

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.pass2lead.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

Refer to the exhibit.

The screenshot shows a 'New Use Case' form in the 'ANALYTICS' section. The form is titled 'Monitoring internal account activity'. It includes several dropdown menus: 'ALERT TYPE' (Suspicious Account A...), 'ALERT CATEGORY' (Internal Access), and 'ATTACK STAGE' (Internal Activity). There are also sliders for 'SEVERITY' (set to 90) and 'CONFIDENCE' (set to 80). The 'ENTITY' dropdown menu is highlighted with a red box and has a question mark icon next to it. Below the 'ENTITY' field is a 'QUERY STRING' field with the placeholder 'Type your query'. The 'ALERT STRING TEMPLATE' field contains the text '\$subject_account_name\$ attempted to reset Bob password.'. At the bottom of the form, there is a 'SAVE' button and a 'CANCEL' button. A message at the bottom of the form states '0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE' with an 'ADD' button.

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

QUESTION 2

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 3

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

QUESTION 4

An administrator scheduled a maintenance window for upgrading an IntroSpec 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 5

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

[HPE2-W05 Practice Test](#)

[HPE2-W05 Exam Questions](#)

[HPE2-W05 Braindumps](#)