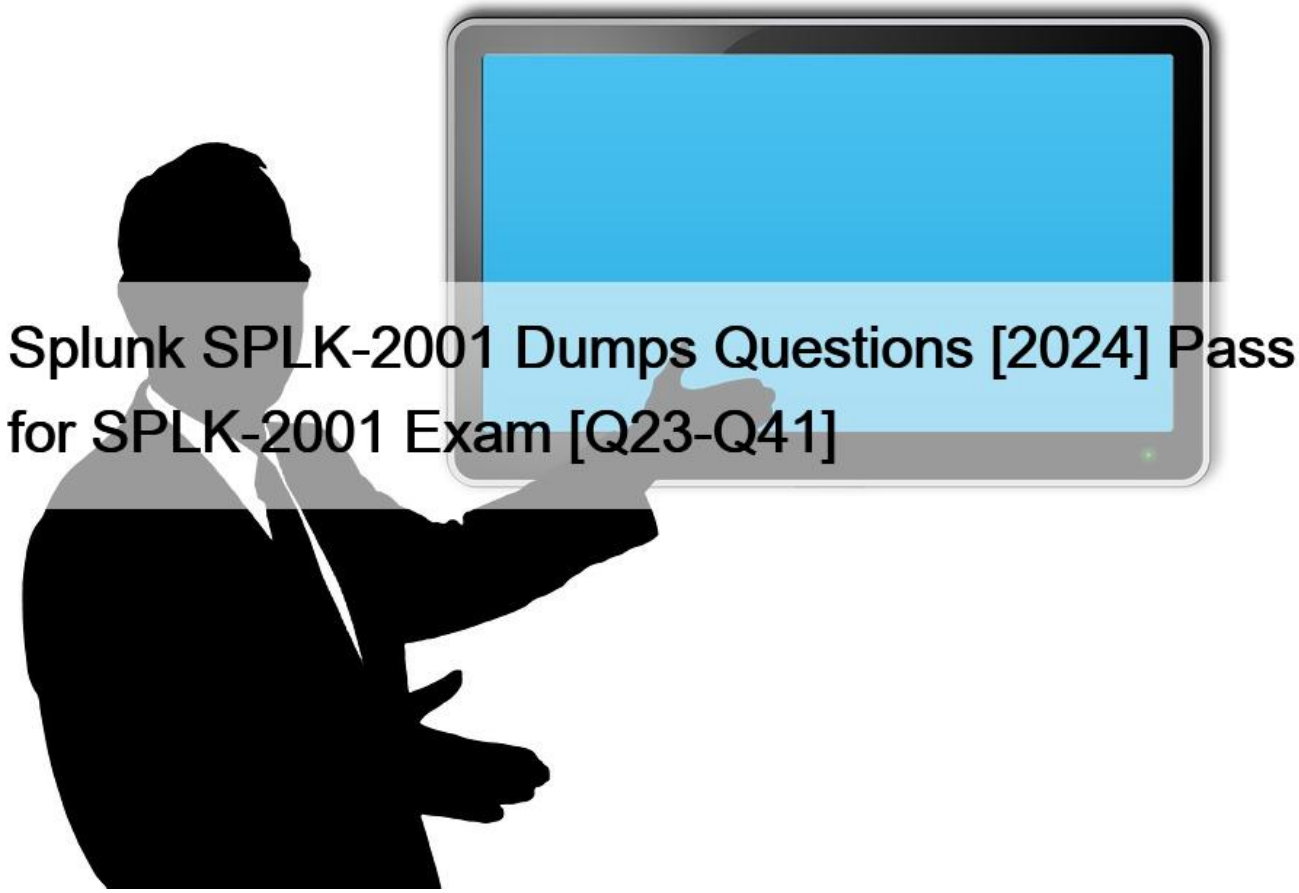
Splunk SPLK-2001 Dumps Questions [2024 Pass for SPLK-2001 Exam [Q23-Q41



Splunk SPLK-2001 Dumps Questions [2024] Pass for SPLK-2001 Exam
Updated Splunk Study Guide SPLK-2001 Dumps Questions

To succeed in the SPLK-2001 certification exam, you need to have a solid understanding of Splunk technology, including its architecture, data models, search processing language, and administrative tasks. SPLK-2001 exam also tests your ability to develop and deploy Splunk apps, work with Splunk data, and create dashboards and reports. With this certification, you can prove to potential employers that you have the skills to handle the most challenging Splunk development and deployment tasks.

Splunk SPLK-2001 certification is highly regarded in the IT industry and is recognized by many organizations as a valuable credential for developers working with Splunk technology. Earning this certification can help developers stand out in a competitive job market and open up new career opportunities.

QUESTION 23

Which of the following is an example of a valid syntax for specifying an absolute time range modifier in a search?
* earliest=01/01/2019:00:00:00
* earliest=01/01/2019T00:00:00
* earliest=2019-01-01 00:00:00
* earliest=2019-01-01T00:00:00

QUESTION 24

How can hiding or showing a panel by clicking on a chart or a table on the same form be performed?
* By using vent drilldown.
* By using workflow action.
* By using contextual drilldown.
* By using visualization drilldown.

QUESTION 25

Suppose the following query in a Simple XML dashboard returns a table including hyperlinks:

<search>

<query>index news sourcetype web_proxy | table sourcetype title link

</query>

</search>

Which of the following is a valid dynamic drilldown element to allow a user of the dashboard to visit the hyperlinks contained in the link field?
* <option name “link.openSearch.viewTarget”>$row.link$</option>
* <drilldown>

<link target=” blank”>$$row.link$$</link>

</drilldown>
* <drilldown>

<link target=”_blank”>$row.link|n$</link>

</drilldown>
* <drilldown>

<link target “_blank”>http://localhost:8000/debug/refresh</link>

</drilldown>

QUESTION 26

Which of the following are characteristics of an add-on? (Select all that apply.)
* Requires navigation file.

* Occupies a unique namespace within Splunk.
* Can depend on add-ons for correct operation.
* Contains technology or components not intended for reuse by other apps.

QUESTION 27

Which of the following is a customization option for the Open in Search panel link button?
* Display the refresh time.
* Show the Export Results button.
* Show link buttons at the bottom of a panel.
* Define an alternative search or target view to use.

QUESTION 28

A KV store collection can be associated with a namespace for which of the following users?
* Nobody
* Users in the admin role.
* Users in the admin and power roles.
* Users in the admin, power, and splunk-system-user roles.

QUESTION 29

How can event logs be collected from a remote Windows machine using a standard Splunk installation and no customization? (Select all that apply.)
* By configuring a WMI input.
* By using HTTP event collector.
* By using a Windows heavy forwarder.
* By using a Windows universal forwarder.

Explanation

The correct answer is A and D, because configuring a WMI input and using a Windows universal forwarder are the ways to collect event logs from a remote Windows machine using a standard Splunk installation and no customization. WMI input is a type of input that collects Windows Management Instrumentation (WMI) data from remote Windows machines. Windows universal forwarder is a lightweight version of Splunk that can forward data from Windows machines to Splunk indexers.

QUESTION 30

When added to an app’s default.meta file, which of the following makes one of its views available to other apps?
* export = app
* export = none
* export = view
* export = system

Explanation

When added to an app’s default.meta file, export = system makes one of its views available to other apps. This means that the view is visible and searchable by all users. The other options are invalid because export = app means that the view is visible and searchable only within the app, export = none means that the view is not visible or searchable by any user, and export = view is not a valid value for the export attribute. For more information, see About configuration file structure and inheritance.

QUESTION 31

What predefined drilldown tokens are available specifically for trellis layouts? (Select all that apply.)
* trellis.Xaxis
* trellis.Yaxis
* trellis.name
* trellis.value

QUESTION 32

When using the Splunk Web Framework to create a global search, which is the correct post-process syntax for the base search shown below?

var searchmain = new SearchManager{{ id: “base-search”,

search: “index= internal | head 10 | fields “*”, preview: true,

cache: true

}};
* var mypostproc1 = new PostProcessManager {{ id: “post1”,

managerid: “base-search”,

search: “| stats count by sourcetype”

}};
* var mypostproc1 = new PostProcessManager{{ id: “post1”,

managerid: “base”,

search: “| stats count by sourcetype”

}};
* var mypostproc1 = new PostProcess{{ id: “post1”,

managerid: “base-search”,

search: “| search stats count by sourcetype”

}};
* You cannot create global searches in the Splunk Web Framework.

QUESTION 33

Which of the following statements describe oneshot searches? (Select all that apply.)
* Are always executed asynchronously.
* Can specify csv as an output format.
* Stream all results upon search completion.
* Can use auto_cancel to set a timeout limit.

QUESTION 34

What predefined drilldown tokens are available specifically for trellis layouts? (Select all that apply.)
* trellis.Xaxis
* trellis.Yaxis
* trellis.name
* trellis.value
Explanation

The correct answer is C and D, because trellis.name and trellis.value are the predefined drilldown tokens available specifically for trellis layouts. Trellis layouts are a way of displaying multiple charts in a grid, each with a different value of a split-by field. The trellis.name token returns the name of the split-by field, and the trellis.value token returns the value of the split-by field for the selected chart.

QUESTION 35

After updating a dashboard in myApp, a Splunk admin moves myApp to a different Splunk instance. After logging in to the new instance, the dashboard is not seen. What could have happened? (Select all that apply.)
* The dashboard’s permissions were set to private.
* User role permissions are different on the new instance.
* The admin deleted the myApp/local directory before packaging.
* Changes were placed in $SPLUNK_HOME/etc./apps/search/default/data/ui/nav
Explanation

The correct answer is A, B, and C because these are the possible reasons why the dashboard is not seen after moving myApp to a different Splunk instance. Option A is correct because if the dashboard’s permissions were set to private, only the owner of the dashboard can see it on the new instance. Option B is correct because if the user role permissions are different on the new instance, the user may not have access to the dashboard.

Option C is correct because if the admin deleted the myApp/local directory before packaging, the dashboard configuration may have been lost. Option D is incorrect because changes placed in

$SPLUNK_HOME/etc/apps/search/default/data/ui/nav do not affect the visibility of the dashboard. You can find more information about dashboard permissions and configuration in the Splunk Developer Guide.

QUESTION 36

In order to successfully accelerate a report, which criteria must the search meet? (Select all that apply.)
* Cannot use event sampling.
* Use a transforming command.
* Use a standard Splunk visualization.
* Commands before the first transforming command must be streamable.
Explanation

The correct answer is A, B, and D because these are the criteria that the search must meet in order to successfully accelerate a report. A report is a saved search that runs on a schedule and returns results in a table or a chart. A report can be accelerated to improve its performance and reduce the load on the Splunk indexers.

Option A is correct because the search cannot use event sampling, which is a technique that reduces the number of events returned by the search. Event sampling can affect the accuracy and consistency of the report results. Option B is correct because the search

must use a transforming command, which is a command that converts the results into a data table with rows and columns. Transforming commands are required for report acceleration, as they enable the creation of summary data. Option D is correct because the commands before the first transforming command must be streamable, which means they can process each event as it is returned by the search. Streamable commands are preferred for report acceleration, as they reduce the memory usage and improve the performance of the search. Option C is incorrect because the search does not need to use a standard Splunk visualization, which is a type of chart or graph that displays the results. The search can use any visualization that is compatible with the report acceleration. You can find more information about report acceleration and the criteria for the search in the Splunk Developer Guide.

QUESTION 37

Which of the following Simple XML elements configure panel link buttons? (Select all that apply.)
* <title>Open In Search</title>
* <option name=”link.visible”>true</option>
* <option name=”trellis.enabled”>false</option>
* <option name=”refresh.link.visible”>false</option>

QUESTION 38

Which of the following is true of a namespace?
* The namespace is a type of token filter.
* The namespace includes an app attribute which cannot be a wildcard.
* The namespace filters the knowledge objects returned by the REST API.
* The namespace does not filter knowledge objects returned by the REST API.

QUESTION 39

Place content to set on page load inside which of the following Simple XML tags?
* <set></set>
* <eval></eval>
* <init></init>
* <value></value>

Explanation

The correct Simple XML tag to place content to set on page load is <init></init>. This tag lets you define tokens and their values that are set when the dashboard loads. The other tags are either invalid or used for different purposes. For more information, see Tokens.

QUESTION 40

Log files related to Splunk REST calls can be found in which indexes? (Select all that apply.)
* _audit
* _internal
* _thefishbucket
* _blocksignature

QUESTION 41

Which of the following are valid request arguments for the REST search endpoints? (Select all that apply.)
* latest_time=rt
* latest_time=now

* earliest_time=-5h@h
* earliest_time=rt_10m@m

Explanation

The valid request arguments for the REST search endpoints are latest_time=now and earliest_time=-5h@h.

These arguments specify the time range for the search, using relative or absolute time modifiers. The other arguments are invalid because they use rt (real-time) modifiers, which are not supported by the REST search endpoints. For more information, see [Specify time modifiers in your search].