KILL EXAMS

PASS

Splunk

SPLK-3002

Splunk IT Service Intelligence Certified Admin

Question: 243

Which scenario would benefit most by implementing ITSI?

A. Monitoring of business services functionality.
B. Monitoring of system hardware.
C. Monitoring of system process statuses
D. Monitoring of retail sales metrics.

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/AboutSI

Question: 244

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

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

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/REBestPractice

Question: 245

What effects does the KPI importance weight of 11 have on the overall health score of a service?

A. At least 10% of the KPIs will go critical.
B. Importance weight is unused for health scoring.
C. The service will go critical.
D. It is a minimum health indicator KP

Answer: D

Explanation:

Reference:
https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/KPIImportance#:~:text=ITSI%20considers%20KPIs%20that%20have,other%20KPIs%20in%20the%20service

Question: 246

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

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.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Entity/About

Question: 247

What are valid ITSI Glass Table editor capabilities? (Choose all that apply.)

A. Creating glass tables.
B. Correlation search creation.
C. Service swapping configuration.
D. Adding KPI metric lanes to glass tables.

Answer: A,C,D

Explanation:

Create a glass table to visualize and monitor the interrelationships and dependencies across your IT and business services.

The service swapping settings are saved and apply the next time you open the glass table. You can add metrics like KPIs, ad hoc searches, and service health scores that update in real time against a background that you design. Glass tables show real-time data generated by KPIs and services.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/GTOverview

Question: 248

When changing a service template, which of the following will be added to linked services by default?

A. Thresholds.
B. Entity Rules.
C. New KPIs.
D. Health score.

Answer: B

Explanation:

Link multiple services to a service template to manage them collectively in IT Service Intelligence (ITSI). A service can only be linked to one service template at a time. When you link a service to a service template, any existing KPIs in the service are preserved and KPIs in the template are added to the service. You can choose to append, replace, or keep entity rules.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/LinkST

Question: 249

After a notable event has been closed, how long will the meta data for that event remain in the KV Store by default?

A. 6 months.
B. 9 months.
C. 1 year.
D. 3 months.

Answer: A

Explanation:

By default, notable event metadata is archived after six months to keep the KV store from growing too large.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/TrimNECollections

Question: 250

What should be considered when onboarding data into a Splunk index, assuming that ITSI will need to use this data?

A. Use | stats functions in custom fields to prepare the data for KPI calculations.
B. Check if the data could leverage pre-built KPIs from modules, then use the correct TA to onboard the data.
C. Make sure that all fields conform to CIM, then use the corresponding module to import related services.
D. Plan to build as many data models as possible for ITSI to leverage

Answer: B

Explanation:

Question: 252

Which of the following best describes a default deep dive?

A. It initially shows the health scores for all services.
B. It initially shows the highest importance KPIs.
C. It initially shows all of the KPIs for a selected service.
D. It initially shows all the entity swim lanes.

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/DeepDives

Question: 253

When deploying ITSI on a distributed Splunk installation, which component must be installed on the search head(s)?

A. SA-ITOA
B. ITSI app
C. All ITSI components
D. SA-ITSI-Licensechecker

Answer: D

Explanation:

Install SA-ITSI-Licensechecker and SA-UserAccess on any license master in a distributed or search head cluster environment. If a search head in your environment is also a license master, the license master components are installed when you install ITSI on the search heads.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Install/InstallDD

Question: 254

Which of the following are deployment recommendations for ITSI? (Choose all that apply.)

A. Deployments often require an increase of hardware resources above base Splunk requirements.
B. Deployments require a dedicated ITSI search head.
C. Deployments may increase the number of required indexers based on the number of KPI searches.
D. Deployments should use fastest possible disk arrays for indexers.

Answer: A,B,C

Explanation:

You might need to increase the hardware specifications of your own Enterprise Security deployment above the minimum hardware requirements depending on your environment. Install Splunk Enterprise Security on a dedicated search head or search head cluster. The Splunk platform uses indexers to scale horizontally. The number of indexers required in an Enterprise Security deployment varies based on the data volume, data type, retention requirements, search type, and search concurrency.

Reference: https://docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning

Question: 255

Besides creating notable events, what are the default alert actions a correlation search can execute? (Choose all that apply.)

A. Ping a host.
B. Send email.
C. Include in RSS feed.
D. Run a script.

Answer: A,B,C,D

Explanation:

Throttling applies to any correlation search alert type, including notable events and actions (RSS feed, email, run script, and ticketing).

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/ConfigCS

Question: 256

Which of the following describes entities? (Choose all that apply.)

A. Entities must be IT devices, such as routers and switches, and must be identified by either IP value, host name, or mac address.
B. An abstract (pseudo/logical) entity can be used to split by for a KPI, although no entity rules or filtering can be used to limit data to a specific service.
C. Multiple entities can share the same alias value, but must have different role values.
D. To automatically restrict the KPI to only the entities in a particular service, select âFilter to Entities in Serviceâ.

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/KPIfilter

Question: 257

Which of the following is a characteristic of base searches?

A. Search expression, entity splitting rules, and thresholds are configured at the base search level.
B. It is possible to filter to entities assigned to the service for calculating the metrics for the serviceâs KPIs.
C. The fewer KPIs that share a common base search, the more efficiency a base search provides, and anomaly detection is more efficient.
D. The base search will execute whether or not a KPI needs it.

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch

Question: 258

In maintenance mode, which features of KPIs still function?

A. KPI searches will execute but will be buffered until the maintenance window is over.
B. KPI searches still run during maintenance mode, but results go to itsi_maintenance_summary index.
C. New KPIs can be created, but existing KPIs are locked.
D. KPI calculations and threshold settings can be modified.

Answer: A

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.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/AboutMW

Question: 259

Where are KPI search results stored?

A. The default index.
B. KV Store.
C. Output to a CSV lookup.
D. The itsi_summary index.

Answer: D

Explanation:

Search results are processed, created, and written to the itsi_summary index via an alert action.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch

Question: 260

Which of the following is an advantage of using adaptive time thresholds?

A. Automatically update thresholds daily to manage dynamic changes to KPI values.
B. Automatically adjust KPI calculation to manage dynamic event data.
C. Automatically adjust aggregation policy grouping to manage escalating severity.
D. Automatically adjust correlation search thresholds to adjust sensitivity over time.

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/TimePolicies

Question: 261

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

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

Explanation:

Reference: https://splunk.github.io/docker-splunk/ARCHITECTURE.html

Question: 262

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

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: A,C,D

Explanation:

ITSI provides a kvstore_to_json.py script 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.

Reference:

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

https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/BackupandRestoreITSIconfi g

Question: 263

When creating a custom deep dive, what color are services/KPIs in maintenance mode within the topology view?

A. Gray

B. Purple
C. Gear Icon
D. Blue

Answer: A

Explanation:

Services, entities, and KPIs that are fully or partially impacted by a maintenance window appear in a dark gray color on pages that display health scores, including service analyzers, service and entity details pages, glass tables, multi-KPI alerts, and deep dives.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/AboutMW

SAMPLE QUESTIONS

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.