Question #1 *Topic 1*

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

sutcocuk 6 months, 4 weeks ago

Selected Answer: A

p380 of slides

Retention and Notable Indexes

• Retention policy (time to hold notable info in KV store after episode is closed) is set in:

• etc/apps/SA-ITOA/local/itsi_notable_event_retention.conf • Default 6 months

upvoted 1 times

qtygbapjpesdayazko 1 year ago

What is the name of the slides?

upvoted 1 times

qtygbapjpesdayazko 1 year, 1 month ago

Selected Answer: A

Stores episode tags that have been moved from the KV store after a default 6 month retention period

upvoted 1 times

otb_282 1 year, 8 months ago

Agreed, 6 months. p410 of slides.

upvoted 2 times

Question #2 *Topic 1*

Which of the following is a best practice for identifying the most effective services with which to start an iterative ITSI deployment?

A. Only include KPIs if they will be used in multiple services.

B. Analyze the business to determine the most critical services.

C. Focus on low-level services.

D. Define a large number of key services early.

Suggested Answer: *A*

Community vote distribution

B (100%)

qtygbapjpesdayazko 1 year ago

What is the name of the slides?

upvoted 1 times

anwar_mian 1 year, 1 month ago

The answer should be B

upvoted 1 times

nareshkumar1985 1 year, 7 months ago

B is the correct answer

upvoted 1 times

Marco63 1 year, 8 months ago

Selected Answer: B

see slides!

upvoted 1 times

otb_282 1 year, 8 months ago

B - Analyze for most critical services.

upvoted 3 times

Question #3 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

sutcocuk 6 months, 4 weeks ago

Selected Answer: A

p455

Service Analyzer: Maintenance Mode

In maintenance mode, service and KPI tiles are dark grey and display a maintenance icon

upvoted 1 times

qtygbapjpesdayazko 1 year ago

What is the name of the slides? Is there a link to download?

upvoted 1 times

nosavotor 1 year, 1 month ago

Best without wildcards

upvoted 1 times

Question #4 *Topic 1*

Which deep dive swim lane type does not require writing SPL?

A. Event lane.

B. Automatic lane.

C. Metric lane.

D. KPI lane.

Suggested Answer: *B*

Community vote distribution

D (100%)

qtygbapjpesdayazko 1 year ago

What is the name of the slides?

upvoted 1 times

anwar_mian 1 year, 1 month ago

KPI Lane do not always require SPL. There is no such thing as Automatic Lane.

Deep Dive has three lanes:

KPI

Metric

Event

upvoted 1 times

Marco63 1 year, 8 months ago

Selected Answer: D

see slides

upvoted 2 times

qtygbapjpesdayazko 1 year, 1 month ago

whats is the name of the file? Thanks!

upvoted 1 times

Marco63 1 year, 8 months ago

D: KPI Lane

upvoted 1 times

otb_282 1 year, 8 months ago

D. KPI lane - as SPL pre-populated from selecting service and KPI, whereas Metric and Event requires ad-hoc search to be written.

Automatic, doesn't exist.

upvoted 4 times

Question #5 *Topic 1*

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.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

Manish7 1 year ago

Selected Answer: BC

BC is correct

upvoted 2 times

nosavotor 1 year, 1 month ago

Friends could you please confirm this answer

upvoted 1 times

Question #6 *Topic 1*

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.

Suggested Answer: *C*

Community vote distribution

C (100%)

sutcocuk 6 months, 4 weeks ago

Selected Answer: C

Best practice: schedule maintenance windows about 15 to 30 minutes before and after actual maintenance work

upvoted 1 times

anwar_mian 1 year, 1 month ago

15-30 Window before and after maintenance.

upvoted 1 times

nosavotor 1 year, 1 month ago

Best without wildcards

upvoted 1 times

Question #7 *Topic 1*

In Episode Review, what is the result of clicking an episode's Acknowledge button?

A. Assign the current user as owner.

B. Change status from New to Acknowledged.

C. Change status from New to In Progress and assign the current user as owner.

D. Change status from New to Acknowledged and assign the current user as owner.

Suggested Answer: *C*

Community vote distribution

C (100%)

sutcocuk 6 months, 4 weeks ago

Selected Answer: C

Acknowledge the episode (status: In Progress owner: you)

upvoted 1 times

anwar_mian 1 year, 1 month ago

Answer should be C - New to In-Progress

upvoted 2 times

nosavotor 1 year, 1 month ago

Best without wildcards

upvoted 1 times

Question #8 *Topic 1*

Which glass table feature can be used to toggle displaying KPI values from more than one service on a single widget?

A. Service templates.

B. Service dependencies.

C. Ad-hoc search.

D. Service swapping.

Suggested Answer: *C*

Community vote distribution

D (100%)

Manish7 1 year ago

Selected Answer: D

D is correct.

upvoted 2 times

anwar_mian 1 year, 1 month ago

Answer should be D.

upvoted 2 times

nareshkumar1985 1 year, 7 months ago

Selected Answer: D

D is the correct answer

upvoted 2 times

otb_282 1 year, 8 months ago

D. Service swapping - slide 39.

upvoted 3 times

Question #9 *Topic 1*

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 service's 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.

Suggested Answer: *B*

Community vote distribution

B (100%)

SamKing 1 year ago

Definitely not C and D , A doesn't seems to be best practice , B should be the closes options

upvoted 2 times

Manish7 1 year ago

Selected Answer: B

B is correct

upvoted 2 times

nosavotor 1 year, 1 month ago

Could someone please verify the accuracy of this answer

upvoted 1 times

Question #10 *Topic 1*

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.

Suggested Answer: *ACD*

Community vote distribution

AC (100%)

Manish7 1 year ago

Selected Answer: AC

A and C are correct, lanes are used in Deep Dives.

upvoted 2 times

otb_282 1 year, 8 months ago

A + C. Think D is just for Deep Dives.

upvoted 3 times

Question #11 *Topic 1*

Which of the following is the best use case for configuring a Multi-KPI Alert?

A. Comparing content between two notable events.

B. Using machine learning to evaluate when data falls outside of an expected pattern.

C. Comparing anomaly detection between two KPIs.

D. Raising an alert when one or more KPIs indicate an outage is occurring.

Suggested Answer: *A*

Community vote distribution

D (100%)

SamKing 1 year ago

D is correct

upvoted 2 times

Manish7 1 year ago

Selected Answer: D

D is correct.

upvoted 3 times

otb_282 1 year, 8 months ago

D. Raising an alert when one or more KPIs indicate an outage is occurring - slide 391.

upvoted 3 times

Question #12 *Topic 1*

In distributed search, which components need to be installed on instances other than the search head?

A. SA-IndexCreation and SA-ITSI-Licensechecker on indexers.

B. SA-IndexCreation and SA-ITOA on indexers; SA-ITSI-Licensechecker and SA-UserAccess on the license master.

C. SA-IndexCreation on idexers; SA-ITSI-Licensechecker and SA-UserAccess on the license master.

D. SA-ITSI-Licensechecker on indexers.

Suggested Answer: *A*

Community vote distribution

C (100%)

Manish7 1 year ago

Selected Answer: C

C is correct.

upvoted 1 times

anwar_mian 1 year, 1 month ago

C should be good answer for a clustered environment. Clustered environment is by default distributed environment, not vice versa.

upvoted 1 times

otb_282 1 year, 8 months ago

C - slide 117.

upvoted 2 times

Question #13 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

C (100%)

Ash_111 8 months, 3 weeks ago

Slight conflict between B and C:
1: slide 427 says:
ITSI Component Locations
• Search heads: all ITSI

• Indexers: SA-IndexCreation
• ITSI indexes
• License Master: SA-ITSI-Licensechecker and SA-UserAccess

per slide 429
Scenario: Distributed Search
• Extract ITSI app package in etc/apps
• Copy SA-IndexCreation to the indexers
• Copy SA-ITSI-Licensechecker
and SA-UserAccess to the license master
• Restart Splunk on all servers
upvoted 1 times

Ash_111 8 months, 3 weeks ago

B - as per slide 429
Scenario: Distributed Search
• Extract ITSI app package in etc/apps
• Copy SA-IndexCreation to the indexers
• Copy SA-ITSI-Licensechecker
and SA-UserAccess to the license master
• Restart Splunk on all servers
upvoted 1 times

Manish7 1 year ago

Selected Answer: C

c is correct
upvoted 3 times

anwar_mian 1 year, 1 month ago

C should be right, since in a distributed or on one-server installation everything should go to the Search Head. In a distributed environment set indexAndForward = false.
upvoted 2 times

otb_282 1 year, 8 months ago

C - slide 117.
upvoted 4 times

Question #14 *Topic 1*

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 “Filter to Entities in Service”.

Suggested Answer: *D*

Community vote distribution

D (100%)

Manish7 1 year ago

Selected Answer: D

D is correct. B is partially correct as we do have service level entity filtrations available too.

upvoted 2 times

otb_282 1 year, 8 months ago

I think B + D.

upvoted 2 times

Question #15 *Topic 1*

Which of the following describes a realistic troubleshooting workflow in ITSI?

A. Correlation Search –> Deep Dive –> Notable Event

B. Service Analyzer –> Notable Event Review –> Deep Dive

C. Service Analyzer –> Aggregation Policy –> Deep Dive

D. Correlation search –> KPI –> Aggregation Policy

Suggested Answer: *A*

Community vote distribution

B (100%)

Manish7 1 year ago

Selected Answer: B

B is correct.

upvoted 3 times

M26051 1 year, 7 months ago

Think its B

upvoted 3 times

Question #16 *Topic 1*

Which of the following accurately describes base searches used for KPIs in a service?

A. Base searches can be used for multiple services.

B. A base search can only be used by its service and all dependent services.

C. All the metrics in a base search are used by one service.

D. All the KPIs in a service use the same base search.

Suggested Answer: *A*

Community vote distribution

A (100%)

Manish7 1 year ago

Selected Answer: A

A is corrcet.

upvoted 2 times

anwar_mian 1 year, 1 month ago

A is correct. Base search is meant for using it in multiple places. It is similar to base search for a dashboard where it can be applied to multiple panels.

upvoted 2 times

M26051 1 year, 7 months ago

A is correct

upvoted 3 times

Question #17 *Topic 1*

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.

Suggested Answer: *A*

M26051 1 year, 7 months ago

A is correct

upvoted 4 times

Question #18 *Topic 1*

ITSI Saved Search Scheduling is configured to use realtime_schedule = 0. Which statement is accurate about this configuration?

A. If this value is set to 0, the scheduler bases its determination of the next scheduled search execution time on the current time.

B. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time.

C. If this value is set to 0, the scheduler may skip scheduled execution periods.

D. If this value is set to 0, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range.

Suggested Answer: *B*

anwar_mian 1 year, 1 month ago

Answer is B.
https://docs.splunk.com/Documentation/Splunk/9.1.1/Admin/Savedsearchesconf
* When set to 'false', the scheduler determines the next scheduled search run
time based on the last run time for the search

upvoted 2 times

nosavotor 1 year, 1 month ago

Could someone help me confirm if this is correct

upvoted 1 times

Question #19 *Topic 1*

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 KPI.

Suggested Answer: *D*

Community vote distribution

D (100%)

Manish7 1 year ago

Selected Answer: D

D is correct.

upvoted 2 times

anwar_mian 1 year, 1 month ago

Answer is D.

https://docs.splunk.com/Documentation/ITSI/4.17.1/SI/KPIImportance

ITSI considers KPIs that have an importance value of 11 as a special case that represents a "minimum health indicator" for the service.

upvoted 2 times

nosavotor 1 year, 1 month ago

Friends could you please confirm this answer

upvoted 1 times

Question #20 *Topic 1*

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

Manish7 1 year ago

Selected Answer: A

A is correct,

upvoted 2 times

anwar_mian 1 year, 1 month ago

Answer should be A

https://docs.splunk.com/Documentation/ITSI/4.17.1/SI/AT

The adaptive thresholds automatically recalculate on a nightly basis so that changes in KPI behavior don't trigger false alerts.

upvoted 2 times

nosavotor 1 year, 1 month ago

I'm not sure about that

upvoted 1 times

Question #21 *Topic 1*

Which of the following applies when configuring time policies for KPI thresholds?

A. A person can only configure 24 policies, one for each hour of the day.

B. They are great if you expect normal behavior at 1:00 to be different than normal behavior at 5:00

C. If a person expects a KPI to change significantly through a cycle on a daily basis, don't use it.

D. It is possible for multiple time policies to overlap.

Suggested Answer: *D*

Community vote distribution

B (100%)

Manish7 1 year ago

Selected Answer: B

B is correct

upvoted 3 times

anwar_mian 1 year, 1 month ago

Answer B makes sense

https://docs.splunk.com/Documentation/ITSI/4.17.1/SI/AT

The adaptive thresholds automatically recalculate on a nightly basis so that changes in KPI behavior don't trigger false alerts.

upvoted 2 times

M26051 1 year, 7 months ago

I think B

upvoted 2 times

tomod1 1 year, 8 months ago

D is incorrect slide 233 states this

upvoted 2 times

otb_282 1 year, 8 months ago

I think B - slide 231.

upvoted 2 times

Question #22 *Topic 1*

What is the main purpose of the service analyzer?

A. Display a list of All Services and Entities.

B. Trigger external alerts based on threshold violations.

C. Allow Analysts to add comments to Alerts.

D. Monitor overall Service and KPI status.

Suggested Answer: *C*

Community vote distribution

D (100%)

Ash_111 8 months, 3 weeks ago

Selected Answer: D

D seems relevant

upvoted 2 times

Manish7 1 year ago

D is correct.

upvoted 2 times

otb_282 1 year, 8 months ago

D - slide 15.

upvoted 4 times

Question #23 *Topic 1*

What is the default importance value for dependent services' health scores?

A. 11

B. 1

C. Unassigned

D. 10

Suggested Answer: *A*

Community vote distribution

A (100%)

sunil343 8 months, 1 week ago

Selected Answer: A

11 is right answer

upvoted 2 times

SamKing 1 year ago

https://docs.splunk.com/Documentation/ITSI/4.17.1/SI/Dependencies#Set_importance_values_for_service_dependencies

upvoted 2 times

nosavotor 1 year, 1 month ago

I'm not sure about that

upvoted 1 times

Question #24 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

vhharan92 8 months, 2 weeks ago

B should be the correct one because the TA will the CIM normalized.

upvoted 2 times

Manish7 1 year ago

Selected Answer: B

B and C both seem correct and related but if it's a single correct option question just go with B.

upvoted 1 times

nosavotor 1 year, 1 month ago

Could someone help me confirm the correctness of this answer

upvoted 1 times

Question #25 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

C (100%)

Baba111222 10 months, 1 week ago

Selected Answer: C

Service Templates: Maintenance -> "KPIs can be added to child services in addition to the KPIs "inherited" from the template"

upvoted 1 times

otb_282 1 year, 8 months ago

C. New KPIs - slide 287.

upvoted 2 times

Question #26 *Topic 1*

Which of the following items describe ITSI Deep Dive capabilities? (Choose all that apply.)

A. Comparing a service's notable events over a time period.

B. Visualizing one or more Service KPIs values by time.

C. Examining and comparing alert levels for KPIs in a service over time.

D. Comparing swim lane values for a slice of time.

Suggested Answer: *BCD*

Community vote distribution

BCD (100%)

Manish7 1 year ago

Selected Answer: BCD

BCD is correct

upvoted 2 times

qtygbapjpesdayazko 1 year, 1 month ago

Im not sure how to respond to that

upvoted 1 times

nosavotor 1 year, 1 month ago

Is this answer accurate friends

upvoted 1 times