SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-3001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which tool Is used to update indexers In E5?

A. Index Updater

B. Distributed Configuration Management

C. indexes.conf

D. Splunk_TA_ForIndexeres. spl

Correct Answer: B

QUESTION 2

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?

A. $SPLUNK_HOME/etc/master-apps/

B. $SPLUNK_HOME/etc/system/local/

C. $SPLUNK_HOME/etc/shcluster/apps

D. $SPLUNK_HOME/var/run/searchpeers/

Correct Answer: C

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 3

Which component normalizes events?

A. SA-CIM.

B. SA-Notable.

C. ES application.

D. Technology add-on.

Correct Answer: A

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

QUESTION 4

Which data model populated the panels on the Risk Analysis dashboard?

A. Risk

B. Audit

C. Domain analysis

D. Threat intelligence

Correct Answer: A

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

QUESTION 5

Following the installation of ES, an admin configured users with the ess_user 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?

A. In Enterprise Security, give the ess_user role the Own Notable Events permission.

B. From the Status Configuration window select the Closed status. Remove ess_user from the status transitions for the Resolved status.

C. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the Closed status.

D. From Splunk Access Controls, select the ess_user role and remove the edit_notable_events capability.

Correct Answer: C

QUESTION 6

Who can delete an investigation?

A. ess_admin users only.

B. The investigation owner only.

C. The investigation owner and ess-admin.

D. The investigation owner and collaborators.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

QUESTION 7

The Add-On Builder creates Splunk Apps that start with what?

A. DA

B. SA

C. TA

D. App-

Correct Answer: C

Reference: https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/

QUESTION 8

Which of the following is a risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf?

A. Indexes might crash.

B. Indexes might be processing.

C. Indexes might not be reachable.

D. Indexes have different settings.

Correct Answer: A

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

QUESTION 9

Where is it possible to export content, such as correlation searches, from ES?

A. Content exporter

B. Configure -> Content Management

C. Export content dashboard

D. Settings Menu -> ES -> Export

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

QUESTION 10

Analysts have requested the ability to capture and analyze network traffic data. The administrator has researched the documentation and, based on this research, has decided to integrate the Splunk App for Stream with ES.

Which dashboards will now be supported so analysts can view and analyze network Stream data?

A. Endpoint dashboards.

B. User Intelligence dashboards.

C. Protocol Intelligence dashboards.

D. Web Intelligence dashboards.

Correct Answer: C

QUESTION 11

What is the bar across the bottom of any ES window?

A. The Investigator Workbench.

B. The Investigation Bar.

C. The Analyst Bar.

D. The Compliance Bar.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/User/Startaninvestigation

QUESTION 12

After installing Enterprise Security, the distributed configuration management tool can be used to create which app to configure indexers?

A. Splunk_DS_ForIndexers.spl

B. Splunk_ES_ForIndexers.spl

C. Splunk_SA_ForIndexers.spl

D. Splunk_TA_ForIndexers.spl

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

QUESTION 13

What is the default schedule for accelerating ES Datamodels?

A. 1 minute

B. 5 minutes

C. 15 minutes

D. 1 hour

Correct Answer: B

QUESTION 14

What can be exported from ES using the Content Management page?

A. Only correlation searches, managed lookups, and glass tables.

B. Only correlation searches.

C. Any content type listed in the Content Management page.

D. Only correlation searches, glass tables, and workbench panels.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Export#:~:text=as%20an%20app-,Export%20content%20from%20Splunk%20Enterprise%20Security%20as,from%20the%20Conte nt%20Management%20page.andtext=You%20can%20export%20any%20type,%2C%20data%20models%2C%20and%20views.

QUESTION 15

Which settings indicated that the correlation search will be executed as new events are indexed?

A. Always-On

B. Real-Time

C. Scheduled

D. Continuous

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches