HPE2-W05 Q&As

Implementing Aruba IntroSpect

Pass HP HPE2-W05 Exam with 100% Guarantee

QUESTION 1

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

QUESTION 2

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

QUESTION 3

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

QUESTION 4

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

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

QUESTION 5

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

QUESTION 6

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

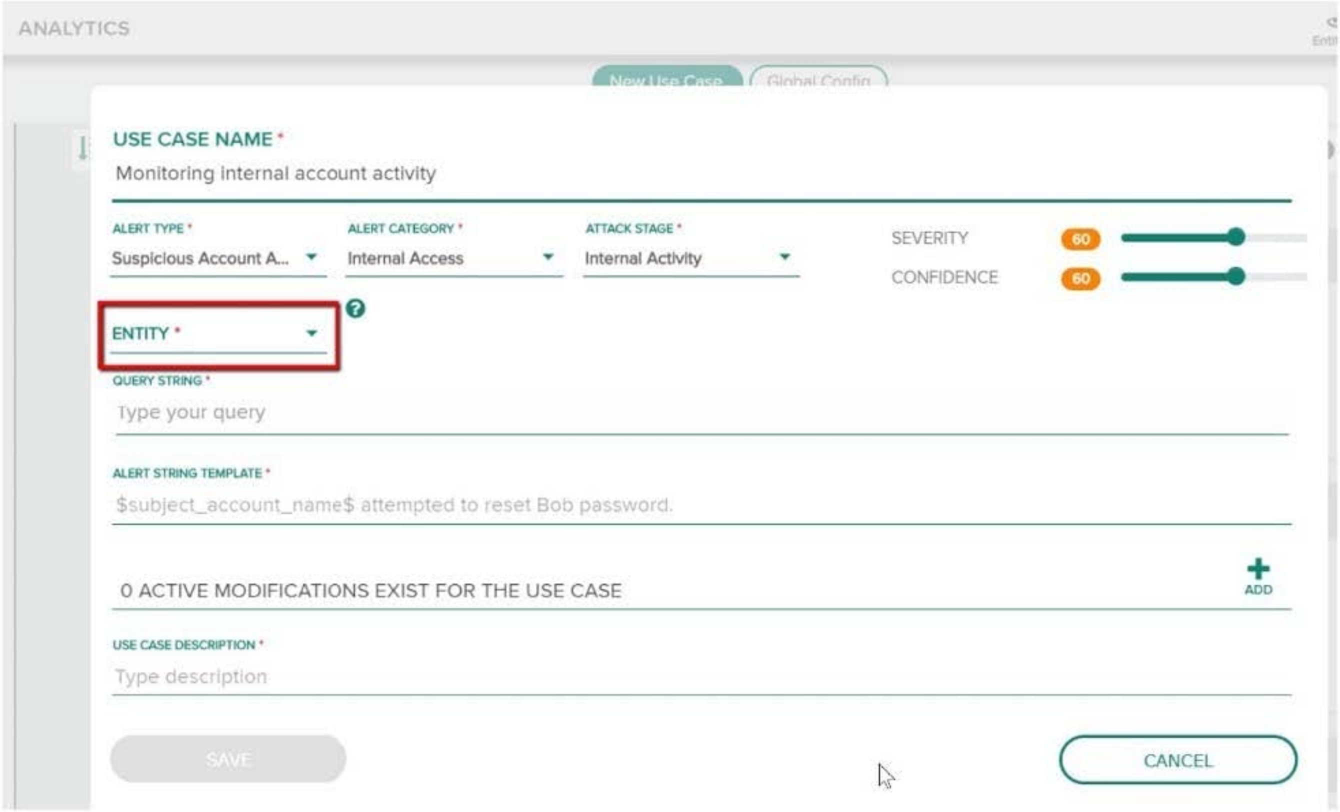
B. No

Correct Answer: A

Reference: https://www.google.com/url?sa=tandrct=jandq=andesrc=sandsource=webandcd=2andved=2ahUKEwiBra-C_HgAhWLsKQKHQ4yDkkQFjABegQICBACandurl=http%3A%2F%2Fsupport.arubanetworks.com% 2FDocumentation%2Ftabid%2F77% 2FDMXModule%2F512%2FCommand%2FCore_Download% 2FMethod%2Fattachment%2FDefault.aspx%3FEntryId% 3D33268andusg=AOvVaw3plzLBTQalED4qNGbdU1Dx

QUESTION 7

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

QUESTION 8

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.)

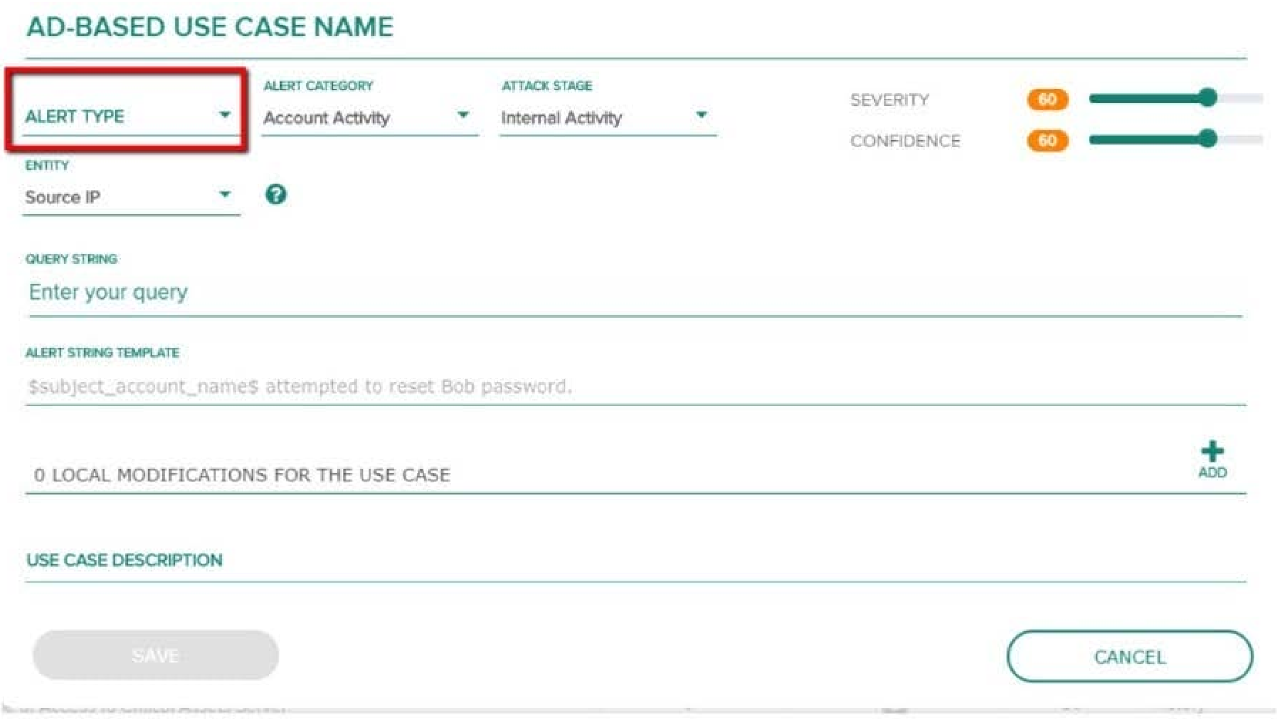
A. Yes

B. No

Correct Answer: B

QUESTION 9

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? (Privilege escalation.)

A. Yes

B. No

Correct Answer: A

QUESTION 10

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

QUESTION 11

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

QUESTION 12

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.)

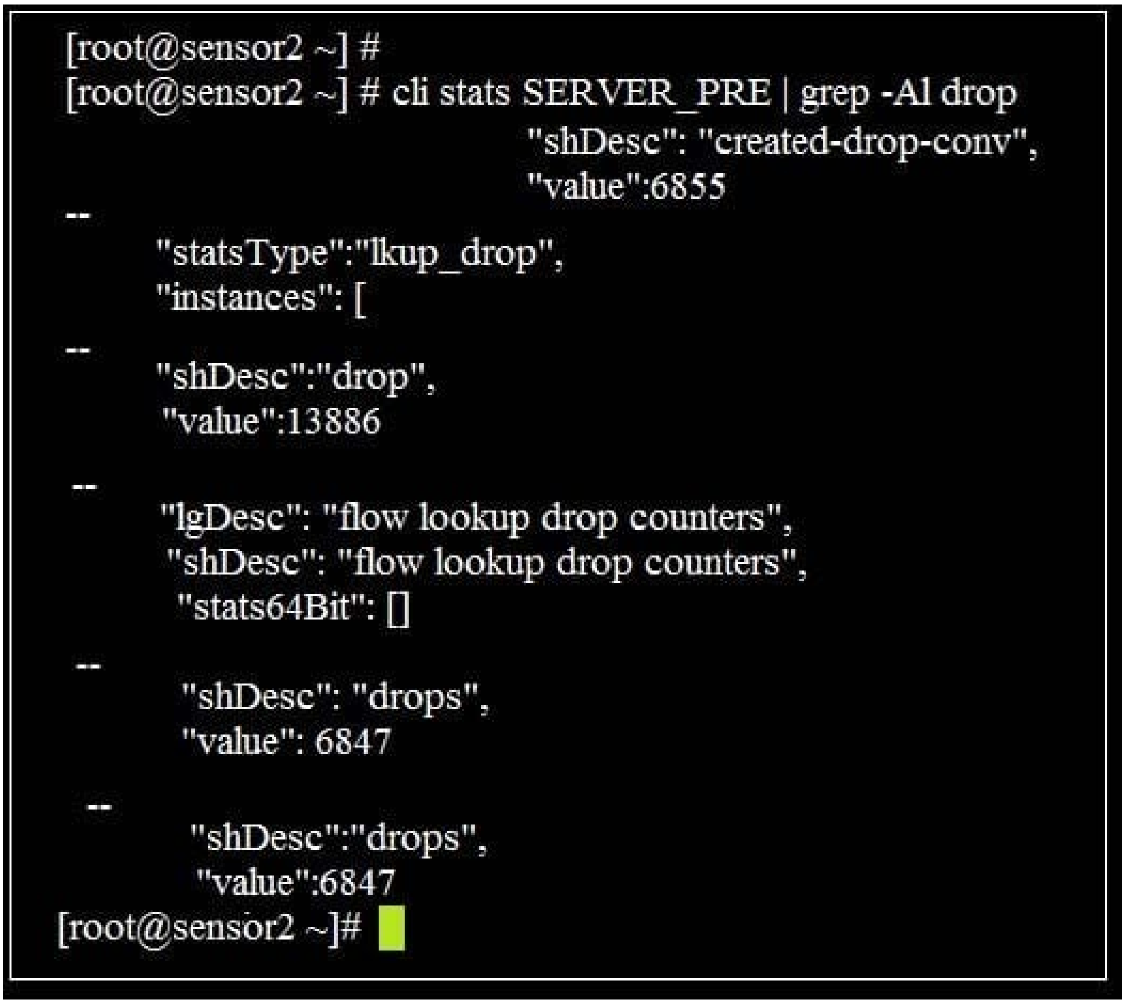
A. Yes

B. No

Correct Answer: A

QUESTION 13

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

QUESTION 14

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.)

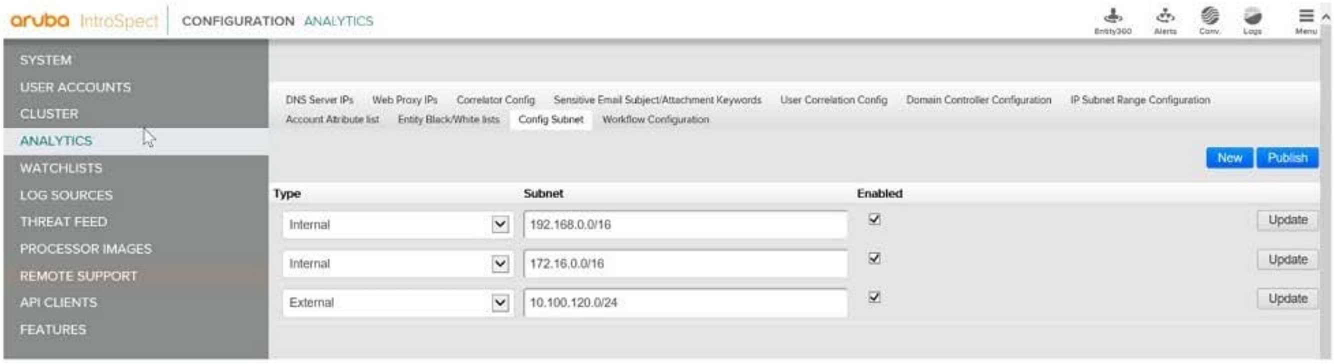
A. Yes

B. No

Correct Answer: B

QUESTION 15

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 andldquo;Config Subnetsandrdquo; 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

Latest HPE2-W05 Dumps HPE2-W05 Practice Test HPE2-W05 Exam Questions