# SPLK-3002 Dumps 2022 New Splunk SPLK-3002 Exam Questions [Q10-Q24


SPLK-3002 Dumps 2022 - New Splunk SPLK-3002 Exam Questions
Free SPLK-3002 braindumps download (SPLK-3002 exam dumps Free Updated)

## Splunk SPLK-3002 Exam Syllabus Topics:

TopicDetailsTopic 1- Managing Notable Events- Define Key Notable Events Terms and their Relationships- Describe Examples of Multi-KPI AlertsTopic 2- Glass Tables, Describe Glass Tables- Use Glass Tables- Design Glass Tables- Configure Glass TablesTopic 3- Define Multi KPI Alerts- Manage Notable Event Storage- Aggregation Policies- Create New Aggregation PoliciesTopic 4- Describe the Notable Events Workflow- Work with Notable Events- Investigating Issues with Deep Dives Topic 5- Anomaly Detection- Enable Anomaly Detection- Work with Generated Anomaly Events- Correlation and Multi KPI Searches- Define New Correlation SearchesTopic 6- Identify What ITSI Does- Describe Reasons for Using ITSI- Examine the ITSI User InterfaceTopic 7- Configure User Access Control- Create Service Level Teams- Troubleshooting ITSI- Backup and Restore- Maintenance Mode, Creating Modules, TroubleshootingTopic 8- Using Entities in KPI Searches- Templates and Dependencies- Use Templates to Manage Services- Define Dependencies Between ServicesTopic 9- Installing and Configuring ITSI- List ITSI Hardware Recommendations- Describe ITSI Deployment Options- Identify ITSI ComponentsTopic 10- Describe the Installation Procedure- Identify Data Input Options for ITSI- Add Custom Data to an ITSI DeploymentTopic 11- Describe Deep Dive Concepts and Their Relationships- Describe Deep Dive Concepts and Their Relationships- Use Default Deep DivesTopic 12- Given Customer Requirements, Plan an ITSI Implementation- Identify Site Entities- Data Audit and Base SearchesTopic 13- Use a Data Audit to Identify Service Key Performance Indicators-

Use a Service Design to Implement Services in ITSI- Thresholds and Time Policies

**NO.10** Within a correlation search, dynamic field values can be specified with what syntax?
* fieldname
* <fieldname /fieldname>
* %fieldname%
* eval(fieldname)

**NO.11** Which of the following are the default ports that must be configured on Splunk to use ITSI?
* SplunkWeb (8405), SplunkD (8519), and HTTP Collector (8628)
* SplunkWeb (8089), SplunkD (8088), and HTTP Collector (8000)
* SplunkWeb (8000), SplunkD (8089), and HTTP Collector (8088)
* SplunkWeb (8088), SplunkD (8089), and HTTP Collector (8000)

**NO.12** After a notable event has been closed, how long will the meta data for that event remain in the KV Store by default?
* 6 months.
* 9 months.
* 1 year.
* 3 months.

Explanation

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

**NO.13** Which capabilities are enabled through “teams”?
* Teams allow searches against the itsi_summary index.
* Teams restrict notable event alert actions.
* Teams restrict searches against the itsi_notable_audit index.
* Teams allow restrictions to service content in UI views.

Explanation

Teams provide presentation-layer security only and not data-level security. It’s still possible for a user with access to the Splunk search bar to look up ITSI summary index data.

**NO.14** Which deep dive swim lane type does not require writing SPL?
* Event lane.
* Automatic lane.
* Metric lane.
* KPI lane.

Explanation

Among all the search configurations, automatic lane doesn’t need to be written in Splunk Processing language.

**NO.15** Which of the following is a good use case regarding defining entities for a service?
* Automatically associate entities to services using multiple entity aliases.
* All of the entities have the same identifying field name.
* Being able to split a CPU usage KPI by host name.
* KPI total values are aggregated from multiple different category values in the source events.

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.

**NO.16** Which of the following items apply to anomaly detection? (Choose all that apply.)
* Use AD on KPIs that have an unestablished baseline of data points. This allows the ML pattern to perform it’s magic.
* A minimum of 24 hours of data is needed for anomaly detection, and a minimum of 4 entities for cohesive analysis.
* Anomaly detection automatically generates notable events when KPI data diverges from the pattern.
* There are 3 types of anomaly detection supported in ITSI: adhoc, trending, and cohesive.

**NO.17** When deploying ITSI on a distributed Splunk installation, which component must be installed on the search head(s)?
* SA-ITOA
* ITSI app
* All ITSI components
* SA-ITSI-Licensechecker

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.

**NO.18** In maintenance mode, which features of KPIs still function?
* KPI searches will execute but will be buffered until the maintenance window is over.
* KPI searches still run during maintenance mode, but results go to itsi_maintenance_summary index.
* New KPIs can be created, but existing KPIs are locked.
* KPI calculations and threshold settings can be modified.

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.

**NO.19** Which index is used to store KPI values?
* itsi_summary_metrics
* itsi_metrics
* itsi_service_health
* itsi_summary

Explanation

The IT Service Intelligence (ITSI) metrics summary index, itsi_summary_metrics, is a metrics-based summary index that stores KPI data.

**NO.20** Which of the following is the best use case for configuring a Multi-KPI Alert?
* Comparing content between two notable events.
* Using machine learning to evaluate when data falls outside of an expected pattern.
* Comparing anomaly detection between two KPIs.
* Raising an alert when one or more KPIs indicate an outage is occurring.

**NO.21** Which glass table feature can be used to toggle displaying KPI values from more than one service on a single widget?
* Service templates.

* Service dependencies.
* Ad-hoc search.
* Service swapping.

**NO.22** Which of the following describes a way to delete multiple duplicate entities in ITSI?
* Via c CSV upload.
* Via the entity lister page.
* Via a search using the | deleteentity command.
* All of the above.

Explanation

Import entities from CSV files that contain one or more entity definitions. Importing entities from CSV files is an efficient way to define multiple entities.

**NO.23** What is the default importance value for dependent services’ health scores?
* 11
* 1
* Unassigned
* 10

Explanation

By default, impacting service health scores have an importance value of 11.

**NO.24** Where are KPI search results stored?
* The default index.
* KV Store.
* Output to a CSV lookup.
* The itsi_summary index.

Explanation

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