# 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.pass4itsure.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 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

**QUESTION 2**

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

**QUESTION 3**

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

**QUESTION 4**

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

**QUESTION 5**

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

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

**QUESTION 6**

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.)

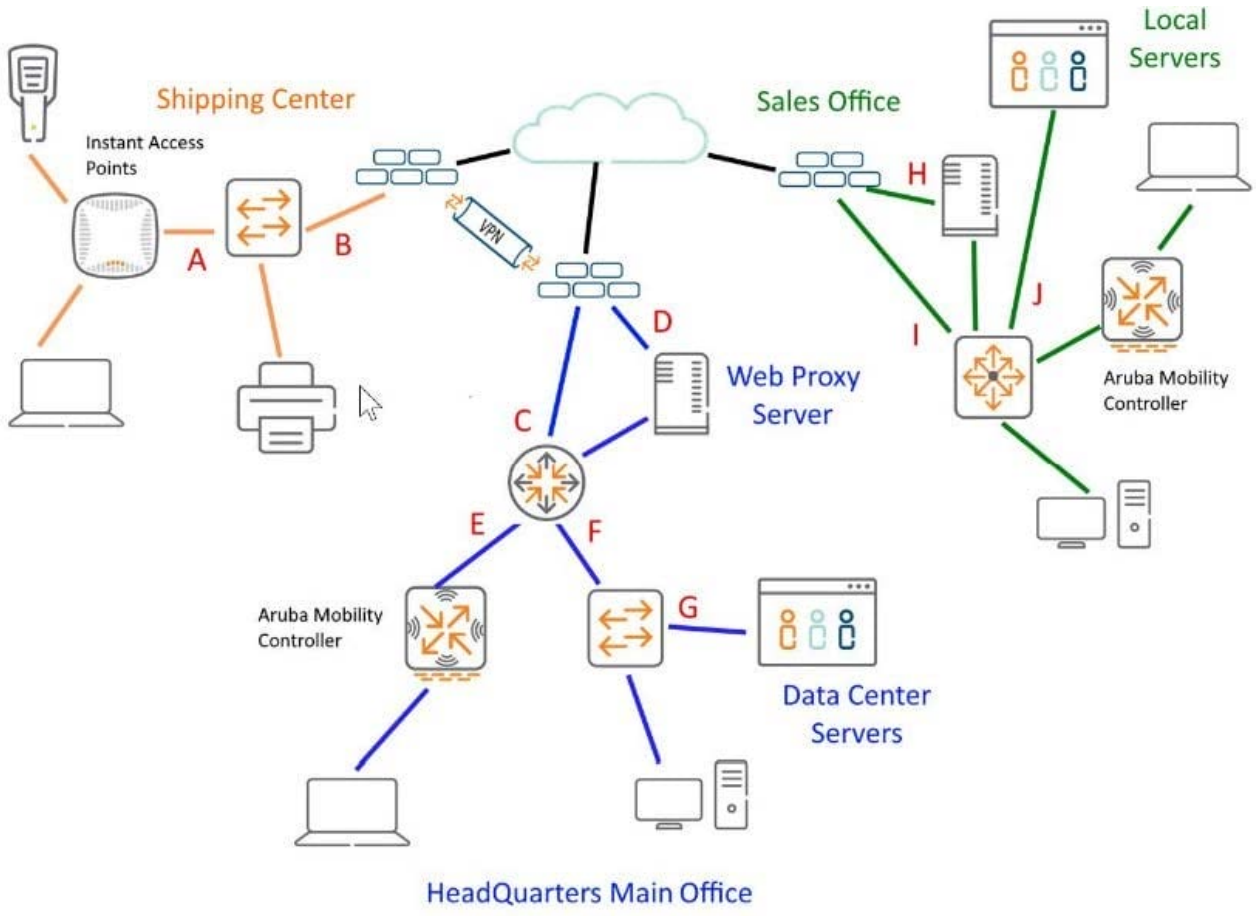
A. Yes

B. No

Correct Answer: A

**QUESTION 7**

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

**QUESTION 8**

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

Reference: IBM QRadar SIEM will push logs to IntroSpect

**QUESTION 9**

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

**QUESTION 10**

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.)

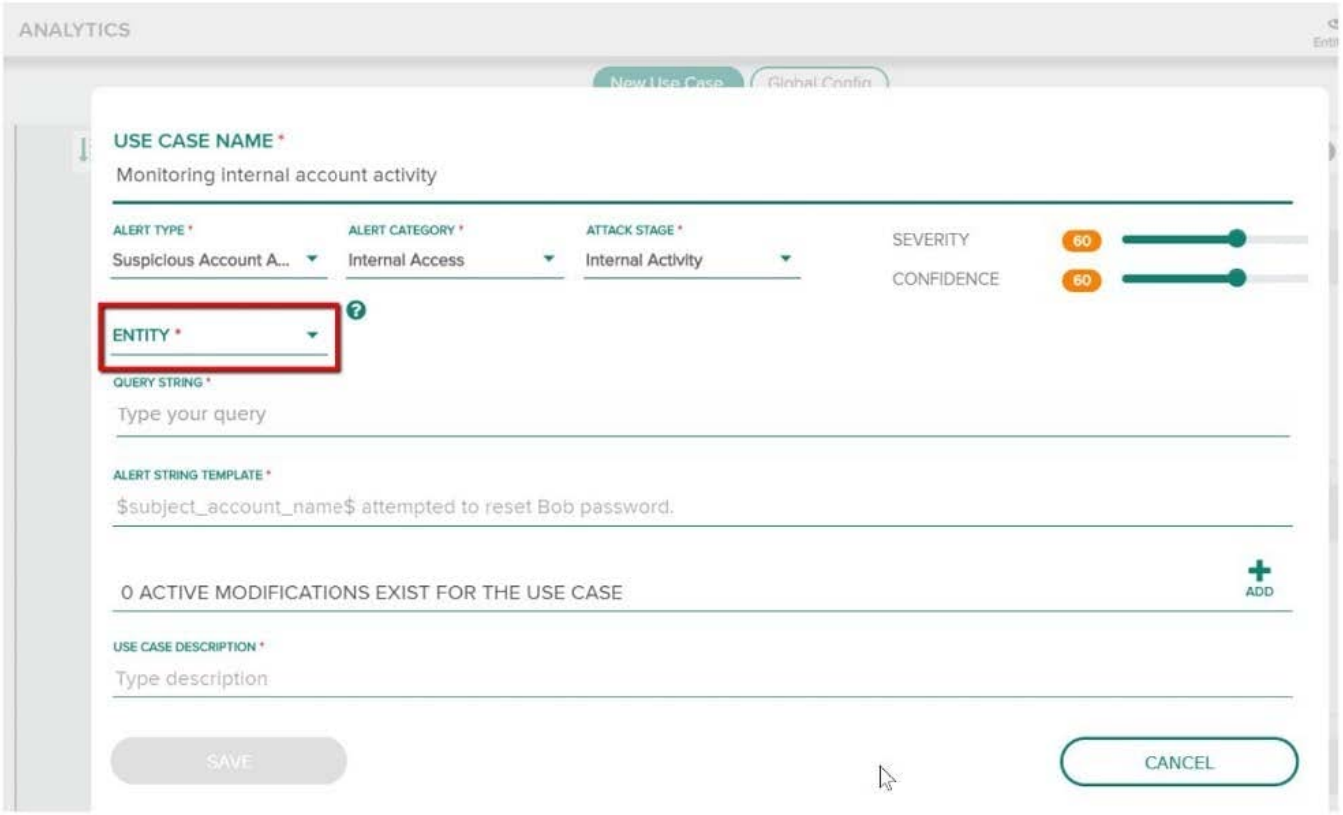
A. Yes

B. No

Correct Answer: B

**QUESTION 11**

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.)

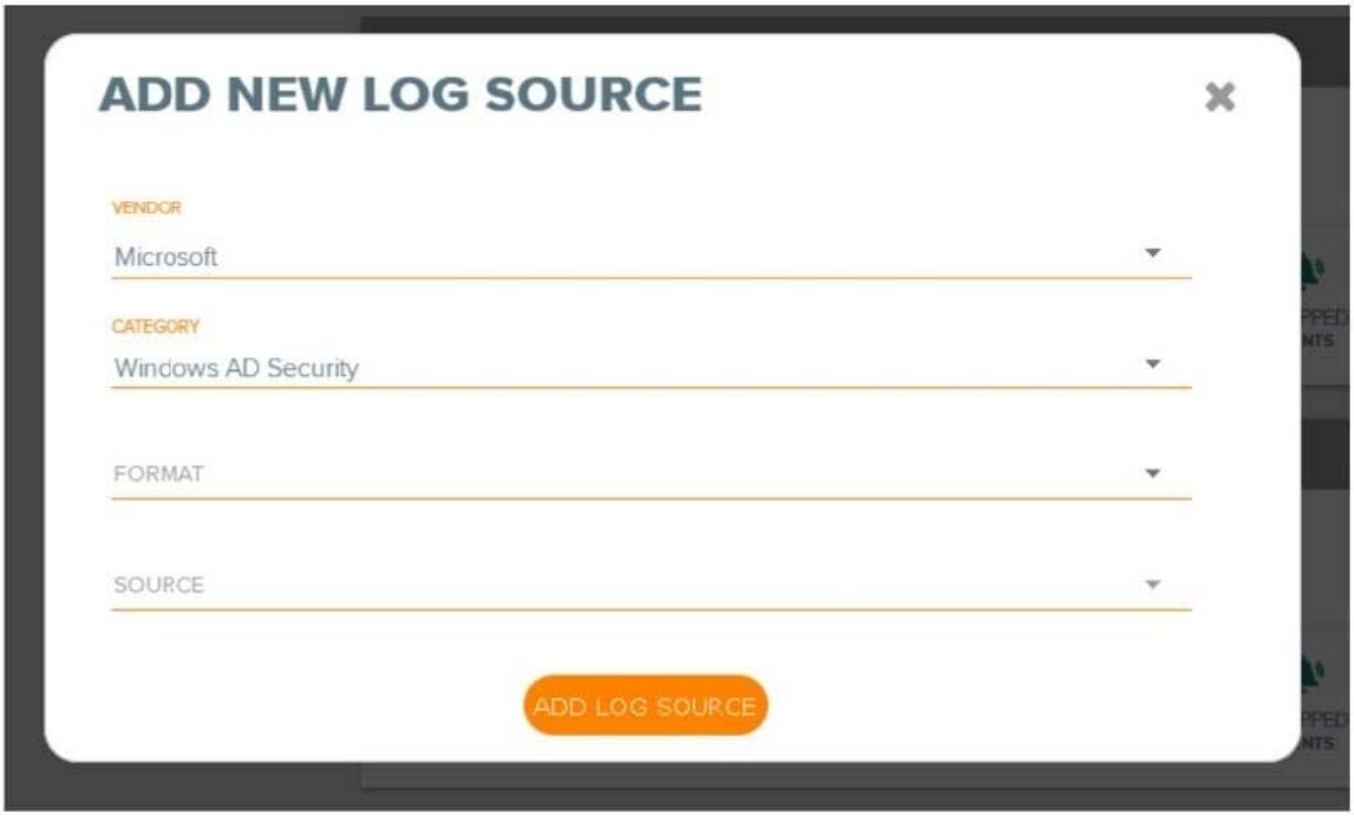
A. Yes

B. No

Correct Answer: A

**QUESTION 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 = Standard, and Source Type = Syslog.)

A. Yes

B. No

Correct Answer: A

**QUESTION 13**

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

**QUESTION 14**

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

**QUESTION 15**

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