[Q25-Q43 Get Special Discount Offer on SPLK-3001 Dumps PDF [UPDATED Jul-2022

Get Special Discount Offer on SPLK-3001 Dumps PDF [UPDATED Jul-2022]
PDF Download Splunk Test To Gain Brilliante Result!

What are the preparation guide for the Splunk SPLK-3001 Certification **Best preparation guide For Splunk SPLK-3001 Certification Check out Splunk SPLK-3001 Certification**

A Splunk SPLK-3001 certification will undoubtedly help you jumpstart your career. In this article, we will talk about the importance of a Splunk SPLK-3001 and how it can take your career to the next level. The SPLK-3001 Certification is one of the few certifications for data engineers that bridges the gap between database administrators and software engineers. With this certification, you'll learn how to design and set up software architectures along with the specific skills required as a database administrator. If a candidate has knowledge and skills that are required to pass Splunk SPLK-3001 Exam and fully prepared with **Splunk SPLK-3001 Dumps** then he should take this Splunk SPLK-3001 exam. You'll also understand how to integrate technologies like Hadoop, Splunk Hunk, and Storm.

What is the registration procedure Splunk SPLK-3001 Certification exam

Here is a list of steps that are required to register for the SPLK-3001 certification exam:

- Register on ExamMerchant.- Make sure you have an active Splunk account.- Log in to your ExamMerchant account and navigate to the ?Splunk? section under ?Search for Exams?.- Search for the certification by filling in ?Splunk SPLK-3001?.

Then click on ?Get Now?.- Click on ?Register for Exam? to register for the SPLK-3001 exam.- Enter your information like name, billing address, contact number, and other details, then click on ?Register?.- A confirmation email will be sent to your registered email ID within 24 hours of registration.- Your certification status will be available in the next 24-48 hours after your registration is complete.- Verify the SPLK-3001 exam details in order to proceed to the next step.- Purchase the exam through your ExamMerchant account.- After you purchase, complete the transaction on ExamMerchant and follow the instructions to download your exam. Attach the SPLK-3001 certificate and Splunk login details on it for verification.- Take a print of your SPLK-3001 certificate and keep it safe for future uses. **QUESTION 25**

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 26

Which indexes are searched by default for CIM data models?
* notable and default
* summary and notable
* _internal and summary
* All indexes

Reference:

https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

QUESTION 27

When ES content is exported, an app with a .spl extension is automatically created. What is the best practice when exporting and importing updates to ES content?
* Use new app names each time content is exported.
* Do not use the .spl extension when naming an export.
* Always include existing and new content for each export.
* Either use new app names or always include both existing and new content.

QUESTION 28

Which of the following are examples of sources for events in the endpoint security domain dashboards?
* Investigation final results status.
* Workstations, notebooks, and point-of-sale systems.
* REST API invocations.
* Lifecycle auditing of incidents, from assignment to resolution.

QUESTION 29

To which of the following should the ES application be uploaded?
* The indexer.
* The KV Store.
* The search head.
* The dedicated forwarder.

Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecuritySHC

QUESTION 30

Which of the following threat intelligence types can ES download? (Choose all that apply)
* Text
* STIX/TAXII
* VulnScanSPL
* SplunkEnterpriseThreatGenerator

Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Downloadthreatfeed

QUESTION 31

Which data model populates the panels on the Risk Analysis dashboard?
* Risk
* Audit
* Domain analysis
* Threat intelligence

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

QUESTION 32

Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?
* A prefix of CIM_
* A suffix of .spl
* A prefix of TECH_
* A prefix of Splunk_TA_

QUESTION 33

Which of the following ES features would a security analyst use while investigating a network anomaly notable?
* Correlation editor.
* Key indicator search.
* Threat download dashboard.
* Protocol intelligence dashboard.

QUESTION 34

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 35

Which of the following is a risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf?
* Indexes might crash.
* Indexes might be processing.
* Indexes might not be reachable.
* Indexes have different settings.

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf

QUESTION 36

Which correlation search feature is used to throttle the creation of notable events?
* Schedule priority.
* Window interval.
* Window duration.
* Schedule windows.

QUESTION 37

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 38

An administrator is provisioning one search head prior to installing ES. What are the reference minimum requirements for OS, CPU, and RAM for that machine?
* OS: 32 bit, RAM: 16 MB, CPU: 12 cores
* OS: 64 bit, RAM: 32 MB, CPU: 12 cores
* OS: 64 bit, RAM: 12 MB, CPU: 16 cores
* OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware

QUESTION 39

The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of data.

What data model should be checked for potential errors such as skipped searches?
* Web
* Risk
* Performance
* Authentication

Explanation/Reference: https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html

QUESTION 40

What does the risk framework add to an object (user, server or other type) to indicate increased risk?
* An urgency.
* A risk profile.
* An aggregation.
* A numeric score.

Reference:

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

QUESTION 41

When ES content is exported, an app with a .splextension is automatically created.

What is the best practice when exporting and importing updates to ES content?
* Use new app names each time content is exported.
* Do not use the .splextension when naming an export.
* Always include existing and new content for each export.
* Either use new app names or always include both existing and new content.

QUESTION 42

Which of the following are examples of sources for events in the endpoint security domain dashboards?
* REST API invocations.
* Investigation final results status.
* Workstations, notebooks, and point-of-sale systems.
* Lifecycle auditing of incidents, from assignment to resolution.

Explanation/Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

QUESTION 43

Adaptive response action history is stored in which index?
* cim_modactions
* modular_history
* cim_adaptiveactions
* modular_action_history

SPLK-3001 Dumps are Available for Instant Access: https://www.dumpsmaterials.com/SPLK-3001-real-torrent.html]