

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

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 2

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 3

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 4

You are administering an IntroSpect Installation. While monitoring the load on the IntroSpect Packet Processors, you think that one Packet Processor is overloaded. Is this a correct statement about the possible overload? (As a general rule, the data rate should be below 9000 event/sec.)

- A. Yes B. No

Correct Answer: B

QUESTION 5

Refer to the exhibit.

The screenshot shows a web interface for configuring an analytics use case. The title is 'ANALYTICS'. At the top, there are buttons for 'New Use Case' and 'Global Config'. The main form has the following sections:

- USE CASE NAME ***: Monitoring internal account activity
- ALERT TYPE ***: Suspicious Account A...
- ALERT CATEGORY ***: Internal Access
- ATTACK STAGE ***: Internal Activity
- SEVERITY**: 90 (with a slider)
- CONFIDENCE**: 60 (with a slider)
- ENTITY ***: (This field is highlighted with a red box and has a question mark icon next to it)
- QUERY STRING ***: Type your query
- ALERT STRING TEMPLATE ***: \$subject_account_name\$ attempted to reset Bob password.
- 0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE** (with an '+ ADD' button)
- USE CASE DESCRIPTION ***: Type description

At the bottom, there are 'SAVE' and 'CANCEL' buttons.

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

[Latest HPE2-W05 Dumps](#)

[HPE2-W05 Exam Questions](#)

[HPE2-W05 Braindumps](#)