**Vendor:**HP

**Exam Code:**HPE2-W05

**Exam Name:**Implementing Aruba IntroSpect

**Version:**Demo

**QUESTION 1**

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 2**

A network administrator is looking for an option to set the maximum data retention period to 180 days in the IntroSpect Analyzer. Is this a correct statement about data retention in IntroSpect? (The data retention period cannot exceed 90 days.)

A. Yes

B. No

Correct Answer: B

---

**QUESTION 3**

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? (Enter a new host name with the command #>/opt/niara/analyzer/lib/hadoop/rename-an-node {analyzer FQDN} in the CLI.)

A. Yes

B. No

Correct Answer: A

Reference: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx? EntryId=27256

---

**QUESTION 4**

You are troubleshooting ClearPass with IntroSpect, and you notice that in Access Tracker the IntroSpect Logon Logoff actions profile is executing. However, the ClearPass Log Source on the IntroSpect Analyzer is showing dropped entries.

Would this be a good troubleshooting step? (Confirm that the ClearPass context action is sending the User name, IP Address, Entity Type, and User Role)

A. Yes

B. No

Correct Answer: A

---

**QUESTION 5**

You deploy IntroSpect Analyzer in your existing network. You want to monitor email for suspect malware activity. Would this action be supported by IntroSpect? (Deploy Splunk SIEM to gather logs from the email servers.)

A. Yes

B. No

Correct Answer: A

---

**QUESTION 6**

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? (SSH into the Packet Processor, and log in as "admin" and issue the command #>shutdown -r now.)

A. Yes

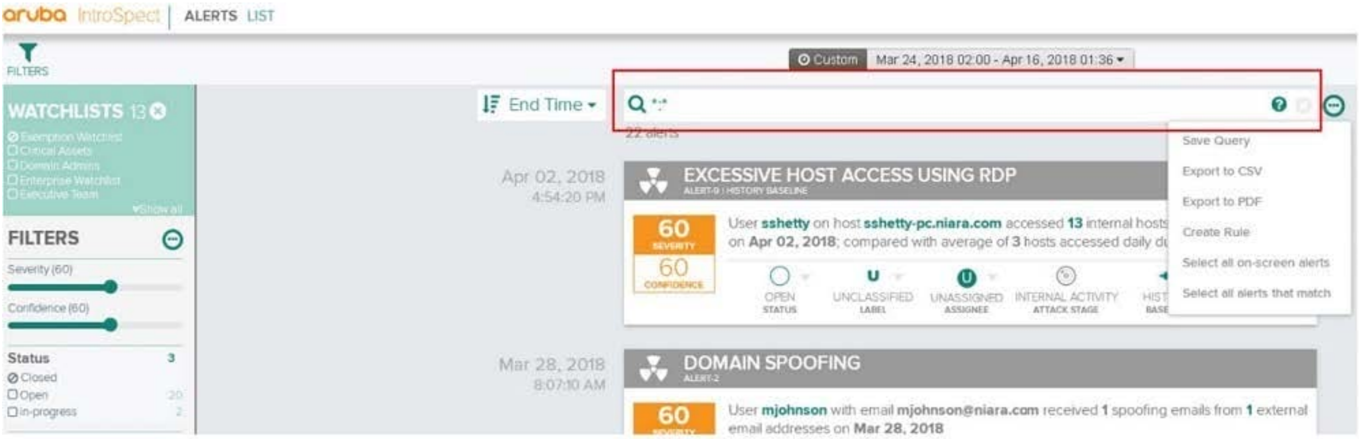
B. No

Correct Answer: B

---

**QUESTION 7**

Refer to the exhibit.



User sshetty on host sshetty-pc.niara.com accessed 13 internal hosts on Apr 02, 2018; compared with average of 3 hosts accessed daily du

User mjohnson with email mjohnson@niara.com received 1 spoofing emails from 1 external email addresses on Mar 28, 2018

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 8**

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? (Contact the firewall administrator from the site and see if any rules have changed that may be blocking TCP port 389.)

A. Yes

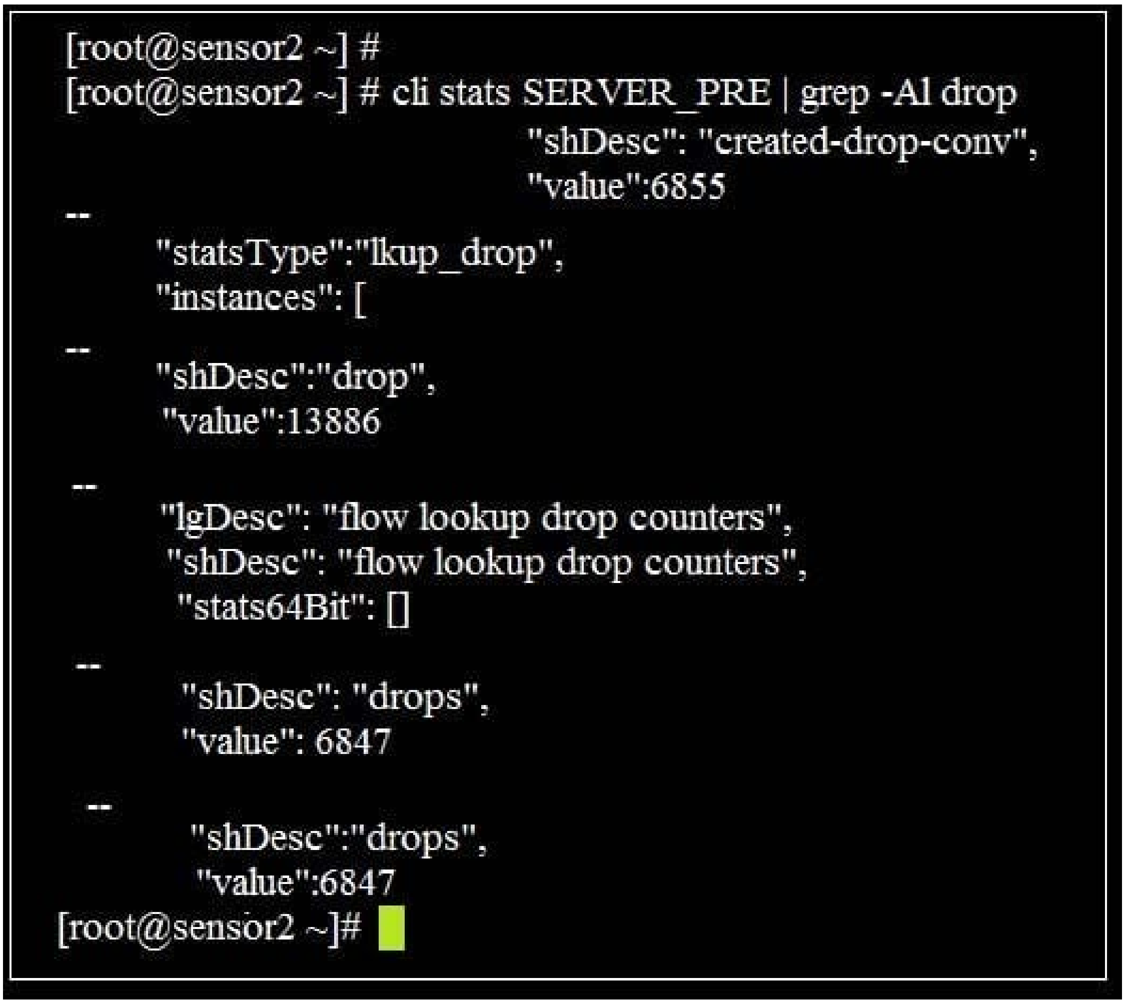
B. No

Correct Answer: B

---

**QUESTION 9**

Refer to the exhibit.



```
[root@sensor2 ~] #
[root@sensor2 ~] # cli stats SERVER_PRE | grep -A1 drop
                                    "shDesc": "created-drop-conv",
                                    "value":6855
--
       "statsType":"lkup_drop",
       "instances": [
--
       "shDesc":"drop",
        "value":13886

 --
        "lgDesc": "flow lookup drop counters",
         "shDesc": "flow lookup drop counters",
          "stats64Bit": []

 --
          "shDesc": "drops",
          "value": 6847

 --
           "shDesc":"drops",
            "value":6847
[root@sensor2 ~]#
```

You are monitoring a new virtual packet processor with a network tap. You run the command "cli stats SERVER_PRE | gre-a1 drop" and then return an hour later and run the same command, but notice there is a significant increase in the number dropped packets.

Could this be a reason for the increase? (The Packet Processor may not be allocated the proper number of memory allocated on the VM server for the size of the TAP.)

A. Yes

B. No

Correct Answer: B

---

**QUESTION 10**

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? (Check the authentication service being used in ClearPass for the Login - Logout enforcement policy.)

A. Yes

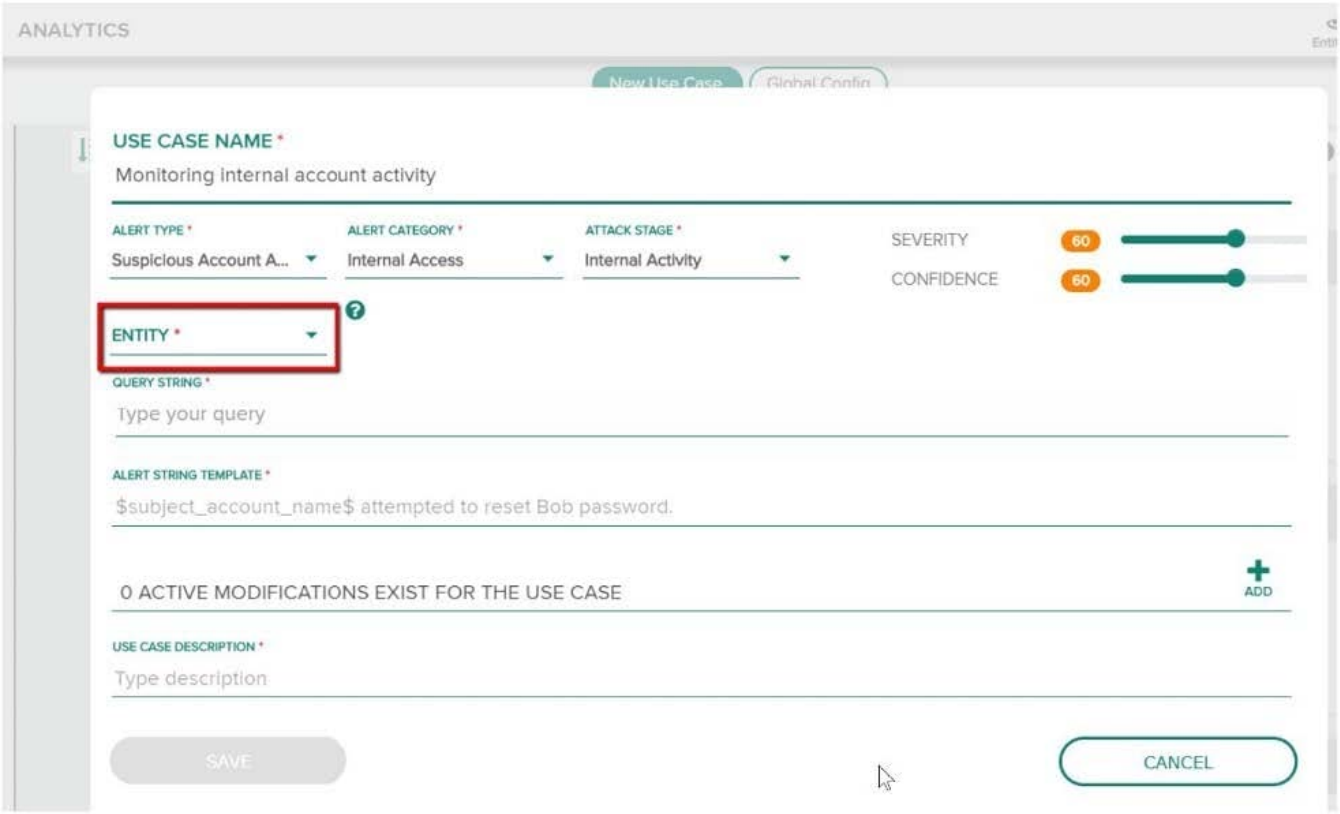
B. No

Correct Answer: B

---

**QUESTION 11**

Refer to the exhibit.



USE CASE NAME *
Monitoring internal account activity

ALERT TYPE * Suspicious Account A...

ALERT CATEGORY * Internal Access

ATTACK STAGE * Internal Activity

SEVERITY 60

CONFIDENCE 60

ENTITY *

QUERY STRING *
Type your query

ALERT STRING TEMPLATE *
$subject_account_name$ attempted to reset Bob password.

0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE

USE CASE DESCRIPTION *
Type description

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? (Host name.)

A. Yes

B. No

Correct Answer: A

---

**QUESTION 12**

While investigating alerts you notice an entity has triggered a peer alert for visiting recruiting websites. Two days later the same user accessed the office for the first time in the late evening. You also noticed that they downloaded more data than their peers through the VPN session. Based on these conditions, is this a possible cause? (This user has just become a flight risk, and is now sending data off the network to use in their next job.)

A. Yes

B. No

Correct Answer: A