Free Questions for SPLK-3001 by vceexamstest

Shared by Lyons on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is a recommended pre-installation step?

Options:

A- Disable the default search app.

B- Configure search head forwarding.

C- Download the latest version of KV Store from MongoDBxom.

D- Install the latest Python distribution on the search head.

Answer:

B

Question 2

Question Type: MultipleChoice

Analysts have requested the ability to capture and analyze network traffic dat

a. The administrator has researched the documentation and, based on this research, has decided to integrate the Splunk App for Stream with ES.

Which dashboards will now be supported so analysts can view and analyze network Stream data?

Options:

A- Endpoint dashboards.

B- User Intelligence dashboards.

C- Protocol Intelligence dashboards.

D- Web Intelligence dashboards.

Answer:

C

Question 3

Question Type: **MultipleChoice**

A newly built custom dashboard needs to be available to a team of security analysts In ES. How is It possible to Integrate the new dashboard?

Options:

A- Add links on the ES home page to the new dashboard.

B- Create a new role Inherited from es_analyst, make the dashboard permissions read-only, and make this dashboard the default view for the new role.

C- Set the dashboard permissions to allow access by es_analysts and use the navigation editor to add it to the menu.

D- Add the dashboard to a custom add-in app and install it to ES using the Content Manager.

Answer:

C

Question 4

Question Type: MultipleChoice

Where should an ES search head be installed?

Options:

A- On a Splunk server with top level visibility.

B- On any Splunk server.

C- On a server with a new install of Splunk.

D- On a Splunk server running Splunk DB Connect.

Answer:

B

Question 5

Question Type: MultipleChoice

Which lookup table does the Default Account Activity Detected correlation search use to flag known default accounts?

Options:

A- Administrative Identities

B- Local User Intel

C- Identities

D- Privileged Accounts

Answer:

C

Question 6

Question Type: MultipleChoice

What is the bar across the bottom of any ES window?

Options:

A- The Investigator Workbench.

B- The Investigation Bar.

C- The Analyst Bar.

D- The Compliance Bar.

Answer:

B

Question 7

Question Type: MultipleChoice

Following the Installation of ES, an admin configured Leers with the ss_uso r role the ability to close notable events. How would the admin restrict these users from being able to change the status of Resolved notable events to closed?

Options:

A- From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the closed status.

B- From the Status Configuration windows select the closed status. Remove ess_use r from the status transitions for the Resolved status.

C- In Enterprise Security, give the ess_user role the own Notable Events permission.

D- From Splunk Access Controls, select the ess_user role and remove the edit_notabie_events capability.

Answer:

B

Question 8

Question Type: MultipleChoice

Which of these Is a benefit of data normalization?

Options:

A- Reports run faster because normalized data models can be optimized for better performance.

B- Dashboards take longer to build.

C- Searches can be built no matter the specific source technology for a normalized data type.

D- Forwarder-based inputs are more efficient.

Answer:

A

Question 9

Question Type: MultipleChoice

When using distributed configuration management to create the Splunk_TA_ForIndexers package, which three files can be included?

Options:

A- indexes.conf, props.conf, transforms.conf

B- web.conf, props.conf, transforms.conf

C- inputs.conf, props.conf, transforms.conf

D- eventtypes.conf, indexes.conf, tags.conf

Answer:

A

Question 10

Question Type: MultipleChoice

Which of the following actions may be necessary before installing ES?

Options:

A- Redirect distributed search connections.

B- Purge KV Store.

C- Add additional indexers.

D- Add additional forwarders.

Answer:

C

Question 11

Question Type: MultipleChoice

Which tool Is used to update indexers In E5?

Options:

A- Index Updater

B- Distributed Configuration Management

C- indexes.conf

D- Splunk_TA_ForIndexeres. spl

Answer:

B

Question 12

Question Type: MultipleChoice

Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?

Options:

A- SplunkWeb (8068), Splunk Management (8089), KV Store (8000)

B- SplunkWeb (8390), Splunk Management (8323), KV Store (8672)

C- SplunkWeb (8000), Splunk Management (8089), KV Store (8191)

D- SplunkWeb (8043), Splunk Management (8088), KV Store (8191)

Answer:

C

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

To Get Premium Files for SPLK-3001 Visit

https://www.p2pexams.com/products/splk-3001

For More Free Questions Visit

https://www.p2pexams.com/splunk/pdf/splk-3001