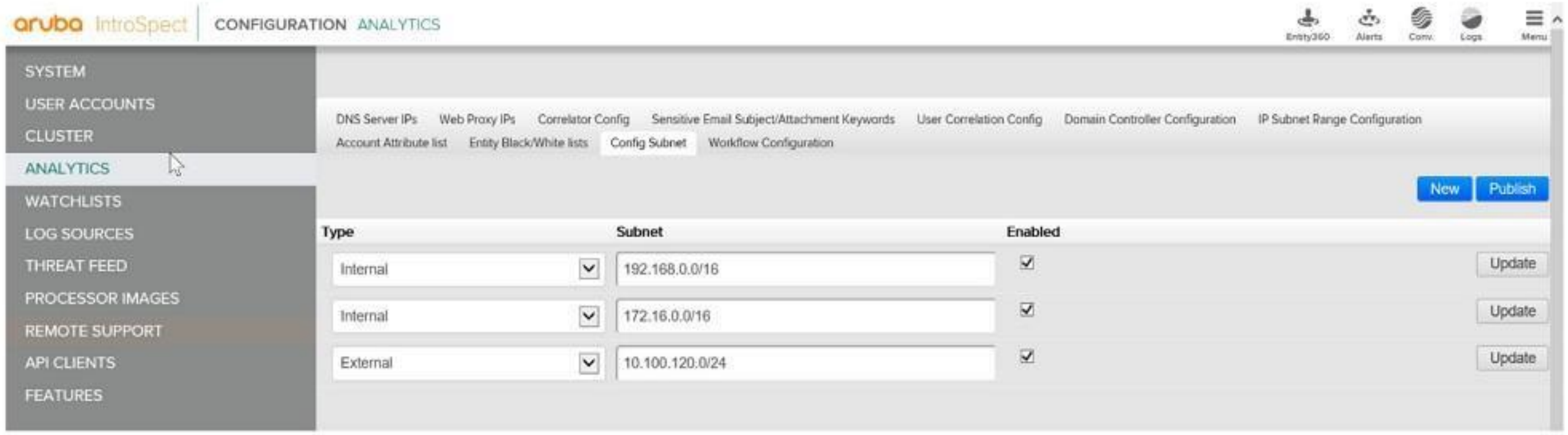
QUESTION 83
While looking at the conversations page you notice one user account logging into a number of servers on a regular basis. Is this information that you can draw from this activity? (This could be a service account and should be excluded from correlating Logon events with devices, or every device it logs into will be credited to it as the owner.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 84

Refer to the exhibit.



Type	Subnet	Enabled	
Internal	192.168.0.0/16	☑	Update
Internal	172.16.0.0/16	☑	Update
External	10.100.120.0/24	☑	Update

You are working with an IntroSpect Analyzer which is configured to monitor your network. You have navigated to the &ldquo;Config Subnets&rdquo; page to verify whether the internal and external subnets are configured properly. Is this a correct assessment of the screen? (The 10.100.120 subnet is incorrectly listed as external.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
A security analyst is monitoring the traffic which is accessing internal and external resources. They find abnormal activity, indicating communication between a compromised internal user(host) and internal infrastructure, and found a suspicious malware activity. Is this a correct attack stage classification for this activity? (Exfiltration.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A security analyst is monitoring the traffic which is accessing internal and external resources. They find abnormal activity, indicating communication between a compromised internal user(host) and internal infrastructure, and found a suspicious malware activity. Is this a correct attack stage classification for this activity? (Infection.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 87

You are visiting a site configured with IntroSpect, and the on-site admin tells you that they do not think that one of their database servers has fired any alerts for large download or strange access patterns. Could this be a reason? (The database server needs to be listed in an entity whitelist.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
You are visiting a site configured with IntroSpect, and the on-site admin tells you that they do not think that one of their database servers has fired any alerts for large download or strange access patterns. Could this be a reason? (The database server needs to be listed under Configuration>Analytics>User Correlation Config.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Arube IntroSpect establishes different types of baselines to perform user or device behavior analysis. Is this a correct description of a baseline that IntroSpect establishes? (Individual history baseline: this typically takes 10 to 14 days to establish a “steady state” that can be used.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Arube IntroSpect establishes different types of baselines to perform user or device behavior analysis. Is this a correct description of a baseline that IntroSpect establishes? (Peer entity baselines: this typically takes 5 to 7 days to establish a “steady state” that can be used.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
While talking to an associate, they ask you to describe how different alerts in IntroSpect indicate compromise on the network. Would this be a correct statement? (When an entity accesses a database for the first time, this would always indicate a compromise.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
While talking to an associate, they ask you to describe how different alerts in IntroSpect indicate compromise on the network. Would this be a correct statement? (An entity that scans known TCP ports on a large number of IP addresses in a subnet could be a malware gathering information.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

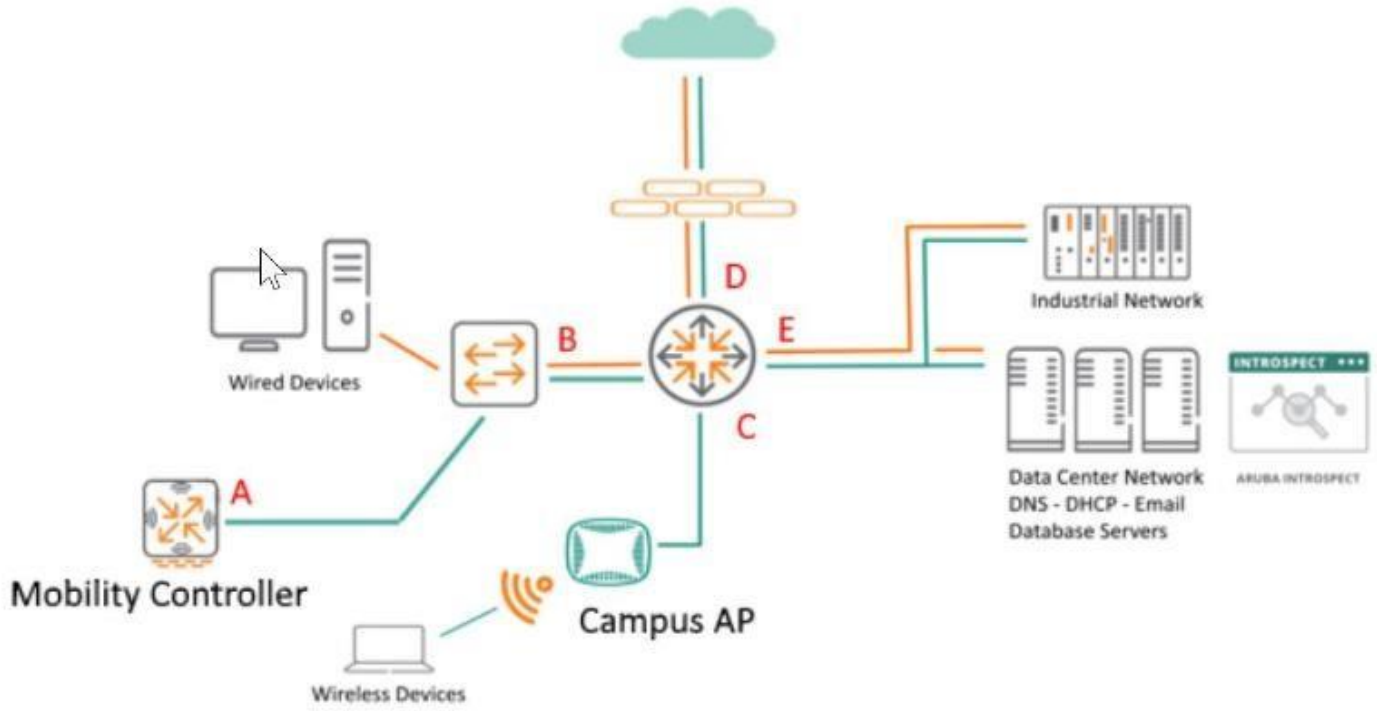
QUESTION 93
While talking to an associate, they ask you to describe how different alerts in IntroSpect indicate compromise on the network. Would this be a correct statement? (If an entity executes a large download followed a few days later by a large upload to DropBox, this could be an indication that the entity is compromised.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Refer to the exhibit.



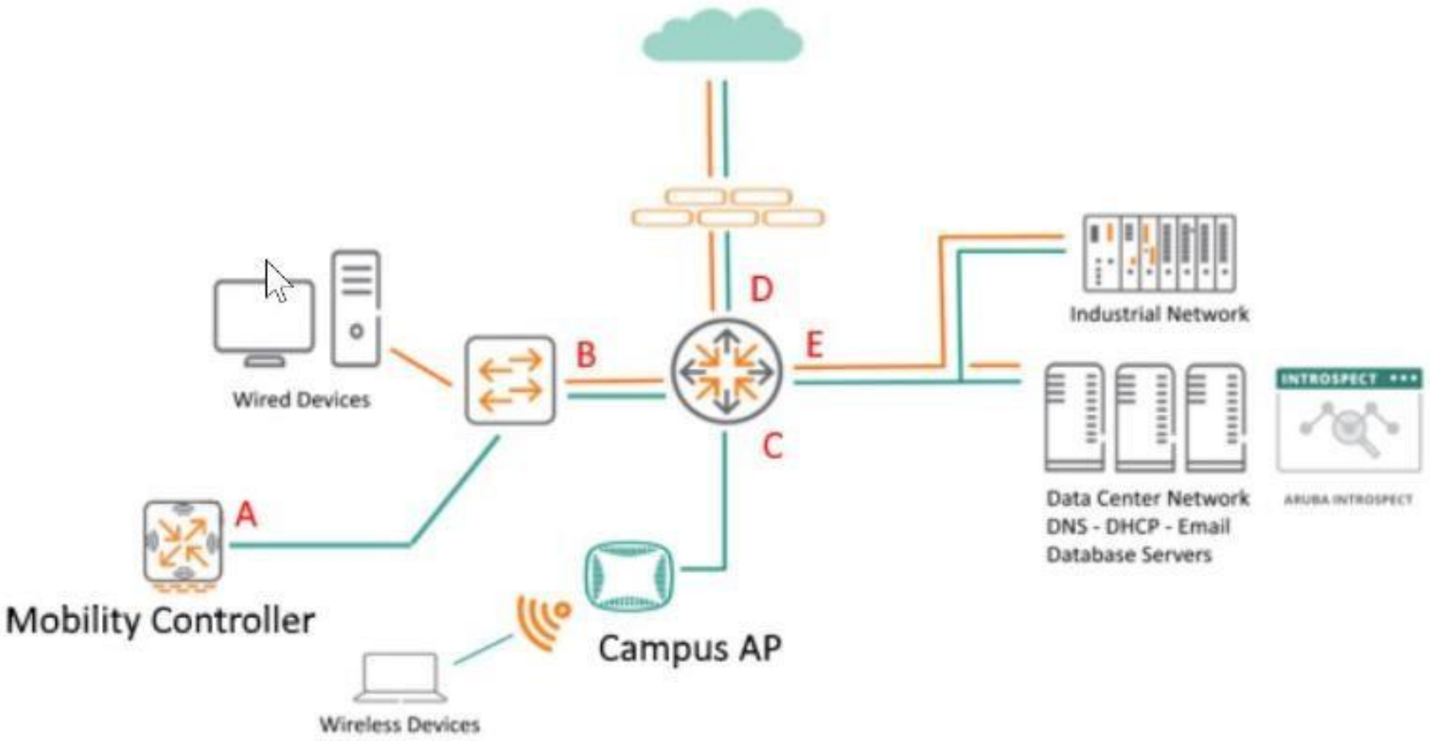
You are monitoring network traffic and considering DNS flow patterns. Where is a good location to place the Network Tap or Taps? (Location B will capture wired clients DNS requests while Location A will capture wireless client DNS.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Refer to the exhibit.



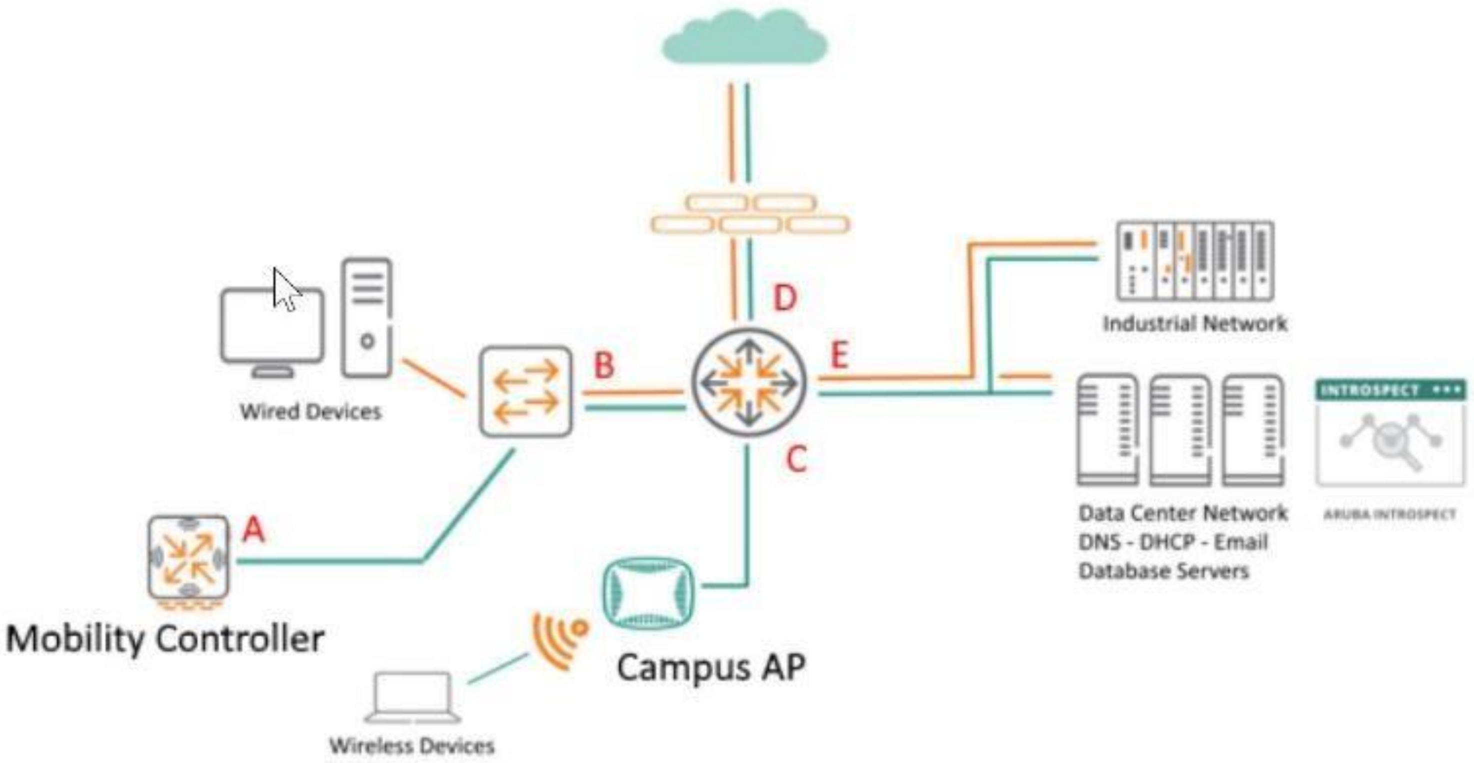
You are monitoring network traffic and considering DNS flow patterns. Where is a good location to place the Network Tap or Taps? (Location D will capture all DNS requests.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Refer to the exhibit.



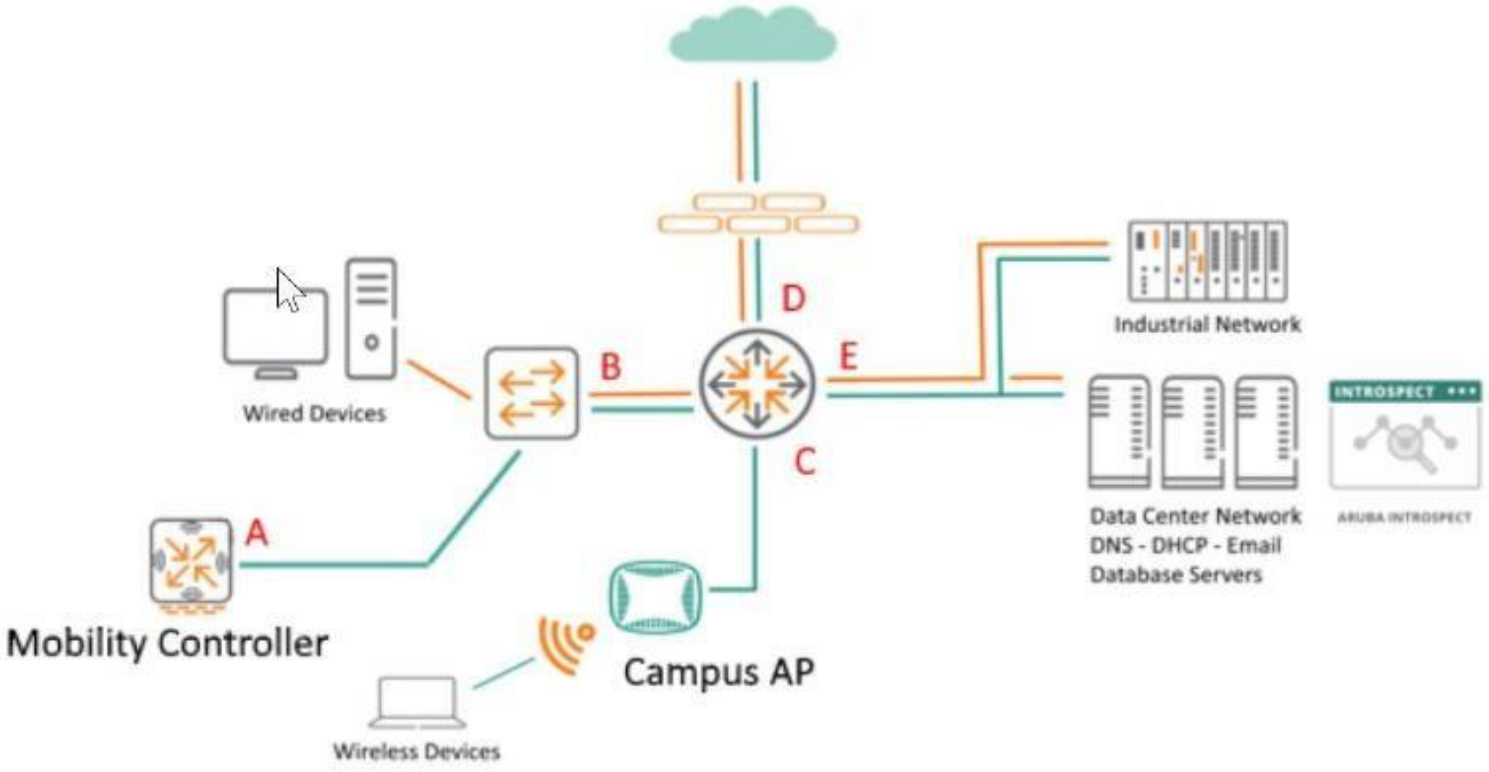
You are monitoring network traffic and considering DNS flow patterns. Where is a good location to place the Network Tap or Taps? (Location C.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Refer to the exhibit.



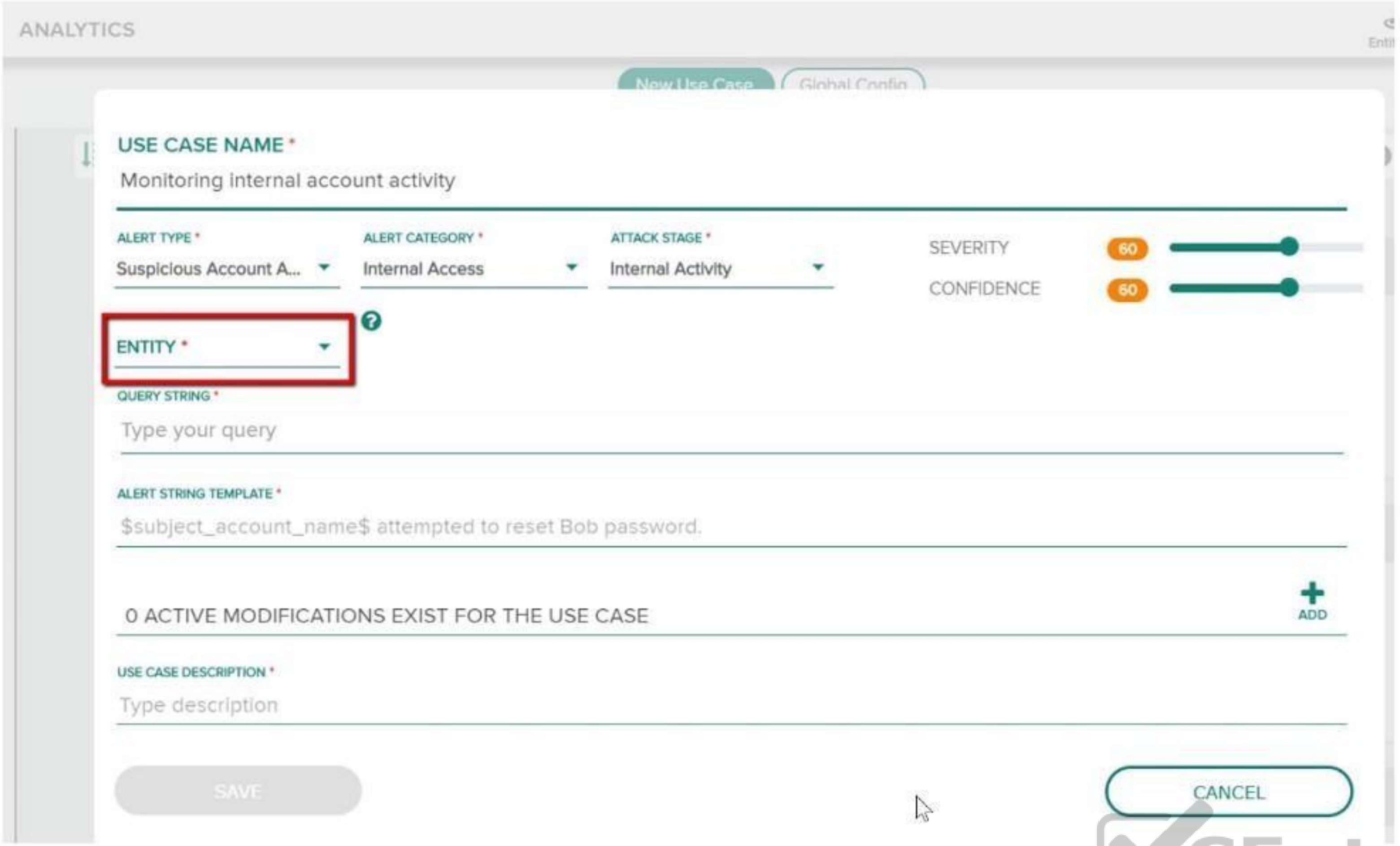
You are monitoring network traffic and considering DNS flow patterns. Where is a good location to place the Network Tap or Taps? (Location A.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Refer to the exhibit.



USE CASE NAME *
Monitoring internal account activity

ALERT TYPE *: Suspicious Account A...
ALERT CATEGORY *: Internal Access
ATTACK STAGE *: Internal Activity
SEVERITY 60
CONFIDENCE 60

ENTITY *

QUERY STRING *
Type your query

ALERT STRING TEMPLATE *
$subject_account_name$ attempted to reset Bob password.

0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE

USE CASE DESCRIPTION *
Type description

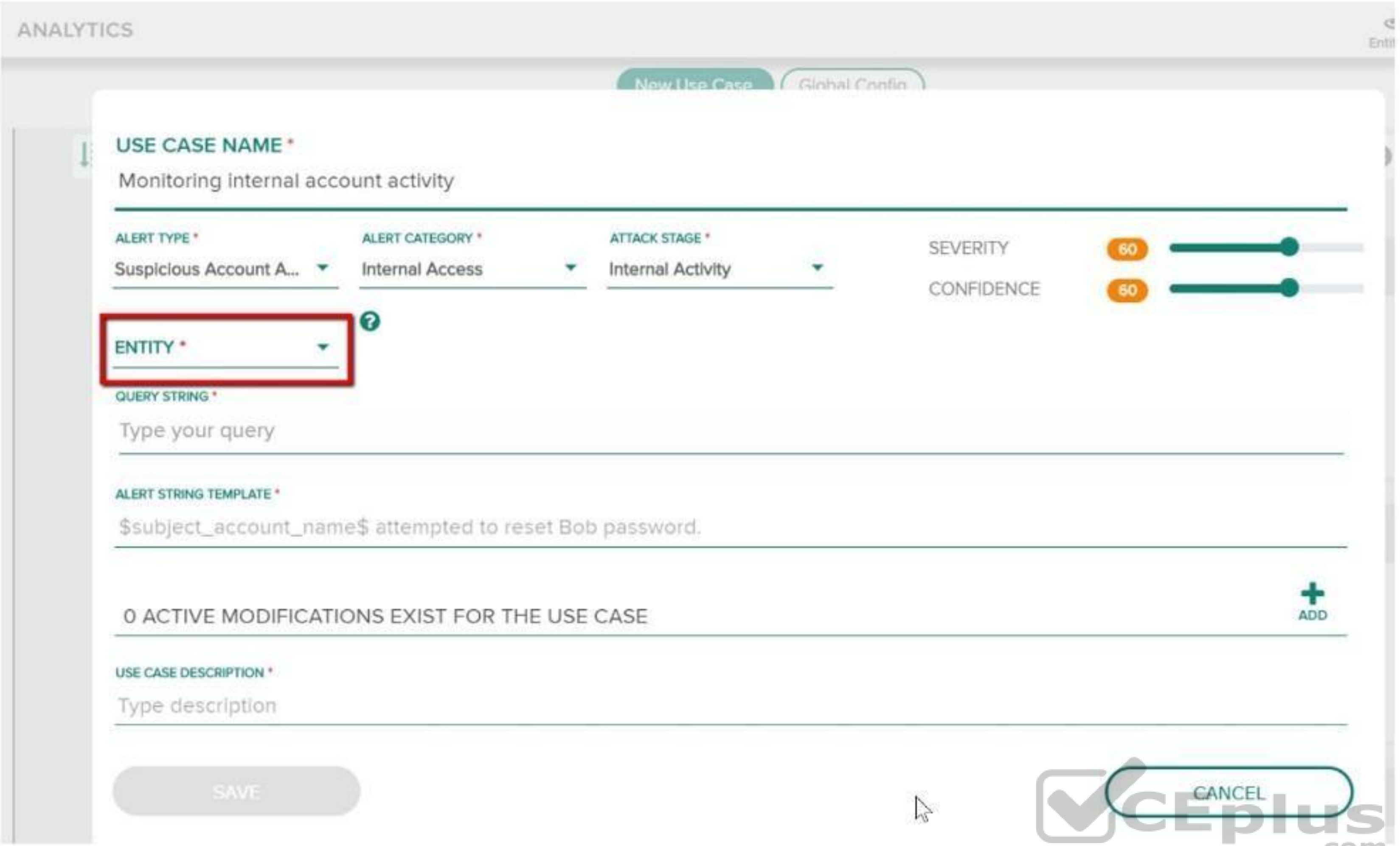
You have been assigned a task to monitor, analyze, and find those entities who are trying to access internal resources without having valid user credentials. You are creating an AD-based use case to look for this activity. Could you use this entity type to accomplish this? (Host name.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Refer to the exhibit.



USE CASE NAME *
Monitoring internal account activity

ALERT TYPE * Suspicious Account A...

ALERT CATEGORY * Internal Access

ATTACK STAGE * Internal Activity

SEVERITY 60

CONFIDENCE 60

ENTITY *

QUERY STRING *
Type your query

ALERT STRING TEMPLATE *
$subject_account_name$ attempted to reset Bob password.

0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE

USE CASE DESCRIPTION *
Type description

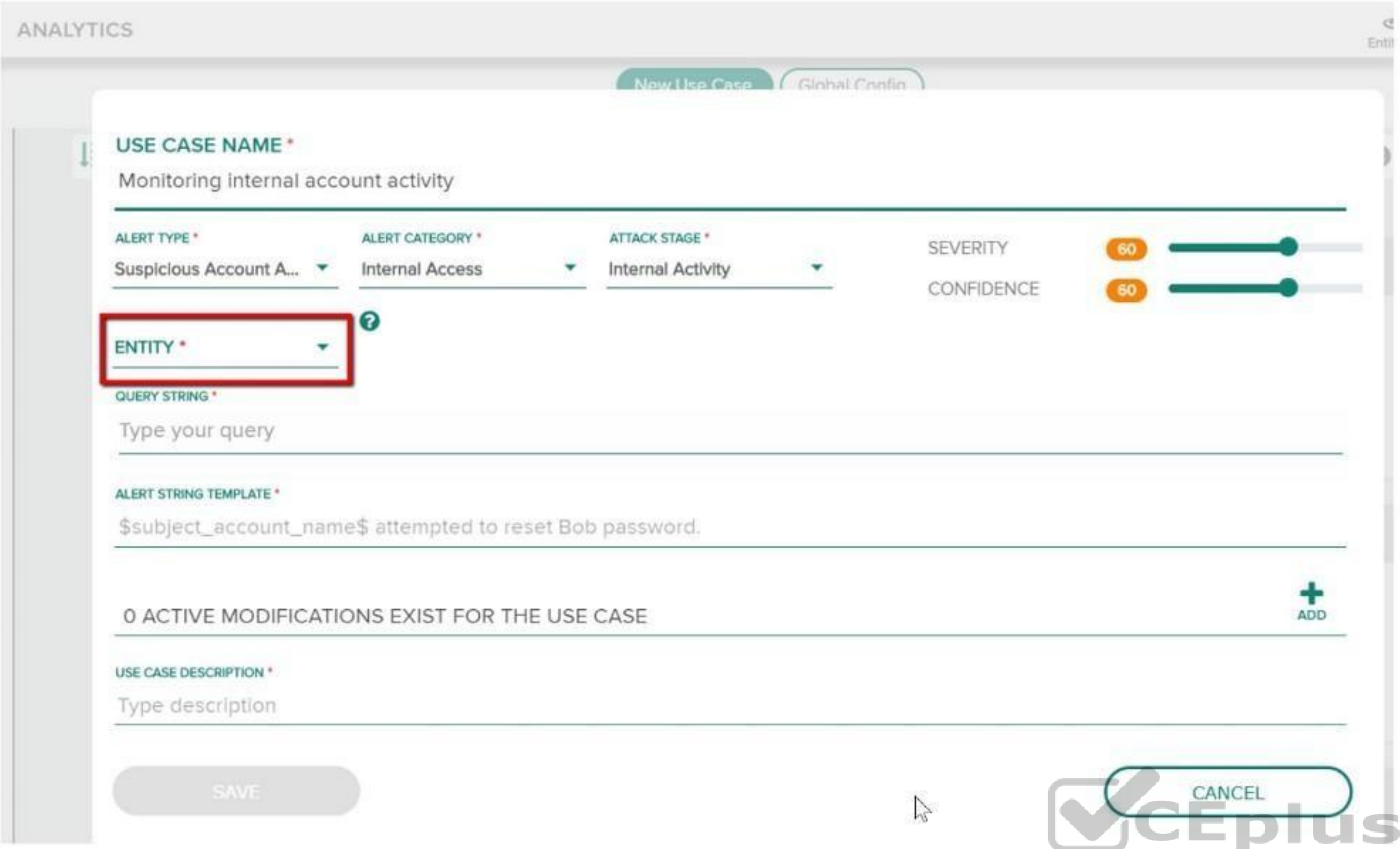
You have been assigned a task to monitor, analyze, and find those entities who are trying to access internal resources without having valid user credentials. You are creating an AD-based use case to look for this activity. Could you use this entity type to accomplish this? (Dest Host.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Refer to the exhibit.



USE CASE NAME *
Monitoring internal account activity

ALERT TYPE * Suspicious Account A...

ALERT CATEGORY * Internal Access

ATTACK STAGE * Internal Activity

SEVERITY 60

CONFIDENCE 60

ENTITY *

QUERY STRING *
Type your query

ALERT STRING TEMPLATE *
$subject_account_name$ attempted to reset Bob password.

0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE

USE CASE DESCRIPTION *
Type description

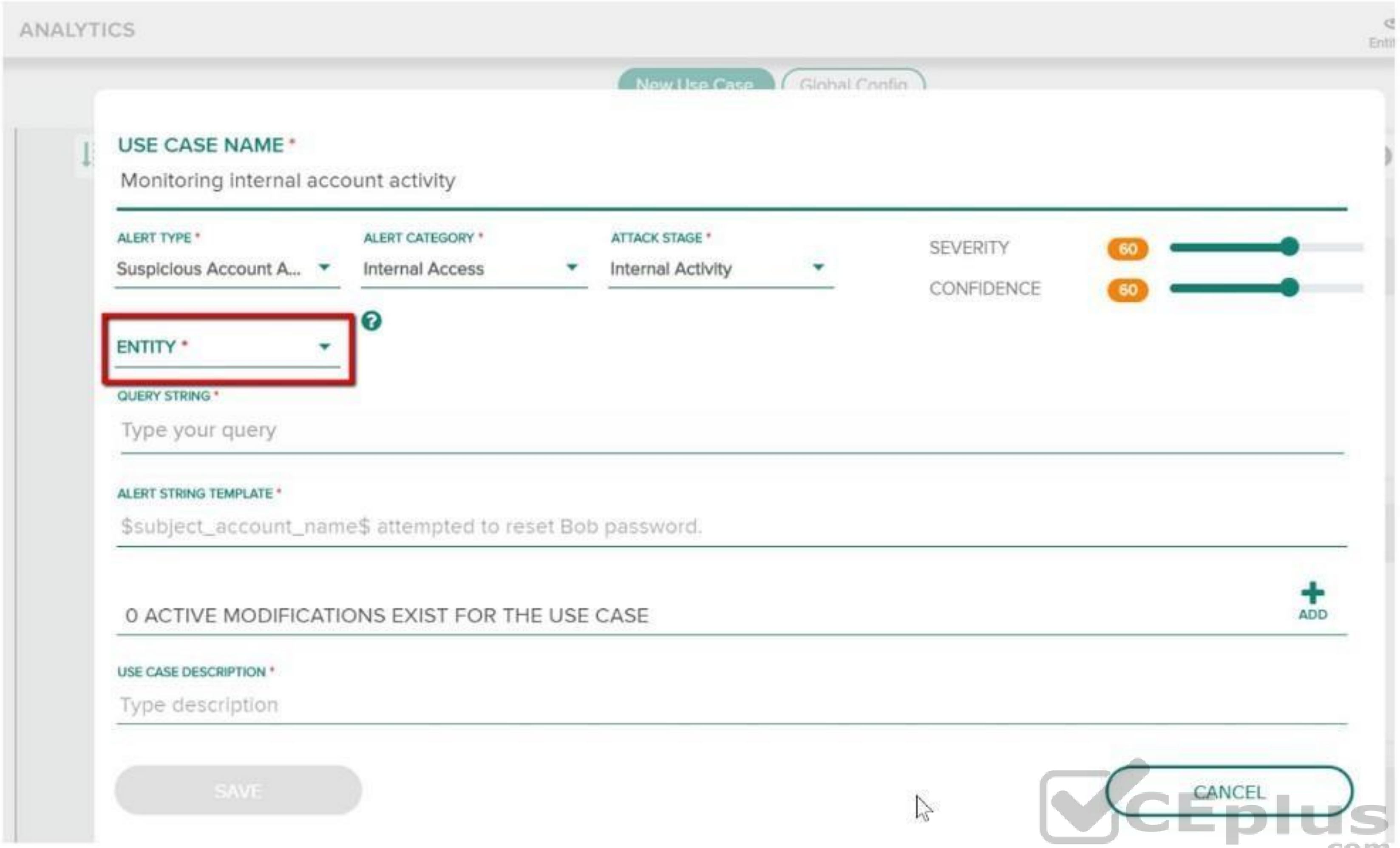
You have been assigned a task to monitor, analyze, and find those entities who are trying to access internal resources without having valid user credentials. You are creating an AD-based use case to look for this activity. Could you use this entity type to accomplish this? (Source Host.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Refer to the exhibit.



USE CASE NAME *
Monitoring internal account activity

ALERT TYPE * Suspicious Account A...

ALERT CATEGORY * Internal Access

ATTACK STAGE * Internal Activity

SEVERITY 60

CONFIDENCE 60

ENTITY *

QUERY STRING *
Type your query

ALERT STRING TEMPLATE *
$subject_account_name$ attempted to reset Bob password.

0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE

USE CASE DESCRIPTION *
Type description

You have been assigned a task to monitor, analyze, and find those entities who are trying to access internal resources without having valid user credentials. You are creating an AD-based use case to look for this activity. Could you use this entity type to accomplish this? (Dest IP.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Your company has found some suspicious conversations for some internal users. The security team suspects those users are communicating with entities in other countries. You have been assigned the task of identifying those users who are either uploading or downloading files from servers in other countries. Is this the best way to visualize conversations of suspected users in this scenario? (Visualizing conversation graphs.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 103

Your company has found some suspicious conversations for some internal users. The security team suspects those users are communicating with entities in other countries. You have been assigned the task of identifying those users who are either uploading or downloading files from servers in other countries. Is this the best way to visualize conversations of suspected users in this scenario? (Visualizing Applications and Ports.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
An admin is evaluating entity activity alerts for large internal downloads, excessive host access, accessing hosts with SSH, and host and port scans. Is this a correct reason for these types of alerts? (a malware seeking command and control.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
An admin is evaluating entity activity alerts for large internal downloads, excessive host access, accessing hosts with SSH, and host and port scans. Is this a correct reason for these types of alerts? (an attacker conducting reconnaissance on the network.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106 Would this be a proper correlation between entity and attack stage? (You see an alert for a user sending DNS requests for TOR sites, and correlate this to data exfiltration.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107 Would this be a proper correlation between entity and attack stage? (There is an alert for port scans by an entity, and you correlate that to a malware doing recon.)

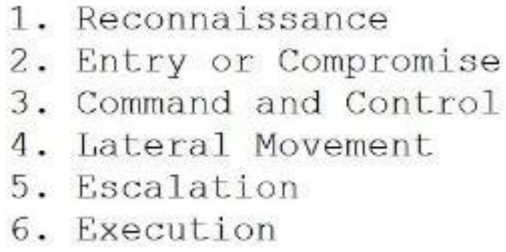
A. Yes

B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
In a conversation with a colleague you are asked to give them an idea of what type of monitor source you would use for each attack stage.



1. Reconnaissance
2. Entry or Compromise
3. Command and Control
4. Lateral Movement
5. Escalation
6. Execution

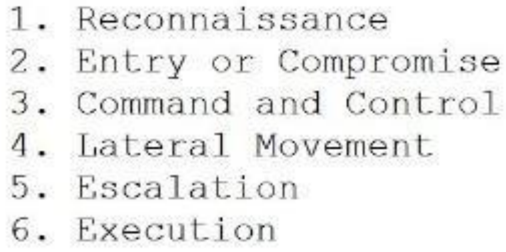
Would this be a correct correlation? (For “Command and Control” you can monitor DNS through AMON on the Aruba Mobility Controllers.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
In a conversation with a colleague you are asked to give them an idea of what type of monitor source you would use for each attack stage.



1. Reconnaissance
2. Entry or Compromise
3. Command and Control
4. Lateral Movement
5. Escalation
6. Execution

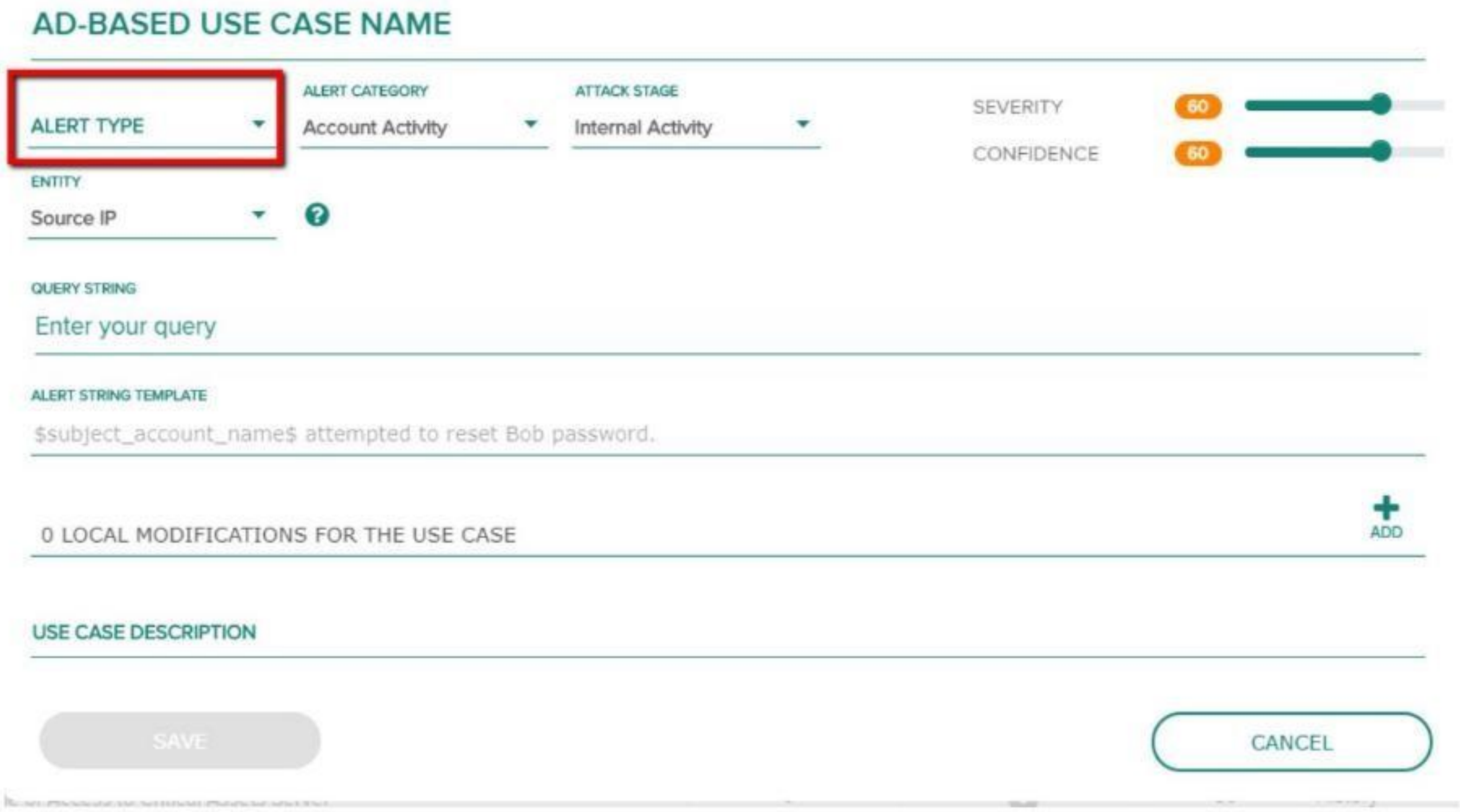
Would this be a correct correlation? (For “Command and Control” you can monitor DNS through network tap ports.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Refer to the exhibit.



AD-BASED USE CASE NAME

ALERT TYPE

ALERT CATEGORY: Account Activity

ATTACK STAGE: Internal Activity

SEVERITY: 60

CONFIDENCE: 60

ENTITY: Source IP

QUERY STRING: Enter your query

ALERT STRING TEMPLATE: $subject_account_name$ attempted to reset Bob password.

0 LOCAL MODIFICATIONS FOR THE USE CASE

USE CASE DESCRIPTION

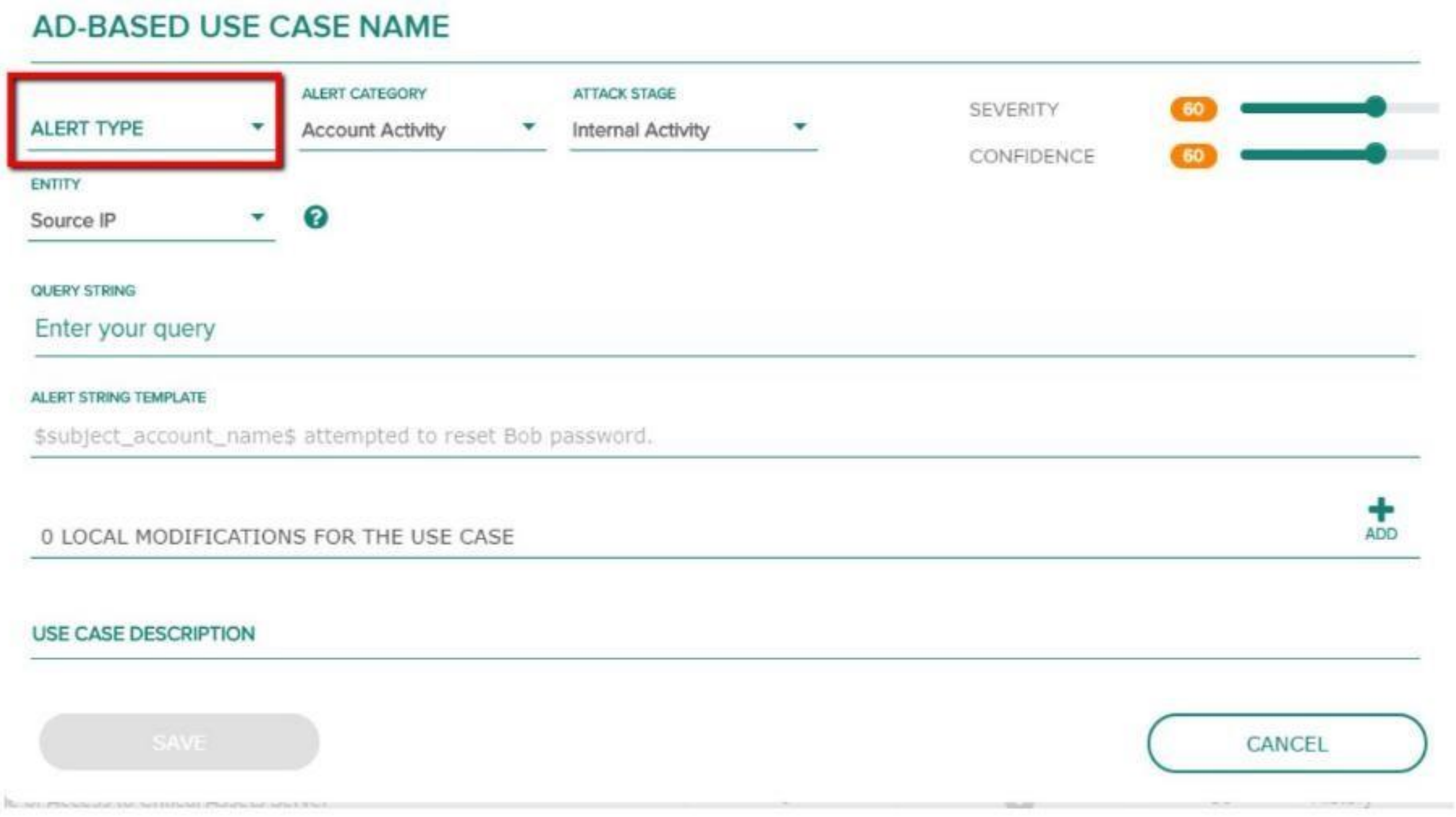
Which alert is not supported by AD-based use case? (Suspicious user login.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Refer to the exhibit.



ALERT TYPE

ALERT CATEGORY: Account Activity

ATTACK STAGE: Internal Activity

SEVERITY 60

CONFIDENCE 60

ENTITY: Source IP

QUERY STRING: Enter your query

ALERT STRING TEMPLATE: $subject_account_name$ attempted to reset Bob password.

0 LOCAL MODIFICATIONS FOR THE USE CASE

USE CASE DESCRIPTION

Which alert is not supported by AD-based use case? (Privilege escalation.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
You want to create a use case to get alerts when the behavior of an internal user has deviated from the norm of other users that work in the same department. Is this a suitable baseline for this use case? (Peer baseline based on the LDAP department from Active Directory.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
While investigating alerts you notice a user entity has triggered a historical alert for Large Internal Data Download. While investigating the alert, you notice that the download came from a different device than normal for the user. Based on these conditions, is this a possible cause? (This is a classic user account take over pattern.)

A. Yes

B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
The company has a DMZ with an application server where customers can upload and access their product orders. The security admin wants to know how you configure IntroSpect to monitor this server. Should this be part of your plan? (List the IP subnet of the DMZ as “External” under the Main Menu > Analytics>Global Config>so that alerts for the server will show up as IN-to-OUT traffic.)

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
The company has a DMZ with an application server where customers can upload and access their product orders. The security admin wants to know how you configure IntroSpect to monitor this server. Should this be part of your plan? (Configure the server in the DMZ as a High Value Asset in Menu>Configuration>Analytics>Correlator Config>so that IntroSpect will monitor the server for access patterns.)

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: