100% Money Back Guarantee

Vendor:HP

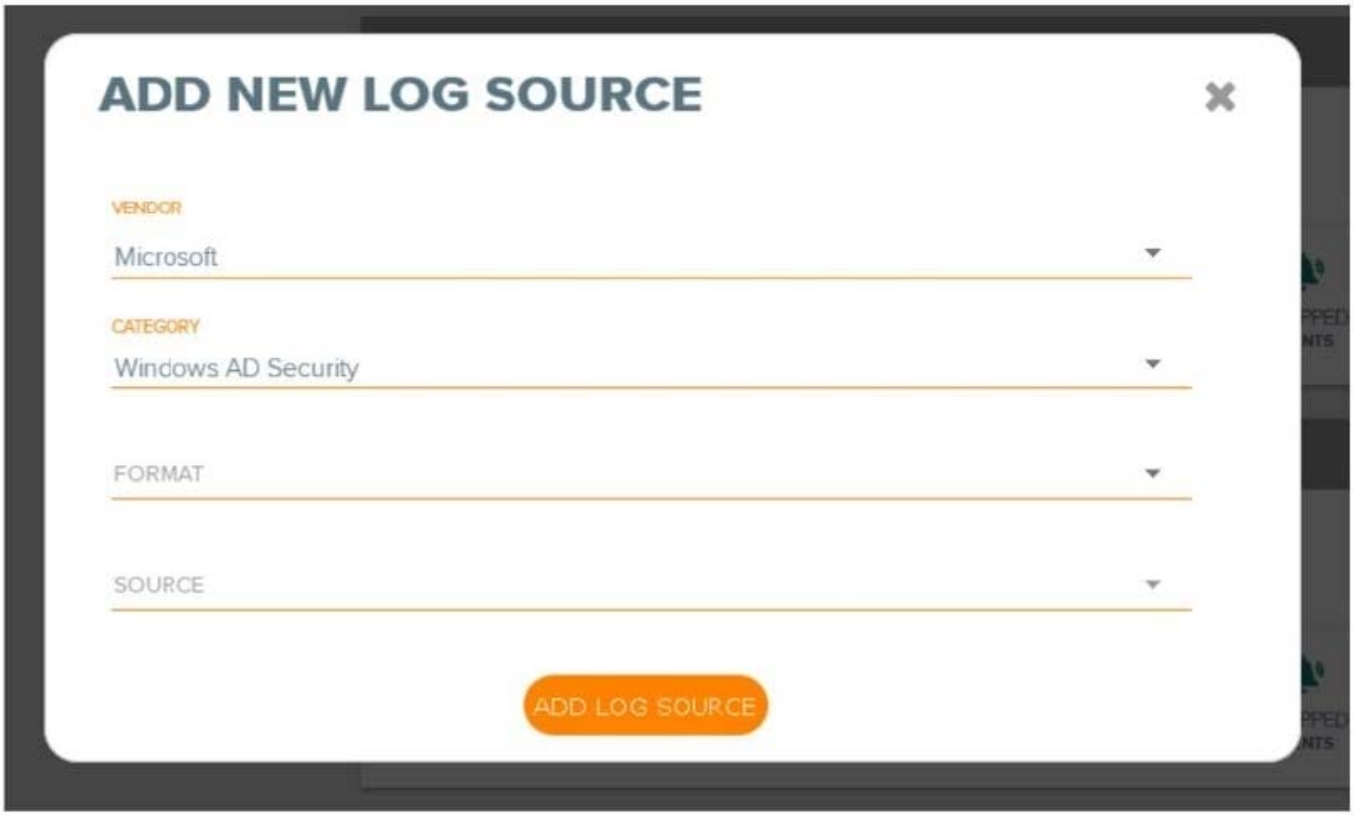
Exam Code:HPE2-W05

Exam Name: Implementing Aruba IntroSpect

Version: Demo

QUESTION 1

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 = Snare, and Source Type = Syslog.)

A. Yes

B. No

Correct Answer: B

QUESTION 2

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? (an attacker conducting reconnaissance on the network.)

A. Yes

B. No

Correct Answer: A

QUESTION 3

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 4

You are visiting a site configured with IntroSpect, and the on-site admin tells you that they do not think that one of their database servers has fired any alerts for large download or strange access patterns. Could this be a reason? (The database server needs to be listed in an entity whitelist.)

A. Yes

B. No

Correct Answer: A

QUESTION 5

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 6

You are configuring a ClearPass Cluster to send endpoint context to an IntroSpect Analyzer for the wireless network. You want to test the setup after you have installed the XML file with the enforcement profiles and actions. Can this method be used to test that the setup is functioning correctly? (Connect to the wireless network, and send a test authentication from a test device/user in the network. Observe the results in Access Tracker.)

A. Yes

B. No

Correct Answer: A

QUESTION 7

You are planning to configure ClearPass to send endpoint context to IntroSpect. You need to create a checklist of functions that must be enabled in ClearPass to support this. Is this an option that is required? (Ingress Event Processing.)

A. Yes

B. No

Correct Answer: B

QUESTION 8

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? (Just restart the system by executing "shutdown ? now" command during the reboot; when prompted, select the option for "reset processor".)

A. Yes

B. No

Correct Answer: B

QUESTION 9

While looking in the IntroSpect Analyzer Conversations screen you see there are a large number of DNS sessions coming from one IP address on the data center network VLAN. Would this be a logical next step? (The device at the IP address could be infected with malware seeking Command and Control. You should audit the device.)

A. Yes

B. No

Correct Answer: A

QUESTION 10

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 11

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 12

You are visiting a site configured with IntroSpect, and the on-site admin tells you that they do not think that one of their database servers has fired any alerts for large download or strange access patterns. Could this be a reason? (The database server needs to be listed under Configuration>Analytics>User Correlation Config.)

A. Yes

B. No

Correct Answer: B