DUMPSARENA

Intel Security Certified Product Specialist

McAfee MA0-104

Version Demo

Total Demo Questions: 9

Total Premium Questions: 92

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

One or more storage allocations, which together specify a total amount of storage, coupled with a data retention time that specifies the maximum number of days a log is to be stored, is known as a

A. Storage Volume.

B. Storage Pool.

C. Storage Device.

D. Storage Area Network (SAN).

ANSWER: B

Explanation:

Storage Pool. is correct because, in McAfee Enterprise Security Manager terminology, a storage pool is the logical retention configuration that combines one or more underlying storage allocations into a defined capacity for event and log data. The pool also includes the retention period, expressed as the maximum number of days records are retained. These two settings work together: allocated capacity establishes how much data can be held, while the retention setting defines the intended lifecycle for that data. As new events arrive, the SIEM uses the configured pool and its retention policy to manage stored log data in accordance with available capacity and the organization's operational, investigative, and compliance requirements. This logical construct lets administrators organize storage and retention independently of the physical disk infrastructure, while providing a clear target for data collection and long-term log preservation. Storage planning is a core aspect of SIEM deployment because event volume, retention requirements, and available capacity directly affect historical search and forensic investigation capabilities. See the Trellix Enterprise Security Manager product information and Trellix Support for product documentation and administration resources.

QUESTION NO: 2

Analysts can effectively use the McAfee SIEM to identify threats by ?

A. focusing on aggregated and correlated events data.

B. disabling aggregation, so all data are visible.

C. studying ELM archives, to analyze the original data

D. use the streaming event viewer to analyze data.

ANSWER: A

Explanation:

Focusing on aggregated and correlated events data is correct because McAfee SIEM is designed to turn high-volume security telemetry into actionable security intelligence. Individual logs often lack sufficient context to establish whether an activity is benign or malicious. Aggregation groups similar events and reduces noise, allowing analysts to identify meaningful patterns across large data sets. Correlation then connects related activity from different sources, such as endpoint, network, authentication, and security-device events, to reveal attack sequences and indicators that would be difficult to recognize from isolated records. This prioritization enables analysts to investigate incidents based on their risk, context, and relationship to other observed activity rather than manually reviewing every raw event. McAfee Enterprise Security Manager provides correlation, alarms, dashboards, and investigative views for this purpose, helping a security operations team detect and respond to threats efficiently. This approach also aligns with log-management guidance that emphasizes centralized analysis and correlation of events to support incident identification and response. See the McAfee Enterprise Security Manager product information and NIST's Guide to Computer Security Log Management.

QUESTION NO: 3

Which of the following is the minimum number of CPUs required to build a virtual image Enterprise Security Manager (ESM)?

A. Two units

B. Four units

C. Six units

D. Eight units

ANSWER: D

Explanation:

Eight units is the minimum CPU allocation required for a virtual Enterprise Security Manager (ESM) image. ESM is the central analytics and correlation component of the McAfee Enterprise Security Manager SIEM platform. It must ingest and normalize event data, execute correlation rules, maintain searchable event information, and support the management interface. Those concurrent workloads require a substantial baseline of processing capacity even in a small deployment. Allocating eight virtual CPUs ensures that the virtual appliance meets the documented minimum platform sizing baseline rather than merely having enough resources to boot. CPU allocation is only one part of virtual ESM planning; administrators should also provision the required memory, storage capacity and performance, and supported hypervisor configuration. Actual resource needs can increase significantly with event rate, retention requirements, correlation content, reporting, and the number of connected data sources. For the applicable ESM release, always validate sizing and virtual-platform prerequisites in the product documentation before deployment. Current Enterprise Security Manager product information is available from Trellix Enterprise Security Manager, and product documentation can be accessed through the Trellix Documentation portal.

QUESTION NO: 4

In the Default Summary view on the Enterprise Security manager (ESM). which of the following panels shows the baseline averages?

A. Event Summary

B. Normalized Event Summary

C. Event Distribution

D. Baseline Average

ANSWER: C

Explanation:

Event Distribution is correct. In the Enterprise Security Manager Default Summary view, this panel presents event activity over the selected time period and includes the baseline average as a visual comparison point. The baseline represents an expected or historical level of event activity, enabling an analyst to quickly identify deviations such as unusually high or low event volumes. Comparing current event patterns with this established average is valuable during initial triage because it adds context beyond the raw number of events: activity that might appear significant in isolation can be normal for that environment, while a smaller deviation from established behavior can warrant investigation. The Event Distribution visualization is therefore the dashboard component intended to expose baseline-related trends directly in the summary view. Enterprise Security Manager is the central console for collecting, normalizing, correlating, and investigating security data, and dashboard views provide the operational context needed for monitoring that data. See the Trellix product documentation portal for Enterprise Security Manager product guides and the Enterprise Security Manager product overview for the platform's monitoring and analytics role.

QUESTION NO: 5

When preparing to apply a patch to the Enterprise Security Manager (ESM) and completing the ESM checklist, the command cat/proc7mdstat has been issued to determine RAID functionally The system returns an active drive result identified as [U J What action should be taken?

A. Apply the patch, this is a properly functional RAID which can be upgraded.

B. Apply the patch, drive 1 is active and can be upgraded.

C. Apply the patch, drive 2 is active and can be upgraded.

D. Contact support before proceeding with the upgrade.

ANSWER: D

Explanation:

Contact support before proceeding with the upgrade. Before an Enterprise Security Manager patch is installed, the appliance storage subsystem must be healthy because patching involves substantial disk activity, service restarts, and potentially a reboot. Linux software RAID status is reviewed through `/proc/mdstat`; a healthy mirrored array normally reports every expected member as available, commonly shown with a full set of `U` indicators. The reported active-drive state indicates that the RAID status needs assessment rather than being accepted as a confirmed healthy array. A degraded, rebuilding, inactive, or otherwise unexpected array condition can leave the appliance exposed to data loss or an unsuccessful upgrade if maintenance proceeds. Support can validate the exact array state, determine whether a disk has failed or synchronization is pending, and provide the appropriate remediation steps before authorizing the patch. This preserves event data and avoids compounding an existing storage issue during a software change. The Linux RAID documentation describes how `md` array status is represented and monitored in `/proc/mdstat`: Linux kernel MD documentation. For appliance-specific diagnostics and approved remediation, use the Trellix Support portal.

QUESTION NO: 6

Which of the following statements about Client Data Sources is TRUE?

A. They will have VIPS, Policy and Agent rights.

B. They will be displayed on the Receiver Properties > Data Sources table.

C. They will appear on the System Navigation tree.

D. They can have independent time zones.

ANSWER: C

Explanation:

They will appear on the System Navigation tree. In McAfee SIEM, a Client Data Source represents a client-side log collection configuration associated with a managed receiver. The System Navigation tree is the central hierarchical view used to locate and manage system components, including receivers and the data sources configured beneath them. Displaying Client Data Sources in this tree gives an administrator a direct way to select a source and review or manage its collection-related configuration in the context of its receiver.

This placement reflects the relationship between the SIEM infrastructure and the event sources it collects: the receiver is a managed system component, and its configured data sources are visible within the navigation hierarchy. Administrators can therefore use the tree to identify the relevant receiver and then access its Client Data Source entries. McAfee SIEM documentation describes system navigation and receiver/data-source administration as connected parts of the console workflow. For current product documentation, consult the Trellix Documentation portal; legacy McAfee enterprise documentation is also available through the McAfee Product Documentation page.

QUESTION NO: 7

Which of the following is the minimum amount of disk space required to install the McAfee Enterprise Security Manager (ESM) as a virtual machine?

A. 100 GB

B. 250GB

C. 500 GB

D. 1 TB

ANSWER: B

Explanation:

250GB is the minimum disk-space allocation required for a virtualized McAfee Enterprise Security Manager installation. ESM is a SIEM platform that needs persistent local storage not only for the operating system and application components, but also for its database, configuration data, event indexing, temporary processing files, and operational overhead. Assigning the documented minimum virtual disk size ensures that the appliance can complete installation successfully and has the baseline capacity needed to initialize its services and data structures.

This value is a deployment prerequisite, not a sizing recommendation for every production environment. Actual storage requirements can grow substantially based on event volume, retention periods, correlation activity, enabled data sources, and whether other ESM-related roles are deployed. Administrators should therefore treat 250GB as the minimum starting point and perform capacity planning before deploying a production SIEM. Trellix maintains ESM product and documentation resources at Trellix Enterprise Security Manager and Trellix Product Documentation.

QUESTION NO: 8

Which of the following are the three compression ratios available for raw logs being handled by the ELM?

A. 10:1,14:1.19:1

B. 14:1,18:1,20:1

C. 14:1,17:1.21:1

D. 14:1,17:1,20:1

ANSWER: D

Explanation:

The correct set is **14:1, 17:1, 20:1**. In the McAfee Enterprise Security Manager environment, the Enterprise Log Manager (ELM) retains raw, original event data for long-term storage, search, investigation, and evidentiary purposes. Because raw logs can consume substantial disk capacity, ELM uses configurable compression to reduce storage requirements while preserving the event content needed for later retrieval and analysis. The available raw-log compression levels are expressed as approximate compression ratios: 14:1, 17:1, and 20:1. These values allow an administrator to balance retained-storage capacity against the processing and operational considerations associated with compressing and retrieving archived raw events. The ratio is an approximation of the storage reduction achieved for the log data; actual results can vary according to the log source, event format, repetition in the data, and other characteristics of the collected events. This setting is specifically relevant to ELM raw-log handling, rather than event normalization or correlation behavior in ESM. Trellix maintains the current product documentation portal at Trellix Documentation, and product background for the SIEM/ESM platform is available at Trellix Enterprise Security Manager.

QUESTION NO: 9

The historical ACE function allows the user to perform retrospective correlations on older data. In which of the following devices is the data located that the historical correlation engine uses?

A. ELM

B. REC

C. ADM

D. ESM

ANSWER: A

Explanation:

ELM is correct because the Event Logger Manager is the McAfee SIEM component designed to retain and provide access to long-term, detailed event data. Historical ACE (Advanced Correlation Engine) performs retrospective correlation by searching events that have already been collected and stored, rather than limiting analysis to the real-time event stream. The historical correlation engine uses the event repository available through the ELM to retrieve the older records required to evaluate correlation-rule conditions across the selected time range.

This separation supports both operational goals of the SIEM platform: current events can be processed for immediate monitoring and alerting, while archived event records remain available for investigations, compliance searches, and retrospective threat hunting. Because the ELM provides the retained event-data source, it enables Historical ACE to identify patterns that may only become apparent after new indicators, rules, or investigative context are available. Trellix identifies Enterprise Security Manager as a platform for centralized security-event analysis and investigations, with event data retention and search being core SIEM capabilities. See the Trellix Enterprise Security Manager product page and the Trellix documentation and support portal for product documentation resources.