SPLK-3001.VCEplus.premium.exam.60q

Number: SPLK-3001
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

SPLK-3001

Splunk Enterprise Security Certified Admin

Version 1.0

Exam A

QUESTION 1

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

A. DA-
B. SA-
C. TA-D. App-

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 2 Which of the following are examples of sources for events in the endpoint security domain dashboards?

A. REST API invocations.
B. Investigation final results status.
C. Workstations, notebooks, and point-of-sale systems.
D. Lifecycle auditing of incidents, from assignment to resolution.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 3
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?

A. `$fieldname$`
B. `"fieldname"`
C. `%fieldname%`
D. `_fieldname_`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

QUESTION 4 What feature of Enterprise Security downloads threat intelligence data from a web server?

A. Threat Service Manager
B. Threat Download Manager
C. Threat Intelligence Parser
D. Therat Intelligence Enforcement

Correct Answer: B
Section: (none)

Explanation
Explanation/Reference:

QUESTION 5 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?

A. Web
B. Risk
C. Performance
D. Authentication

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 6 In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?

A. Save the settings.
B. Apply the correct tags.
C. Run the correct search.
D. Visit the CIM dashboard.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 7
What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?

A. ess_user
B. ess_admin
C. ess_analyst
D. ess_reviewer

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 8 Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?

A. VIP
B. Priority
C. Importance
D. Criticality

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 9 What does the risk framework add to an object (user, server or other type) to indicate increased risk?

A. An urgency.
B. A risk profile.
C. An aggregation.
D. A numeric score.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 10 Which indexes are searched by default for CIM data models?

A. `notable` and `default`
B. `summary` and `notable`
C. `_internal` and `summary`
D. All indexes

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 11 Which setting is used in `indexes.conf` to specify alternate locations for accelerated storage?

A. `thawedPath`
B. `tstatsHomePath`
C. `summaryHomePath`
D. `warmToColdScript`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

QUESTION 12 Which of the following is a way to test for a property normalized data model?

A. Use Audit -> Normalization Audit and check the Errors panel.

B. Run a `| datamodel` search, compare results to the CIM documentation for the datamodel.
C. Run a `| loadjob` search, look at tag values and compare them to known tags based on the encoding.
D. Run a `| datamodel` search and compare the results to the list of data models in the ES normalization guide.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 13
Which argument to the `| tstats` command restricts the search to summarized data only?

A. `summaries=t`
B. `summaries=all`
C. `summariesonly=t`
D. `summariesonly=all`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

QUESTION 14 When investigating, what is the best way to store a newly-found IOC?

A. Paste it into Notepad.
B. Click the “Add IOC” button.
C. Click the “Add Artifact” button.
D. Add it in a text note to the investigation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15 How is it possible to navigate to the list of currently-enabled ES correlation searches?

A. Configure -> Correlation Searches -> Select Status “Enabled”
B. Settings -> Searches, Reports, and Alerts -> Filter by Name of “Correlation”
C. Configure -> Content Management -> Select Type “Correlation” and Status “Enabled”
D. Settings -> Searches, Reports, and Alerts -> Select App of “SplunkEnterpriseSecuritySuite” and filter by “-Rule”

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 16 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
Section: (none)
Explanation

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

QUESTION 17 Which of the following are data models used by ES?
(Choose all that apply)

A. Web
B. Anomalies
C. Authentication
D. Network Traffic

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 18 At what point in the ES installation process should `Splunk_TA_ForIndexes.spl` be deployed to the indexers?

A. When adding apps to the deployment server.
B. `Splunk_TA_ForIndexers.spl` is installed first.
C. After installing ES on the search head(s) and running the distributed configuration management tool.
D. `Splunk_TA_ForIndexers.spl` is only installed on indexer cluster sites using the cluster master and the `splunk apply cluster-bundle` command.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 19 Which correlation search feature is used to throttle the creation of notable events?

A. Schedule priority.
B. Window interval.
C. Window duration.
D. Schedule windows.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 20
Both “Recommended Actions” and “Adaptive Response Actions” use adaptive response. How do they differ?

A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
D. Recommended Actions show a list of Adaptive Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

QUESTION 21 What does the Security Posture dashboard display?

A. Active investigations and their status.
B. A high-level overview of notable events.
C. Current threats being tracked by the SOC.
D. A display of the status of security tools.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Security Posture dashboard is designed to provide high-level insight into the notable events across all domains of your deployment, suitable for display in a Security Operations Center (SOC). This dashboard shows all events from the past 24 hours, along with the trends over the past 24 hours, and provides real-time event information and updates.

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

QUESTION 22 “10.22.63.159”, “websvr4”, and “00:26:08:18: CF:1D” would be matched against what in ES?

A. A user.
B. A device.
C. An asset.
D. An identity.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups

QUESTION 24
Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?

A. Lookup searches.
B. Summarized data.
C. Security metrics.
D. Metrics store searches.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 25 Which of the following is a key feature
of a glass table?

A. Rigidity.
B. Customization.
C. Interactive investigations.
D. Strong data for later retrieval.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
An administrator is asked to configure an “Nslookup” adaptive response action, so that it appears as a selectable option in the notable event’s action menu when an analyst is working in the Incident Review dashboard. What steps would the administrator take to configure this option?

A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup
B. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?

A. Configure -> Incident Management -> Notable Event Statuses

B. Configure -> Content Management -> Type: Correlation Search
C. Configure -> Incident Management -> Incident Review Settings -> Event ManagementD. Configure -> Incident Management -> Incident Review Settings -> Table Attributes

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 28
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?

A. Intrusion Center
B. Protocol Analysis
C. User Intelligence
D. Threat Intelligence

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 29 Adaptive response action history is stored
in which index?

A. `cim_modactions`
B. `modular_history`
C. `cim_adaptiveactions`
D. `modular_action_history`

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 30 Which of the following actions would not reduce the number of false positives from a correlation search?

A. Reducing the severity.
B. Removing throttling fields.
C. Increasing the throttling window.
D. Increasing threshold sensitivity.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 Where is the Add-On Builder
available from?

A. GitHub
B. SplunkBase
C. www.splunk.com
D. The ES installation package

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 32
Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?

A. A prefix of `CIM_`
B. A suffix of `.spl`
C. A prefix of `TECH_`
D. A prefix of `Splunk_TA_`

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 33
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
Section: (none)
Explanation

Explanation/Reference:
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 34 How is notable event
urgency calculated?

A. Asset priority and threat weight.
B. Alert severity found by the correlation search.
C. Asset or identity risk and severity found by the correlation search.
D. Severity set by the correlation search and priority assigned to the associated asset or identity.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 35
What kind of value is in the red box in this picture?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

A. A risk score.
B. A source ranking.
C. An event priority.
D. An IP address rating.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector

QUESTION 36 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
Section: (none)
Explanation

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

QUESTION 37 Which of the following threat intelligence types can ES download? (Choose all that apply)

A. Text
B. STIX/TAXII
C. VulnScanSPL
D. SplunkEnterpriseThreatGenerator

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 38
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?

A. Install ES on the existing search head.
B. Add a new search head and install ES on it.
C. Increase the number of CPUs and amount of memory on the search head, then install ES.
D. Delete the non-CIM-compliant apps from the search head, then install ES.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 39 Enterprise Security's dashboards primarily pull data from what type of knowledge object?

A. Tstats
B. KV Store
C. Data models
D. Dynamic lookups

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Splexicon:Knowledgeobject

QUESTION 40 To which of the following should the ES application be uploaded?

A. The indexer.
B. The KV Store.
C. The search head.
D. The dedicated forwarder.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 41 If a username does not match the 'identity' column in the identities list, which column is checked next?

A. Email.
B. Nickname
C. IP address.
D. Combination of Last Name, First Name.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 42 Which of the following features can the Add-on Builder configure in a new add-on?

A. Expire data.
B. Normalize data.
C. Summarize data.
D. Translate data.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

QUESTION 43 What is the maximum recommended volume of indexing per day, per indexer, for a non-cloud (on-prem) ES deployment?

A. 50 GB
B. 100 GB
C. 300 GBD. 500 MB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

QUESTION 44 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: A
Section: (none)
Explanation

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

QUESTION 45 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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

QUESTION 46 Where are attachments to investigations stored?

A. KV Store
B. `notable` index
C. `attachments.csv` lookup
D. `<splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments`

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 47 Which data model populated the panels on the Risk Analysis dashboard?

A. Risk
B. Audit
C. Domain analysis
D. Threat intelligence

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 48 How is it possible to navigate to the ES graphical Navigation Bar editor?

A. Configure -> Navigation Menu
B. Configure -> General -> Navigation
C. Settings -> User Interface -> Navigation -> Click on “Enterprise Security”
D. Settings -> User Interface -> Navigation Menus -> Click on “default” next to SplunkEnterpriseSecuritySuite

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

QUESTION 49
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?

A. OS: 32 bit, RAM: 16 MB, CPU: 12 cores B.
OS: 64 bit, RAM: 32 MB, CPU: 12 cores C.
OS: 64 bit, RAM: 12 MB, CPU: 16 cores

D. OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 50 What tools does the Risk Analysis dashboard provide?

A. High risk threats.
B. Notable event domains displayed by risk score.
C. A display of the highest risk assets and identities.
D. Key indicators showing the highest probability correlation searches in the environment.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 51
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?

A. Use new app names each time content is exported.
B. Do not use the `.spl` extension when naming an export.
C. Always include existing and new content for each export.
D. Either use new app names or always include both existing and new content.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52 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
Section: (none)
Explanation

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

QUESTION 53
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
Section: (none)
Explanation

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

QUESTION 54
The Brute Force Access Behavior Detected correlation search is enabled, and is generating many false positives. Assuming the input data has already been validated. How can the correlation search be made less sensitive?

A. Edit the search and modify the notable event status field to make the notable events less urgent.
B. Edit the search, look for where or xswhere statements, and after the threshold value being compared to make it less common match.
C. Edit the search, look for where or xswhere statements, and alter the threshold value being compared to make it a more common match.
D. Modify the urgency table for this correlation search and add a new severity level to make notable events from this search less urgent.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 55 Which of the following actions can improve overall search performance?

A. Disable indexed real-time search.
B. Increase priority of all correlation searches.
C. Reduce the frequency (schedule) of lower-priority correlation searches.
D. Add notable event suppressions for correlation searches with high numbers of false positives.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following ES features would a security analyst use while investigating a network anomaly notable?

A. Correlation editor.
B. Key indicator search.
C. Threat download dashboard.
D. Protocol intelligence dashboard.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

QUESTION 57

Which component normalizes events?

A. SA-CIM.
B. SA-Notable.
C. ES application.
D. Technology add-on.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 58
An administrator wants to ensure that none of the ES indexed data could be compromised through tampering. What feature would satisfy this requirement?

A. Index consistency.
B. Data integrity control.
C. Indexer acknowledgement.
D. Index access permissions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html

QUESTION 59 What is the first step when preparing to install ES?

A. Install ES.
B. Determine the data sources used.C. Determine the hardware required.
D. Determine the size and scope of installation.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 What is the default schedule for accelerating ES Datamodels?

A. 1 minute
B. 5 minutes
C. 15 minutes
D. 1 hour

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels