Vendor: Splunk

Exam Code: SPLK-3002

Exam Name: Splunk IT Service Intelligence Certified Admin

Version: DEMO

QUESTION 1
What is an episode?

A. A workflow task.
B. A deep dive.
C. A notable event group.
D. A notable event.

Answer: C
Explanation:
An episode is a deduplicated group of notable events occurring as part of a larger sequence, or an incident or period considered in isolation. An episode helps you reduce alert noise and focus on the most important issues affecting your IT services. An episode is created by an aggregation policy, which is a set of rules that determines how to group notable events based on certain criteria, such as severity, source, title, and so on. You can use episode review to view, manage, and resolve episodes in ITSI.

QUESTION 2
Which index will contain useful error messages when troubleshooting ITSI issues?

A. _introspection
B. _internal
C. itsi_summary
D. itsi_notable_audit

Answer: B
Explanation:
The index that will contain useful error messages when troubleshooting ITSI issues is:
B) _internal. This is true because the _internal index contains logs and metrics generated by Splunk processes, such as splunkd and metrics.log. These logs can help you diagnose problems with your Splunk environment, including ITSI components and features.

QUESTION 3
Which of the following is a recommended best practice for service and glass table design?

A. Plan and implement services first, then build detailed glass tables.
B. Always use the standard icons for glass table widgets to improve portability.
C. Start with base searches, then services, and then glass tables.
D. Design glass tables first to discover which KPIs are important.

Answer: A
Explanation:
A is the correct answer because it is recommended to plan and implement services first, then build detailed glass tables that reflect the service hierarchy and dependencies. This way, you can ensure that your glass tables provide accurate and meaningful service-level insights. Building glass tables first might lead to unnecessary or irrelevant KPIs that do not align with your service goals.

QUESTION 4
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: ABC
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.
A, B, and C are correct answers because ITSI deployments often require more hardware resources than base Splunk requirements due to the high volume of data ingestion and processing. ITSI deployments also require a dedicated search head that runs the ITSI app and handles all ITSI-related searches and dashboards. ITSI deployments may also increase the number of required indexers based on the number and frequency of KPI searches, which can generate a large amount of summary data.

QUESTION 5
What are valid considerations when designing an ITSI Service? (Choose all that apply.)

A. Service access control requirements for ITSI Team Access should be considered, and appropriate teams provisioned prior to creating the ITSI Service.
B. Entities, entity meta-data, and entity rules should be planned carefully to support the service design and configuration.
C. Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summary index.
D. Backfill of a KPI should always be selected so historical data points can be used immediately and alerts based on that data can occur.

Answer: ABC
Explanation:
A, B, and C are correct answers because service access control requirements for ITSI Team Access should be considered before creating the ITSI Service, as different teams may have different permissions and views of the service data. Entities, entity meta-data, and entity rules should also be planned carefully to support the service design and configuration, as they determine how ITSI maps data sources to services and KPIs. Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summary index for faster retrieval and analysis.

QUESTION 6
Anomaly detection can be enabled on which one of the following?

A. KPI
B. Multi-KPI alert
C. Entity
D. Service

Answer: A

Explanation:
A is the correct answer because anomaly detection can be enabled on a KPI level in ITSI. Anomaly detection allows you to identify trends and outliers in KPI search results that might indicate an issue with your system. You can enable anomaly detection for a KPI by selecting one of the two anomaly detection algorithms in the KPI configuration panel.

QUESTION 7
Which index is used to store KPI values?

A. itsi_summary_metrics
B. itsi_metrics
C. itsi_service_health
D. itsi_summary

Answer: A
Explanation:
A is the correct answer because the itsi_summary_metrics index is used to store KPI values in ITSI. This index improves the performance of the searches dispatched by ITSI, particularly for very large environments. Every KPI is summarized in both the itsi_summary events index and the itsi_summary_metrics metrics index.

QUESTION 8
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:
D is the correct answer because KPI search results are stored in the itsi_summary index in ITSI. This index is an events index that stores the results of scheduled KPI searches. Summary indexing lets you run fast searches over large data sets by spreading out the cost of a computationally expensive report over time.

QUESTION 9
Which ITSI functions generate notable events? (Choose all that apply.)

A. KPI threshold breaches.
B. KPI anomaly detection.
C. Multi-KPI alert.
D. Correlation search.

Answer: ABD
Explanation:
After you configure KPI thresholds, you can set up alerts to notify you when aggregate KPI severities change. ITSI generates notable events in Episode Review based on the alerting rules you configure. Anomaly detection generates notable events when a KPI IT Service Intelligence (ITSI) deviates from an expected pattern.
Notable events are typically generated by a correlation search.

A, B, and D are correct answers because ITSI can generate notable events when a KPI breaches a threshold, when a KPI detects an anomaly, or when a correlation search matches a defined pattern. These are the main ways that ITSI can alert you to potential issues or incidents in your IT environment.

QUESTION 10
Which of the following describes a way to delete multiple duplicate entities in ITSI?

A. Via c CSV upload.
B. Via the entity lister page.
C. Via a search using the | deleteentity command.
D. All of the above.

Answer: D
Explanation:
D is the correct answer because ITSI provides multiple ways to delete multiple duplicate entities. You can use a CSV upload to overwrite existing entities with new or updated information, or delete them by setting the action field to delete. You can also use the entity lister page to select multiple entities and delete them in bulk. Alternatively, you can use a search command called | deleteentity to delete entities that match certain criteria.

QUESTION 11
Which capabilities are enabled through "teams"?

A. Teams allow searches against the itsi_summary index.
B. Teams restrict notable event alert actions.
C. Teams restrict searches against the itsi_notable_audit index.
D. Teams allow restrictions to service content in UI views.

Answer: D
Explanation:
D is the correct answer because teams allow you to restrict access to service content in UI views such as service analyzers, glass tables, deep dives, and episode review. Teams also control access to services and KPIs for editing and viewing purposes. Teams do not affect the ability to search against the itsi_summary index, restrict notable event alert actions, or restrict searches against the itsi_notable_audit index.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**