HPE2-W05 Q&As

Implementing Aruba IntroSpect

Pass HP HPE2-W05 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/hpe2-w05.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

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 ? now" command during the reboot; when prompted, select the option for "reset processor".)

A. Yes

B. No

Correct Answer: B

QUESTION 2

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.)

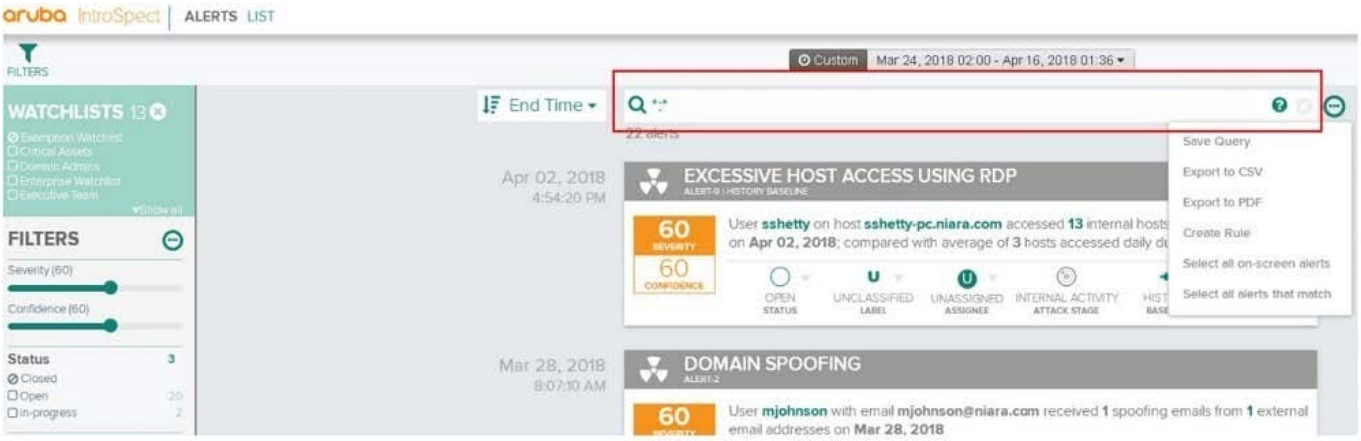
A. Yes

B. No

Correct Answer: B

QUESTION 3

Refer to the exhibit.



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

QUESTION 4

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.)

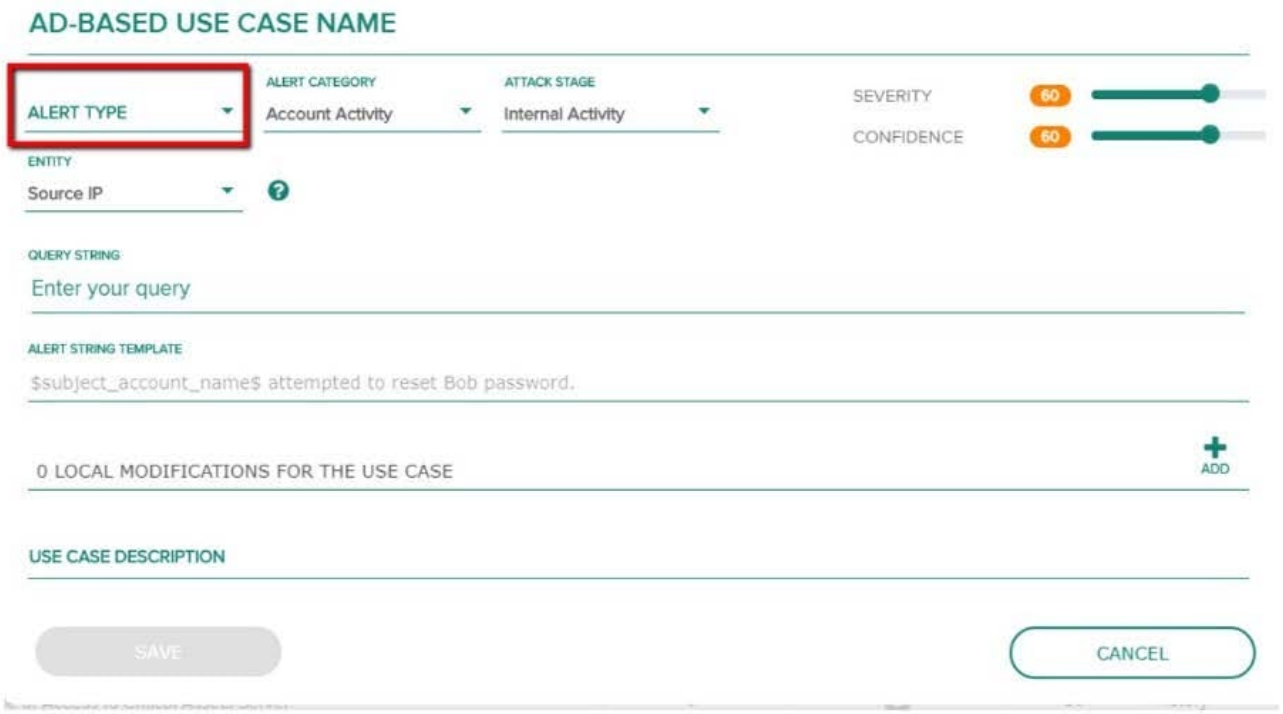
A. Yes

B. No

Correct Answer: B

QUESTION 5

Refer to the exhibit.



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

A. Yes

B. No

Correct Answer: A

QUESTION 6

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 7

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

QUESTION 8

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

QUESTION 9

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.)

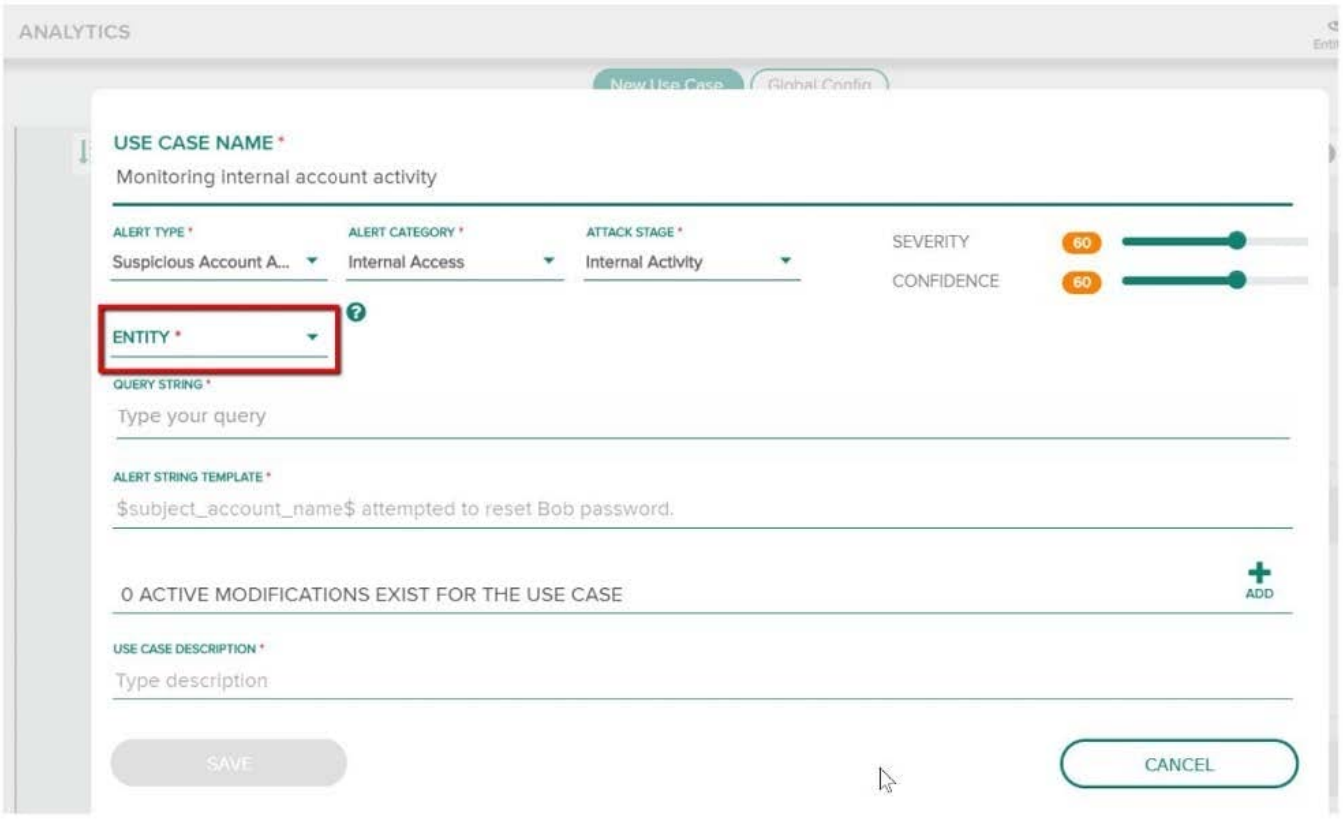
A. Yes

B. No

Correct Answer: B

QUESTION 10

Refer to the exhibit.



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

QUESTION 11

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.)

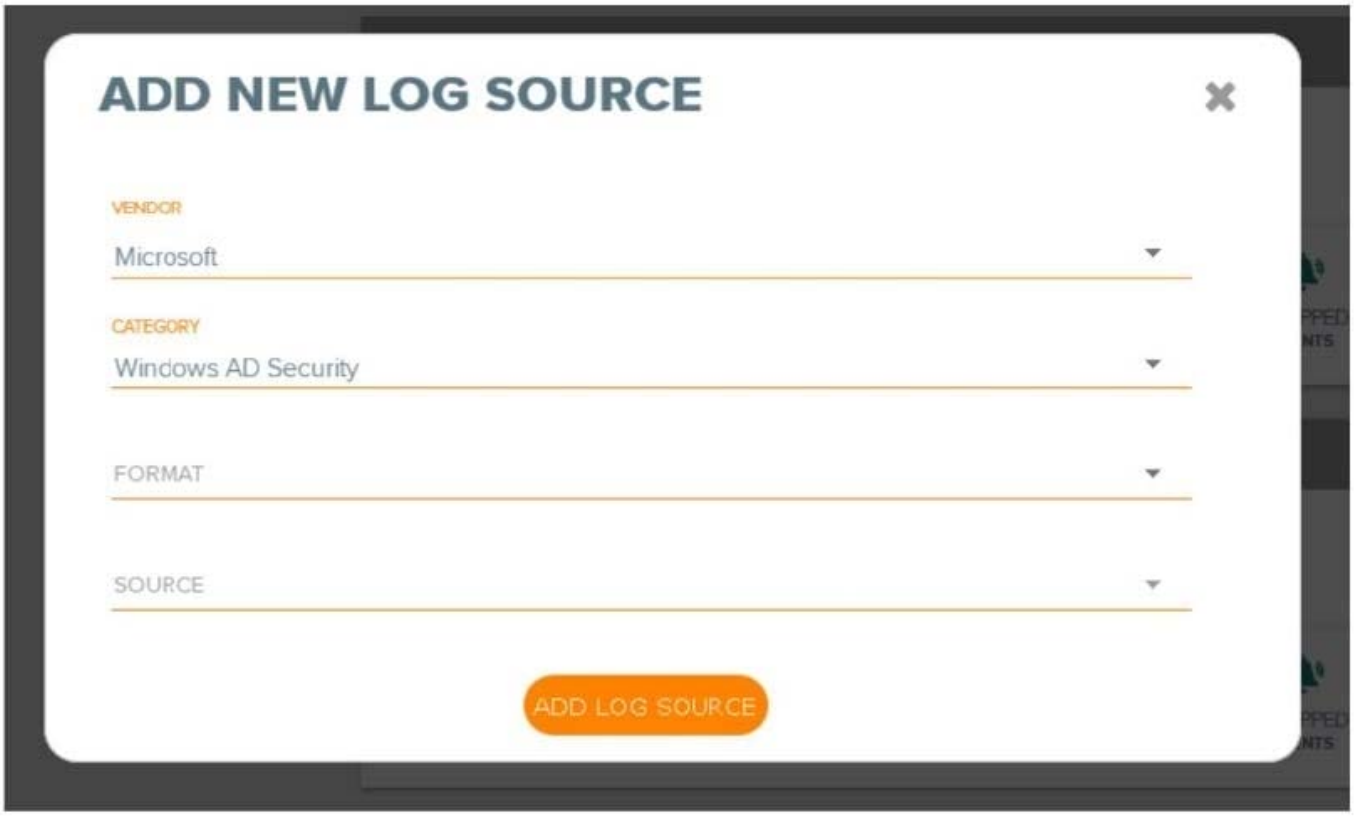
A. Yes

B. No

Correct Answer: B

QUESTION 12

Refer to the exhibit.



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

QUESTION 13

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 14

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

QUESTION 15

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