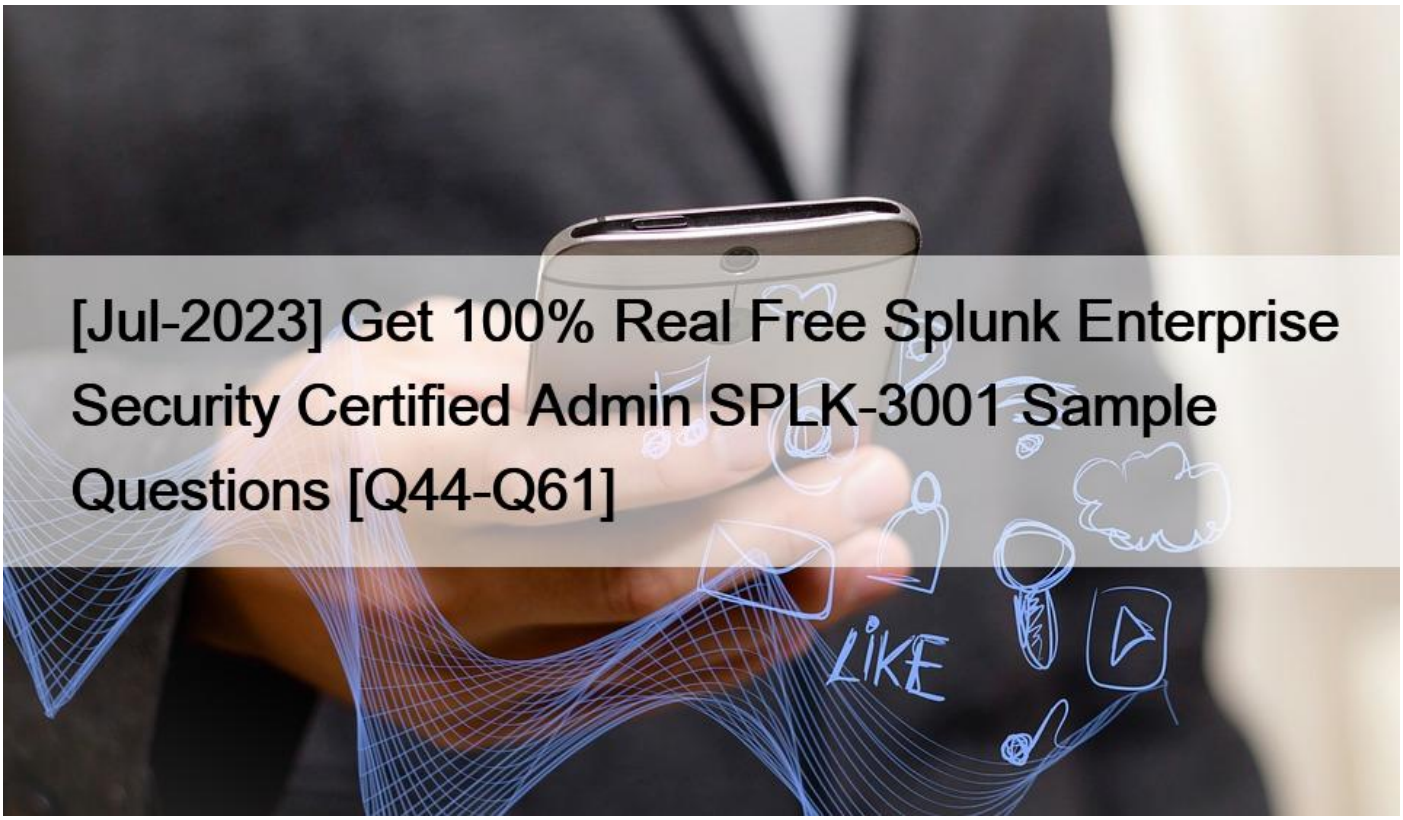
[Jul-2023 Get 100% Real Free Splunk Enterprise Security Certified Admin SPLK-3001 Sample Questions [Q44-Q61



[Jul-2023] Get 100% Real Free Splunk Enterprise Security Certified Admin SPLK-3001 Sample Questions
Accurate SPLK-3001 Questions with Free and Fast Updates

The exam consists of 60 multiple-choice questions and is timed at 90 minutes. Candidates are required to achieve a passing score of 70% or higher to earn their certification. The exam is available in English and can be taken online or at a proctored testing center.

There you can get information about the guide to Prepare the Splunk SPLK-3001 Exam

For prep work of Splunk SPLK-3001 Exam. Two significant kinds of resources originally there are the research study summaries in addition to publications that are specified as well as excellent for developing understanding from ground up after that there are video clip tutorials along with talks that can somehow minimize the pain of with research study and also are instead a lot much less degree for some leads yet these demand time in addition to concentration from the student. Smart Prospects that wish to produce a strong structure in all test subjects together with also associated contemporary technologies normally incorporate video clip talks with research study develops to revenue of both nevertheless there is one vital prep job tool as typically disregarded by a lot of leads the strategy Exams. No person such as insolvency, generally in complicated setups where accreditation needs a large quantity of study, prep work, and also an interest. An initiative is so demanding that it can even break students' nerves. Our download examinations are so effective that you will definitely fail to remember the failings. Problems and additionally remedies are so preferably established that there is no opportunity of failing. Nevertheless, there is little scenario where the student has truly quit operating after acquiring our help, nevertheless, even if they do, we provide a full reimbursement of the settlement. Method Exams are constructed to make pupils comfy with genuine Examination circumstances. If we see the statistics most students fail not as a result of that preparation

task yet because of take a look at anxiousness the problem of the unknown. Dumpleader expert team recommends you to prepare some notes on these subjects along with it do not forget to exercise Splunk **SPLK-3001 Dump** which had in reality been made up by our Professionals Group, Both these will aid you a bargain to eliminate this test with excellent marks.

QUESTION 44

In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?
* Save the settings.
* Apply the correct tags.
* Run the correct search.
* Visit the CIM dashboard.

Reference:

https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata

QUESTION 45

Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?
* SplunkWeb (8000), Splunk Management (8089), KV Store (8191)
* SplunkWeb (8068), Splunk Management (8089), KV Store (8000)
* SplunkWeb (8390), Splunk Management (8323), KV Store (8672)
* SplunkWeb (8043), Splunk Management (8088), KV Store (8191)

https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

QUESTION 46

The option to create a Short ID for a notable event is located where?
* The Additional Fields.
* The Event Details.
* The Contributing Events.
* The Description.

Explanation

https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

QUESTION 47

What can be exported from ES using the Content Management page?
* Only correlation searches, managed lookups, and glass tables.
* Only correlation searches.
* Any content type listed in the Content Management page.
* Only correlation searches, glass tables, and workbench panels.

QUESTION 48

Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?
* Lookup searches.
* Summarized data.
* Security metrics.

* Metrics store searches.

Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable

QUESTION 49

ES apps and add-ons from $SPLUNK_HOME/etc/apps should be copied from the staging instance to what location on the cluster deployer instance?

* $SPLUNK_HOME/etc/master-apps/
* $SPLUNK_HOME/etc/system/local/
* $SPLUNK_HOME/etc/shcluster/apps
* $SPLUNK_HOME/var/run/searchpeers/

Explanation

The upgraded contents of the staging instance will be migrated back to the deployer and deployed to the search head cluster members. On the staging instance, copy $SPLUNK_HOME/etc/apps to

$SPLUNK_HOME/etc/shcluster/apps on the deployer. 1. On the deployer, remove any deprecated apps or add-ons in $SPLUNK_HOME/etc/shcluster/apps that were removed during the upgrade on staging. Confirm by reviewing the ES upgrade report generated on staging, or by examining the apps moved into

$SPLUNK_HOME/etc/disabled-apps on staging

QUESTION 50

Following the Installation of ES, an admin configured Leers with the ss_uso r role the ability to close notable events. How would the admin restrict these users from being able to change the status of Resolved notable events to closed?

* From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the closed status.
* From the Status Configuration windows select the closed status. Remove ess_use r from the status transitions for the Resolved status.
* In Enterprise Security, give the ess_user role the own Notable Events permission.
* From Splunk Access Controls, select the ess_user role and remove the edit_notabie_events capability.

QUESTION 51

Which component normalizes events?

* SA-CIM.
* SA-Notable.
* ES application.
* Technology add-on.

Reference:

https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

QUESTION 52

Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?

* SplunkWeb (8068), Splunk Management (8089), KV Store (8000)

* SplunkWeb (8390), Splunk Management (8323), KV Store (8672)
* SplunkWeb (8000), Splunk Management (8089), KV Store (8191)
* SplunkWeb (8043), Splunk Management (8088), KV Store (8191)

QUESTION 53

In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?
* Save the settings.
* Apply the correct tags.
* Run the correct search.
* Visit the CIM dashboard.

QUESTION 54

A newly built custom dashboard needs to be available to a team of security analysts In ES. How is It possible to Integrate the new dashboard?
* Add links on the ES home page to the new dashboard.
* Create a new role Inherited from es_analyst, make the dashboard permissions read-only, and make this dashboard the default view for the new role.
* Set the dashboard permissions to allow access by es_analysts and use the navigation editor to add it to the menu.
* Add the dashboard to a custom add-in app and install it to ES using the Content Manager.

QUESTION 55

To observe what network services are in use in a network’s activity overall, which of the following dashboards in Enterprise Security will contain the most relevant data?
* Intrusion Center
* Protocol Analysis
* User Intelligence
* Threat Intelligence

Explanation

QUESTION 56

Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?
* Security domains.
* Threat intel.
* Assets.
* Domains.

QUESTION 57

A site has a single existing search head which hosts a mix of both CIM and non-CIM compliant applications. All of the applications are mission-critical. The customer wants to carefully control cost, but wants good ES performance. What is the best practice for installing ES?
* Install ES on the existing search head.
* Add a new search head and install ES on it.
* Increase the number of CPUs and amount of memory on the search head, then install ES.
* Delete the non-CIM-compliant apps from the search head, then install ES.

Reference:

https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

QUESTION 58

How is it possible to navigate to the list of currently-enabled ES correlation searches?
* Configure -> Correlation Searches -> Select Status “Enabled”
* Settings -> Searches, Reports, and Alerts -> Filter by Name of “Correlation”
* Configure -> Content Management -> Select Type “Correlation” and Status “Enabled”
* Settings -> Searches, Reports, and Alerts -> Select App of “SplunkEnterpriseSecuritySuite” and filter by “-Rule”

QUESTION 59

When creating custom correlation searches, what format is used to embed field values in the title, description, and drill-down fields of a notable event?
* $fieldname$
* “fieldname”
* %fieldname%
* _fieldname_

QUESTION 60

Accelerated data requires approximately how many times the daily data volume of additional storage space per year?
* 3.4
* 5.7
* 1.0
* 2.5

QUESTION 61

Where is the Add-On Builder available from?
* GitHub
* SplunkBase
* www.splunk.com
* The ES installation package

Reference:

https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

Splunk SPLK-3001 Exam Syllabus Topics:

Topic	Details
1	- Use the Add-on Builder to Build a New add-on- Tuning Correlation Searches- Configure Correlation Search Scheduling and Sensitivity
2	- Examine the Deployment Checklist- Understand Indexing Strategy for ES- Understand ES Data Models- Installation and Configuration
3	- Notable Events Management- Investigations, Security Intelligence- Overview of Security Intel Tools- Forensics, Glass Tables, and Navigation Control
4	- Post-Install Configuration Tasks- Validating ES Data- Plan ES Inputs- Configure Technology add-ons- Design a New add-on for Custom Data
5	- Prepare a Splunk Environment for Installation- Download and Install ES on a Search Head- Understand ES Splunk User Accounts and Roles
6	- Tune ES Correlation Searches- Creating Correlation Searches- Create a Custom Correlation Search- Configuring Adaptive Responses- Search Export- Import
7	- Explore Forensics Dashboards- Examine Glass Tables- Configure Navigation and Dashboard Permissions- Identify Deployment Topologies
8	- Threat Intelligence Framework- Understand and Configure Threat Intelligence- Configure User Activity Analysis

SPLK-3001 Study Guide Realistic Verified Dumps: https://www.dumpleader.com/SPLK-3001_exam.html]