PassQueen
a.k.a dumpsqueen.com

McAfee Certified Product Specialist - DLPE

McAfee MA0-103

Version Demo

Total Demo Questions: 9

Total Premium Questions: 91

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, DLP Endpoint Architecture and Components	7
Topic 2, DLP Endpoint Installation	7
Topic 3, DLP Endpoint Configuration	9
Topic 4, DLP Endpoint Policy Management	49
Topic 5, DLP Endpoint Incident Management	13
Topic 6, DLP Endpoint Troubleshooting	6
Total	91

QUESTION NO: 1

Which of the following advanced security settings are the minimum required for replicating files to the Evidence folder?

A. Full control

B. Read/write

C. Create files/write data and create folders/append data

D. List folder/read data

ANSWER: C

Explanation:

Create files/write data and create folders/append data is the minimum required permission set because replication to an Evidence folder must be able to place collected content into the destination and, where necessary, add data to files or create the required folder structure. In Windows advanced NTFS permissions, *Create files / write data* authorizes creation of files within the target folder, while *Create folders / append data* authorizes creation of subfolders and appending data. These rights provide the precise write capability needed for the replication operation without granting broader administrative control over the Evidence folder.

This follows the least-privilege approach: the account used by the product's replication process should receive only the destination-folder permissions necessary to write replicated evidence. Permissions are evaluated on the folder where content is being replicated, and inherited permissions can affect the effective rights of the account. Administrators should therefore verify the effective NTFS permissions for the replication identity on the Evidence folder and ensure that share permissions do not restrict the required access. Microsoft documents these advanced folder permissions, including the file-creation and folder-creation/append-data rights, at Windows permission constants. Product documentation and support resources are available through the Trellix documentation portal.

QUESTION NO: 2

To remove files from quarantine, which of the following is required?

A. Quarantine release key

B. Restore from quarantine

C. Quarantine purge

D. Agent bypass Code

ANSWER: A

Explanation:

A **Quarantine release key** is required to remove a file from quarantine in McAfee Data Loss Prevention Endpoint. Quarantine is intended to prevent a file that triggered a data-protection rule from being used, copied, or otherwise accessed until an authorized reviewer has evaluated the event. The release key provides the controlled authorization needed to restore access to that specific quarantined content. This design keeps the remediation process separate from ordinary endpoint actions and lets security administrators retain oversight of files that may contain sensitive information.

In practice, an authorized DLP administrator or incident handler reviews the relevant incident and, when release is appropriate under organizational policy, supplies or generates the release authorization for the user. The user can then release the file through the DLP Endpoint workflow. This mechanism supports auditability and reduces the risk that a user can independently reverse a DLP enforcement decision. Trellix's DLP materials describe endpoint controls that identify and protect sensitive data, while product support resources provide the administrative guidance for managing endpoint events and recovery workflows. See Trellix Data Loss Prevention and Trellix Support.

QUESTION NO: 3

Which of the following is an indication of potential data loss?

A. Removable Storage Device rule triggers a lot of incidents for one user

B. Removable Storage File Access rule triggers a lot of incidents for one user

C. Discovery rule triggers a lot of incidents for one user

D. Removable Storage Protection rule triggers a lot of incidents for one user

ANSWER: D

Explanation:

“Removable Storage Protection rule triggers a lot of incidents for one user” is an indication of potential data loss because Removable Storage Protection is specifically designed to control the transfer of protected information to removable media. A sustained or unusually high number of protection incidents associated with one user can indicate repeated attempts to write sensitive files to USB storage or other removable devices without meeting the organization’s protection requirements. This pattern warrants investigation because removable media can easily leave the organization’s controlled environment, increasing the likelihood that sensitive data could be exposed, copied, or lost.

DLP incident monitoring is intended to give administrators visibility into policy events and identify behavior that may require follow-up. Reviewing the affected files, the user’s business justification, the destination device, and the frequency of events helps determine whether the activity is legitimate or represents a data-handling risk. Trellix describes Data Loss Prevention as technology for discovering, monitoring, and protecting sensitive information across endpoints and other channels. See the Trellix Data Loss Prevention product page and the Trellix documentation portal for product and policy guidance.

QUESTION NO: 4

Which of the following is critical for troubleshooting system health?

A. System log

B. Administrator log

C. Agent log

D. Policy analyzer

ANSWER: A

Explanation:

System log is critical for troubleshooting system health because it records the operational events that indicate whether the product and its underlying components are functioning normally. When a system-health issue is reported, the system log provides the chronological evidence needed to establish what occurred, when it began, and whether a service, component, configuration, or resource condition generated an error or warning. This makes it the primary starting point for correlating symptoms with recorded events and identifying the scope of a failure.

Effective troubleshooting depends on reviewing logged timestamps, event severity, component status messages, and recurring errors around the time the issue occurred. These details help an administrator determine whether the condition is transient, tied to a specific service or host state, or requires escalation with collected diagnostic evidence. Maintaining and reviewing system logs is therefore a core operational practice for monitoring health, investigating incidents, and validating recovery after corrective action. Trellix provides product-specific documentation and support resources through its Product Documentation portal and Knowledge Center, where administrators can locate the relevant logging and troubleshooting guidance for their deployed version.

QUESTION NO: 5

How can remote users who are not connected to the corporate network be protected?

A. Enable online reactions within protection rules

B. Enable location-aware rules for offline users

C. Add local users to user assignment groups

D. Enable offline reactions within protection rules

ANSWER: D

Explanation:

Enable offline reactions within protection rules is correct because McAfee Data Loss Prevention Endpoint must be able to enforce data-protection policy directly on a managed endpoint even when that endpoint cannot communicate with the corporate network or management infrastructure. Protection rules can include reactions intended for offline operation, allowing the installed endpoint client to apply the policy using its locally available configuration. This is particularly important for traveling staff, home users, and any device operating away from the organization's network, where waiting for a server-side or network-connected response could leave sensitive data unprotected. Offline reactions provide the endpoint with the enforcement behavior it needs at the time the monitored action occurs, such as handling an attempted sensitive-data transfer according to the assigned protection rule. The endpoint later reconnects and can resume normal communication and reporting, but the protection decision does not depend on a live corporate-network connection. This endpoint-focused, policy-based approach is a core use case for data-loss-prevention products designed to protect data wherever users work. See the Trellix Data Loss Prevention product overview and the Trellix product documentation portal for product documentation and deployment guidance.

QUESTION NO: 6

To assist with perceived performance issues prior to product installation, the DLP End point Administrator could prepare by

A. disabling unused modules.

B. distributing agent override codes.

C. establishing a system baseline.

D. enabling the system watch dog service.

ANSWER: C

Explanation:

Establishing a system baseline is the appropriate preparation because it records the endpoint's normal operating behavior before the DLP Endpoint software is deployed. A useful baseline includes measurements such as processor utilization, memory consumption, disk activity, logon time, application launch time, network behavior, and the typical workload of representative users. Capturing these measurements beforehand gives the administrator objective evidence for comparing the same device and workload after installation. This makes it possible to distinguish a genuinely deployment-related impact from pre-existing resource pressure, background processes, hardware limitations, or normal variation in endpoint activity.

For a meaningful comparison, baseline data should be collected across normal business cycles and from endpoint types that represent the environment, then retained with the relevant system configuration details. Administrators can use the findings to set realistic performance expectations, identify systems requiring remediation before rollout, and investigate reported slowdowns with reproducible data rather than relying solely on user perception. This aligns with the general purpose of Trellix Data Loss Prevention Endpoint: applying endpoint data-protection controls while allowing organizations to plan, deploy, and operate the product in their specific environment. See the Trellix Data Loss Prevention product information and Trellix Support for product documentation and deployment resources.

QUESTION NO: 7

An organization needs to prevent users from printing documents that contain confidential product-design information. Which type of protection rule can the DLP Endpoint administrator configure?

A. File System Protection Rule

B. Print Protection Rule

C. Network Communication Protection Rule

D. Web Post Protection Rule

ANSWER: B

Explanation:

Print Protection Rule is correct because it monitors and controls protected content when a user attempts to print it from a managed endpoint. The rule can use content-classification criteria to identify confidential design information and apply a response such as blocking the print operation, notifying the user, and creating an incident.

This rule is appropriate because the data-transfer channel in this scenario is printing. File System Protection, Network Communication Protection, and Web Post Protection rules apply to different data-handling activities. See the Trellix Product Documentation portal for DLP Endpoint rule-configuration guidance.

QUESTION NO: 8

The DLP End point administrator needs to prevent sensitive data from being transmitted over FTP. Which Rule can be configured to meet this requirement?

A. File System Protection Rule

B. Cloud Protection Rule

C. Application File Access Protection Rule

D. Network Communication Protection Rule

ANSWER: D

Explanation:

Network Communication Protection Rule is the appropriate rule because it is designed to monitor and control sensitive-data transmissions through network communication channels, including FTP. In DLP Endpoint, this type of rule can inspect outbound data flows for configured data-classification criteria, such as file properties, registered documents, or content matching a defined classification. When the rule detects protected information in an FTP transfer, it can apply the assigned response, such as blocking the transmission, notifying the user, or logging the incident for investigation.

This approach protects data at the point where it leaves the endpoint through a network protocol. The administrator should configure the rule's network communication settings for FTP, select the sensitive-data definitions that require protection, scope the policy to the intended users or endpoint systems, and assign a blocking reaction. This provides protocol-specific enforcement while producing incidents and evidence that can be reviewed in the DLP management console. Trellix maintains DLP Endpoint product documentation and configuration guidance through its documentation portal: Trellix Documentation. Additional information about the endpoint data loss prevention product is available at Trellix Data Loss Prevention.

QUESTION NO: 9

Which of the following DLP features is associated with designating destinations and sources to protect?

A. Text patterns

B. Content Classification

C. Definitions

D. Dictionaries

ANSWER: C

Explanation:

Definitions is correct because McAfee Data Loss Prevention uses definitions as reusable policy objects for describing the entities and conditions to which protection controls apply. A definition can designate relevant sources and destinations, enabling a policy rule to consistently recognize where protected information originates, where it may be sent, or where it may be stored. This lets an administrator build policy logic around organizationally meaningful locations and transfer paths rather than having to recreate those settings independently in every rule.

In practical policy administration, definitions help make DLP controls manageable and consistent. Administrators create the applicable definition once, associate it with the required policy rules, and can then update that definition centrally when an approved destination, monitored source, or business requirement changes. That reuse is especially important in environments with many policies and endpoints, because it provides a structured way to apply the same protection scope throughout the deployment. McAfee DLP is designed to identify, monitor, and protect sensitive data across endpoints and data movement channels; definitions provide the policy-building mechanism for designating the relevant protection scope. See the Trellix Data Loss Prevention product overview and the Trellix documentation portal for product documentation and policy guidance.