SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

QUESTION 1

How should an administrator add a new lookup through the ES app?

A. Upload the lookup file in Settings -> Lookups -> Lookup Definitions

B. Upload the lookup file in Settings -> Lookups -> Lookup table files

C. Add the lookup file to /etc/apps/SplunkEnterpriseSecuritySuite/lookups

D. Upload the lookup file using Configure -> Content Management -> Create New Content -> Managed Lookup

Correct Answer: D

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

QUESTION 2

How does ES know local customer domain names so it can detect internal vs. external emails?

A. Web and email domain names are set in General -> General Configuration.

B. ES uses the User Activity index and applies machine learning to determine internal and external domains.

C. The Corporate Web and Email Domain Lookups are edited during initial configuration.

D. ES extracts local email and web domains automatically from SMTP and HTTP logs.

Correct Answer: C

QUESTION 3

Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?

A. Security domains.

B. Threat intel.

C. Assets.

D. Domains.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Manageinternallookups

QUESTION 4

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 5

ES needs to be installed on a search head with which of the following options?

A. No other apps.

B. Any other apps installed.

C. All apps removed except for TA-*.

D. Only default built-in and CIM-compliant apps.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecurity