

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.leads4pass.com/hpe2-w05.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

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

QUESTION 2

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

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

QUESTION 3

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 4

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

QUESTION 5

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

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

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.)

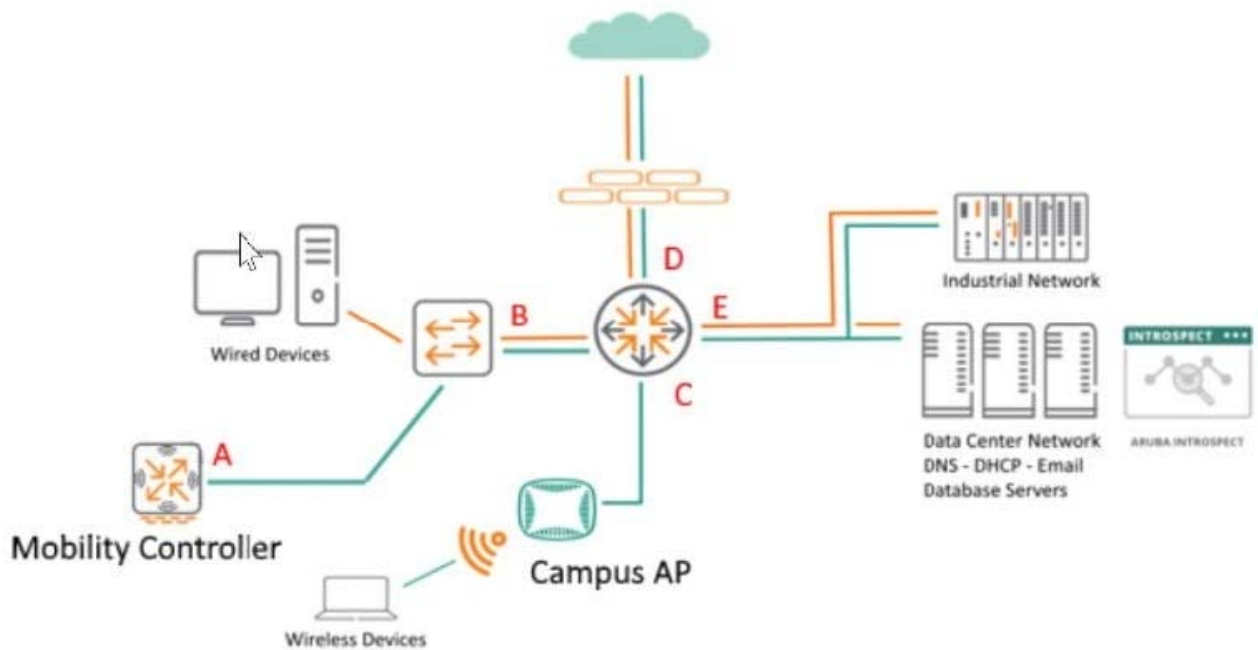
A. Yes

B. No

Correct Answer: A

QUESTION 8

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

QUESTION 9

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

QUESTION 10

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

QUESTION 11

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

QUESTION 12

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

QUESTION 13

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.)

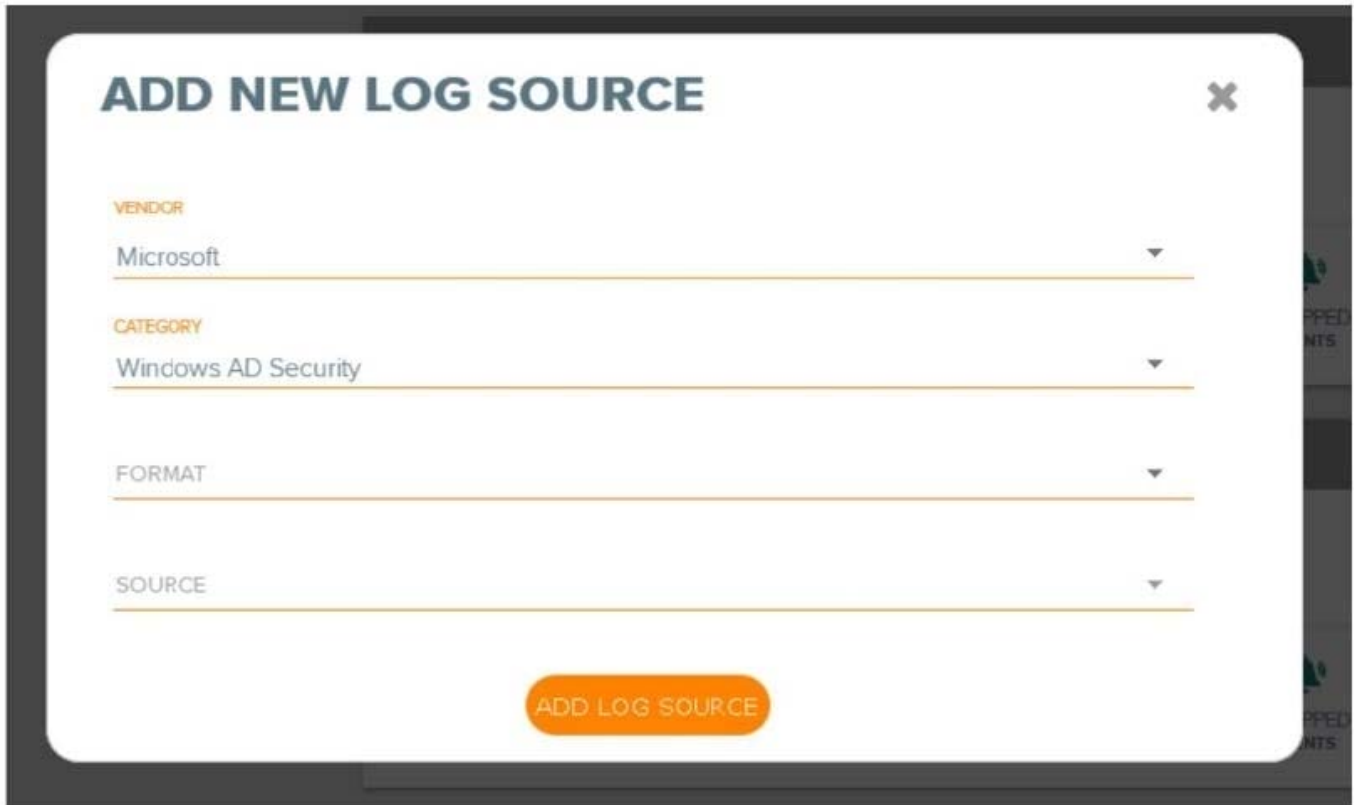
A. Yes

B. No

Correct Answer: A

QUESTION 14

Refer to the exhibit.



ADD NEW LOG SOURCE [X]

VENDOR
Microsoft

CATEGORY
Windows AD Security

FORMAT

SOURCE

ADD LOG SOURCE

An IntroSpec admin is configuring an Aruba IntroSpec 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 15

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