DUMPSsheet

Free Questions for SPLK-3002 by dumpssheet

Shared by Haley on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When in maintenance mode, which of the following is accurate?

Options:

A- Once the window is over, KPIs and notable events will begin to be generated again.

B- KPIs are shown in blue while in maintenance mode.

C- Maintenance mode slots are scheduled on a per hour basis.

D- Service health scores and KPI events are deleted until the window is over.

Answer:

A

Question 2

Question Type: MultipleChoice

When must a service define entity rules?

Options:

A- If the intention is for the KPIs in the service to filter to only entities assigned to the service.

B- To enable entity cohesion anomaly detection.

C- If some or all of the KPIs in the service will be split by entity.

D- If the intention is for the KPIs in the service to have different aggregate vs. entity KPI values.

Answer:

A

Explanation:

Provide a value to filter the service to a specific set of entities. These entity rule values are meant to be custom for each service.

Question 3

Question Type: MultipleChoice

Which of the following is a valid type of Multi-KPI Alert?

Options:

A- Score over composite.

B- Value over time.

C- Status over time.

D- Rise over run.

Answer:

C

Question 4

Question Type: **MultipleChoice**

When installing ITSI to support a Distributed Search Architecture, which of the following items apply? (Choose all that apply.)

Options:

A- Copy SA-IndexCreation to all indexers.

B- Copy SA-IndexCreation to the etc/apps directory on the index cluster master node.

C- Extract installer package into etc/apps directory of the cluster deployer node.

D- Extract ITSI app package into etc/apps directory of search head.

Answer:

A

Explanation:

CopySA-IndexCreationto$SPLUNK_HOME/etc/apps/on all individual indexers in your environment.

Question 5

Question Type: MultipleChoice

Which of the following items describe ITSI Backup and Restore functionality? (Choose all that apply.)

Options:

A- A pre-configured default ITSI backup job is provided that can be modified, but not deleted.

B- ITSI backup is inclusive of KV Store, ITSI Configurations, and index dependencies.

C- kvstore_to_json.py can be used in scripts or command line to backup ITSI for full or partial backups.

D- ITSI backups are stored as a collection of JSON formatted files.

Answer:

C, D

Explanation:

ITSI provides akvstore_to_json.pyscript that lets you backup/restore ITSI configuration data, perform bulk service KPI operations, apply time zone offsets for ITSI objects, and regenerate KPI search schedules.

When you run a backup job, ITSI saves your data to a set of JSON files compressed into a single ZIP file.

https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/kvstorejson

https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/BackupandRestoreITSIconfig

Question 6

Question Type: **MultipleChoice**

How do you automatically restrict a KPI to only the entities in its service, and generate KPI values for each entity?

Options:

A- Select "Yes" for both "Split by Entity" and "Filter to Entities in Service".

B- Select "No" for "Split by Entity" and "Yes" for "Filter to Entities in Service".

C- Select "Yes" for "Split by Entity" and "No" for "Filter to Entities in Service".

D- Select "No" for both "Split by Entity" and "Filter to Entities in Service".

Answer:

A

Question 7

Question Type: **MultipleChoice**

There are two departments using ITSI. Finance and Sales. Analysts in each department should not be allowed to see each other's services. What are the role configuration steps required to accomplish this?

Options:

A- itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_analyst.

B- itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_team_analyst; itoa_sales_analyst, inherited from itoa_team_analyst.

C- itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_team_analyst.

D- itoa_finance_admin, inherited from itoa_team_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_analyst.

Answer:

C

Question 8

Question Type: **MultipleChoice**

For which ITSI function is it a best practice to use a 15-30 minute time buffer?

Options:

A- Correlation searches.

B- Adaptive thresholding.

C- Maintenance windows

D- Anomaly detection.

Answer:

C

Explanation:

It's a best practice to schedule maintenance windows with a 15- to 30-minute time buffer before and after you start and stop your maintenance work. This gives the system an opportunity to catch up with the maintenance state and reduces the chances of ITSI generating false positives during maintenance operations.

Question 9

Question Type: MultipleChoice

Which of the following is a good use case regarding defining entities for a service?

Options:

A- Automatically associate entities to services using multiple entity aliases.

B- All of the entities have the same identifying field name.

C- Being able to split a CPU usage KPI by host name.

D- KPI total values are aggregated from multiple different category values in the source events.

Answer:

A

Explanation:

Define entities before creating services. When you configure a service, you can specify entity matching rules based on entity aliases that automatically add the entities to your service.

Question 10

Question Type: MultipleChoice

Which of the following are the default ports that must be configured on Splunk to use ITSI?

Options:

A- SplunkWeb (8405), SplunkD (8519), and HTTP Collector (8628)

B- SplunkWeb (8089), SplunkD (8088), and HTTP Collector (8000)

C- SplunkWeb (8000), SplunkD (8089), and HTTP Collector (8088)

D- SplunkWeb (8088), SplunkD (8089), and HTTP Collector (8000)

Answer:

C

Question 11

Question Type: MultipleChoice

Which of the following describes enabling smart mode for an aggregation policy?

Options:

A- Configure --> Policies --> Smart Mode --> Enable, select "fields", click "Save"

B- Enable grouping in Notable Event Review, select "Smart Mode", select "fields", and click "Save"

C- Edit the aggregation policy, enable smart mode, select fields to analyze, click "Save"

D- Edit the notable event view, enable smart mode, select "fields", and click "Save"

Answer:

A

Explanation:

1. From the ITSI main menu, clickConfiguration>Notable Event Aggregation Policies.

2. Select a custom policy or the Default Policy.

3. Under Smart Mode grouping, enableSmart Mode.

4. ClickSelect fields. A dialog displays the fields found in your notable events from the last 24 hours.