DUMPSARENA

Splunk IT Service Intelligence Certified Admin Exam

Splunk SPLK-3002

Version Demo

Total Demo Questions: 10

Total Premium Questions: 53

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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.

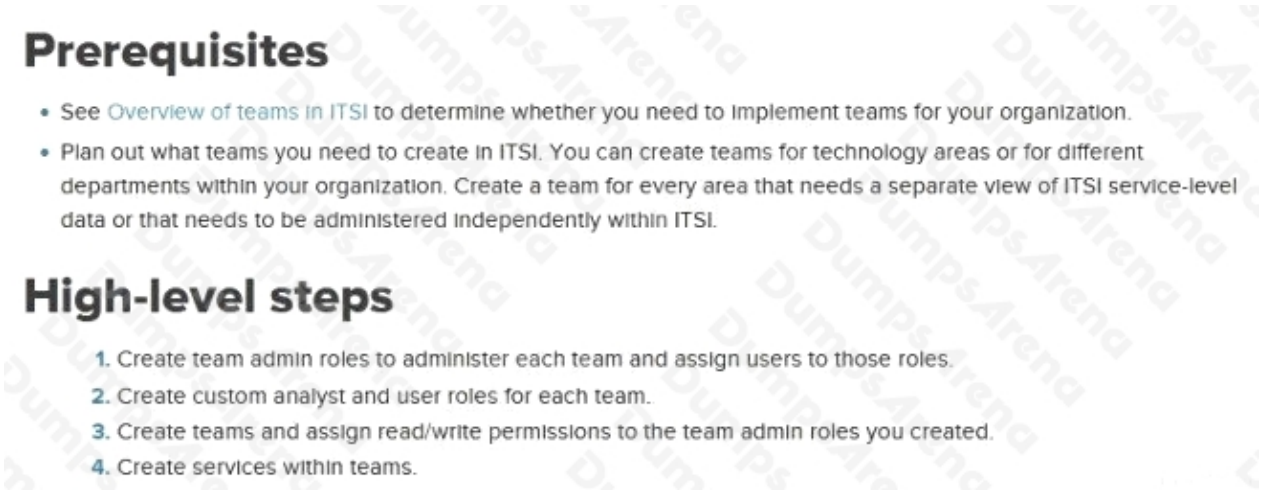
C. Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summary index.

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: A C

Explanation:

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



Prerequisites

- See Overview of teams in ITSI to determine whether you need to implement teams for your organization.
- Plan out what teams you need to create in ITSI. You can create teams for technology areas or for different departments within your organization. Create a team for every area that needs a separate view of ITSI service-level data or that needs to be administered independently within ITSI.

High-level steps

1. Create team admin roles to administer each team and assign users to those roles.
2. Create custom analyst and user roles for each team.
3. Create teams and assign read/write permissions to the team admin roles you created.
4. Create services within teams.

QUESTION NO: 2

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

https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/ServiceSwap

QUESTION NO: 3

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.

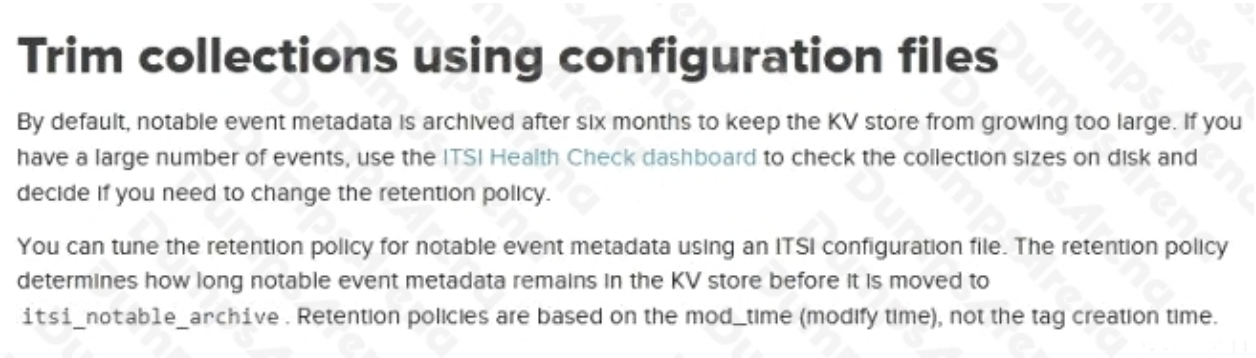
D. 3 months.

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



Trim collections using configuration files

By default, notable event metadata is archived after six months to keep the KV store from growing too large. If you have a large number of events, use the ITSI Health Check dashboard to check the collection sizes on disk and decide if you need to change the retention policy.

You can tune the retention policy for notable event metadata using an ITSI configuration file. The retention policy determines how long notable event metadata remains in the KV store before it is moved to `itsi_notable_archive`. Retention policies are based on the mod_time (modify time), not the tag creation time.

QUESTION NO: 4

Which of the following items apply to anomaly detection? (Choose all that apply.)

A. Use AD on KPIs that have an unestablished baseline of data points. This allows the ML pattern to perform it's magic.

B. A minimum of 24 hours of data is needed for anomaly detection, and a minimum of 4 entities for cohesive analysis.

C. Anomaly detection automatically generates notable events when KPI data diverges from the pattern.

D. There are 3 types of anomaly detection supported in ITSI: adhoc, trending, and cohesive.

ANSWER: B C

Explanation:

The KPI must be split by entity, and a minimum of four entities is required.

If the KPI diverges from the normal pattern, ITSI creates a notable event in Episode Review.

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

QUESTION NO: 5

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 NO: 6

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.

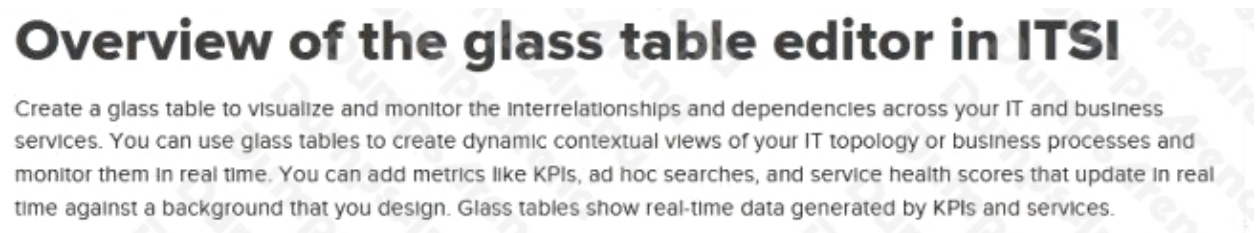
C. Start with base searches, then services, and then glass tables.

D. Design glass tables first to discover which KPIs are important.

ANSWER: D

Explanation:

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



QUESTION NO: 7

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.

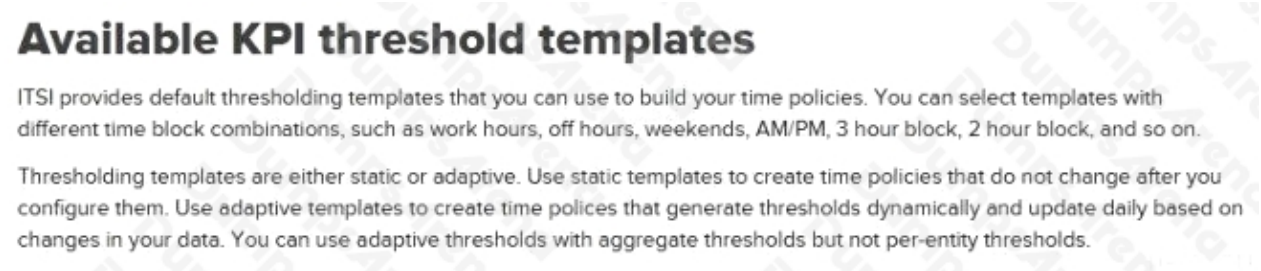
C. Automatically adjust aggregation policy grouping to manage escalating severity.

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



Available KPI threshold templates

ITSI provides default thresholding templates that you can use to build your time policies. You can select templates with different time block combinations, such as work hours, off hours, weekends, AM/PM, 3 hour block, 2 hour block, and so on.

Thresholding templates are either static or adaptive. Use static templates to create time policies that do not change after you configure them. Use adaptive templates to create time polices that generate thresholds dynamically and update daily based on changes in your data. You can use adaptive thresholds with aggregate thresholds but not per-entity thresholds.

QUESTION NO: 8

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.

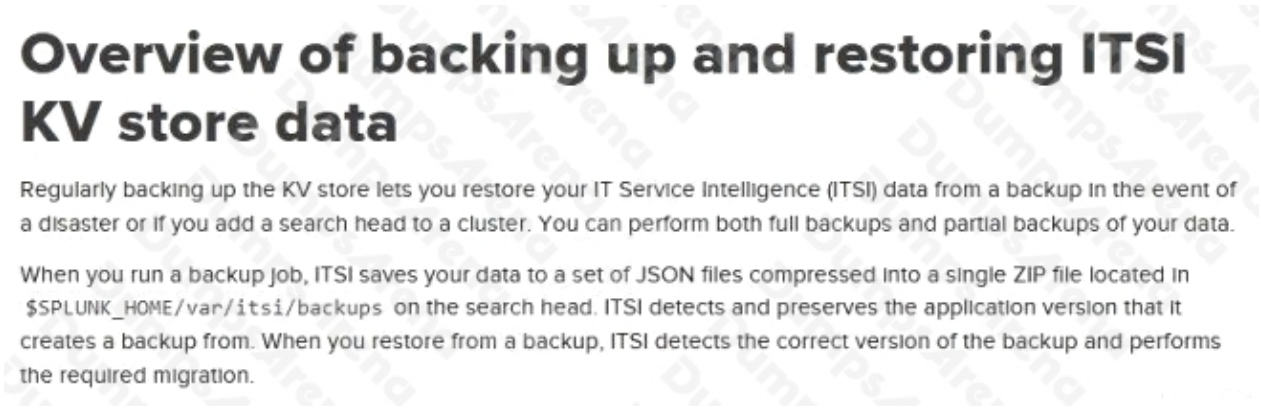
ANSWER: C D

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/BackupandRestoreITSIconfig



Overview of backing up and restoring ITSI KV store data

Regularly backing up the KV store lets you restore your IT Service Intelligence (ITSI) data from a backup in the event of a disaster or if you add a search head to a cluster. You can perform both full backups and partial backups of your data.

When you run a backup job, ITSI saves your data to a set of JSON files compressed into a single ZIP file located in `$SPLUNK_HOME/var/itsi/backups` on the search head. ITSI detects and preserves the application version that it creates a backup from. When you restore from a backup, ITSI detects the correct version of the backup and performs the required migration.

QUESTION NO: 9

Which of the following is a best practice when configuring maintenance windows?

A. Disable any glass tables that reference a KPI that is part of an open maintenance window.

B. Develop a strategy for configuring a service's notable event generation when the service's maintenance window is open.

C. Give the maintenance window a buffer, for example, 15 minutes before and after actual maintenance work.

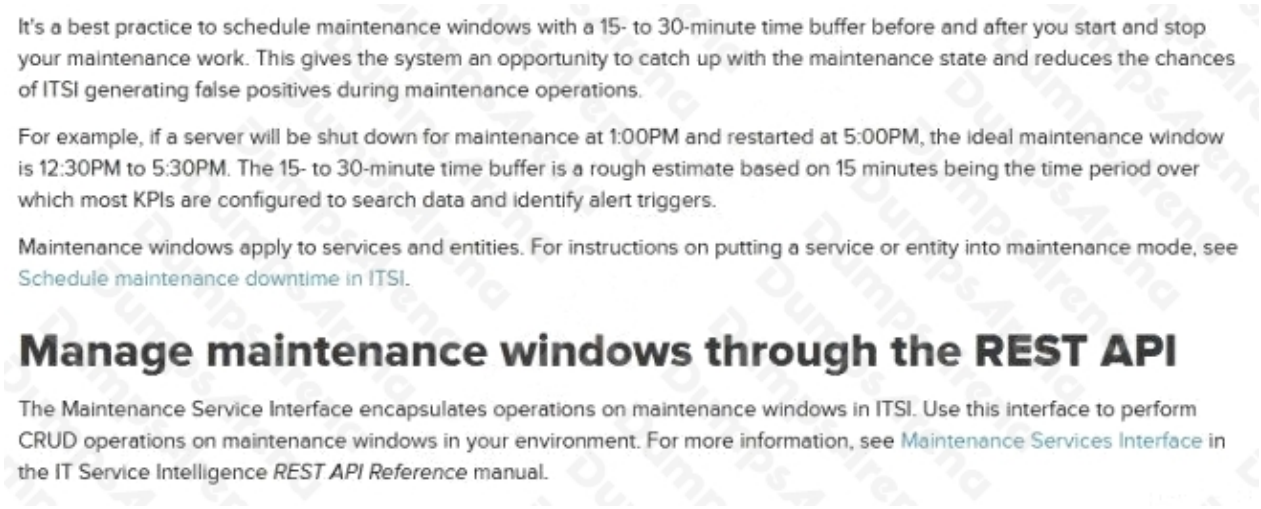
D. Change the color of services and entities that are part of an open maintenance window in the service analyzer.

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.

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



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.

For example, if a server will be shut down for maintenance at 1:00PM and restarted at 5:00PM, the ideal maintenance window is 12:30PM to 5:30PM. The 15- to 30-minute time buffer is a rough estimate based on 15 minutes being the time period over which most KPIs are configured to search data and identify alert triggers.

Maintenance windows apply to services and entities. For instructions on putting a service or entity into maintenance mode, see Schedule maintenance downtime in ITSI.

Manage maintenance windows through the REST API

The Maintenance Service Interface encapsulates operations on maintenance windows in ITSI. Use this interface to perform CRUD operations on maintenance windows in your environment. For more information, see Maintenance Services Interface in the IT Service Intelligence *REST API Reference* manual.

QUESTION NO: 10

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: 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

Actions

Actions are other alert types that a correlation search can trigger. You configure action alerts independently from other alert types, such as Notable Events and Risk Scoring.

Action	Description
Include in RSS feed	Posts the correlation search alert on the Splunk Enterprise RSS feed.
Send email	Sends an email about the correlation search alert. • **Email subject**: The email subject defaults to "Splunk Alert: $name$", where $name$ is the correlation search Search Name. • **Email address(es)**: Insert email addresses and/or distribution lists that should receive the alert. • **Include entity information**: Appends entity information to the subject of the email. • **Include results in email**: Adds the correlation search results in the body of the email in the format you specify. • **Attach results in a PDF**: Includes the correlation search results as a PDF attachment. The schedule_search capability and the admin_all_objects capability are required for PDF delivery scheduling. • **Attach results in a CSV**: Includes the correlation search results as a CSV attachment. **Note:** Email actions require that you configure the mail server in Splunk Enterprise. See Configure email notification settings in the *Alerting Manual*.
Run a script	Triggers a shell script. See Configure a script for an alert action in the *Alerting Manual*.