PassQueen
a.k.a dumpsqueen.com

Certified McAfee Security Specialist - ePO

McAfee MA0-100

Version Demo

Total Demo Questions: 17

Total Premium Questions: 177

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

If you specify the McAfee Agent Policy to collect only minimal properties, the agent collects only which of the following? (Choose two)

A. Installed software information

B. DAT file version number

C. Processor speed

D. Installation path

E. Operation system

ANSWER: B D

Explanation:

When the McAfee Agent policy is configured to collect only minimal properties, the intent is to limit inventory collection to the core information needed for McAfee ePO to identify the managed endpoint and report the protection state of McAfee-managed products. **DAT file version number** is a key protection-status property because it identifies the currently deployed anti-malware detection content. ePO uses reported DAT information to provide visibility into content currency and to support compliance reporting for managed security products.

Installation path is also part of the minimal information reported by the agent. This property identifies the local path associated with the installed McAfee software and enables ePO to maintain the managed-product installation details without performing the broader hardware and software inventory associated with full property collection. Selecting minimal collection reduces the amount of system inventory data sent during agent-to-server communication while retaining these essential managed-product properties. McAfee Agent policy and property-collection behavior are documented in the McAfee Agent Product Guide and related ePO documentation; see Trellix Product Documentation and Trellix Knowledge Center.

QUESTION NO: 2

Extensions that are installed into the ePO server are in what file format?

A. .zip

B. .nap

C. .rar

D. .jar

ANSWER: A

Explanation:

Extensions installed in McAfee ePolicy Orchestrator are supplied and imported as **.zip** packages. An extension adds product-specific capabilities to the ePO console, such as policy pages, queries, reports, dashboards, server tasks, and management interfaces. Administrators install these packages through the Extensions page in ePO, where the server reads the contents of the ZIP archive and registers the extension's components for use in the console. This packaging approach lets a product's interface and supporting definitions be distributed as a single importable file while preserving the structure ePO expects during installation. In practical administration, extensions are commonly installed before, or alongside, deployment of a managed McAfee product so that its policies and configuration options are available in ePO. The .zip package is therefore the expected file type when selecting an extension package for installation. McAfee's ePO documentation describes extension management as an administrative function and identifies the use of extension packages in the console. See the McAfee ePolicy Orchestrator support documentation and the ePolicy Orchestrator Product Guide for extension-management guidance.

QUESTION NO: 3

Which of the following options are required to share policies between ePO servers? (Choose three)

A. Designate the policy

B. Register the server

C. Duplicate the policy

D. Assign the policy

E. Schedule a server task

ANSWER: A B E

Explanation:

Sharing policies between McAfee ePolicy Orchestrator servers requires preparation on the source server, a trusted connection to the other ePO server, and an automated sharing action. **Designate the policy** makes the selected policy available for sharing; ePO does not expose every policy automatically. **Register the server** establishes the remote-server relationship and supplies the connection details and credentials needed for one ePO server to communicate with the other. This registration is the basis for securely exchanging shared objects between the environments. **Schedule a server task** then performs policy sharing on a defined schedule, so designated policy content is exported and made available to the registered server without requiring a manual action each time. Together, these steps provide the required configuration: identify the policy content to share, establish the destination ePO server relationship, and run the policy-sharing process. Trellix maintains ePO product documentation and knowledge resources at Trellix Documentation and Trellix Knowledge Center.

QUESTION NO: 4

To remove computers from ePO using the Active Directory Synchronization task, it is required that the account has access to the:

A. Deleted computers

B. Deleted Objects container

C. Organizational Unit

D. Active Directory.

ANSWER: B

Explanation:

The account used by the Active Directory Synchronization task must have access to the **Deleted Objects container**. When ePO synchronizes systems with Active Directory and is configured to remove systems that no longer exist in the synchronized directory scope, it must be able to identify computer objects that were deleted from Active Directory. Deleted directory objects are retained in the special Deleted Objects container during the applicable retention period rather than being immediately and permanently removed. Access to that container enables ePO to detect those deletions and accurately remove the corresponding managed computer records as part of the synchronization process.

This requirement is especially important because deleted objects have distinct visibility and permission handling in Active Directory. The synchronization account needs the appropriate directory permissions to query this container; otherwise, ePO cannot reliably obtain deletion information needed for automated removal. Microsoft documents that deleted Active Directory objects are stored in the Deleted Objects container and can be accessed for recovery or directory-management operations when the required permissions are present. See Microsoft's Deleted Object Recovery documentation and the Trellix product documentation portal for ePO administration guidance.

QUESTION NO: 5

Product deployment packages are checked into what repository?

A. Distributed

B. Master

C. Fallback

D. Source

ANSWER: B

Explanation:

Master is correct because the Master Repository is the central ePolicy Orchestrator repository into which product software, extensions, updates, and deployment packages are checked in. When an administrator checks in a package through the ePolicy Orchestrator console, the package is stored in the Master Repository and becomes available for use in product deployment tasks and update workflows. The repository maintains the package content and its associated metadata, allowing ePolicy Orchestrator to determine which versions are available and to distribute the appropriate content to managed systems. In environments that use additional repository infrastructure, content is first managed centrally in the Master Repository and can then be replicated to distributed repositories for local agent access. This central check-in process supports controlled software deployment, consistent package versioning, and administrative management of product content across the organization. Trellix documentation for ePolicy Orchestrator describes repository management and package check-in as core administrator activities; see the ePolicy Orchestrator Product Guide and the Trellix Knowledge Center repository guidance.

QUESTION NO: 6

An RSD Sensor has been deployed from the ePO console. However, it has not reported back. Which of the following is the most likely cause? (Choose three)

A. The sensor is unable to resolve the IP address for ePO

B. The sensor is blacklisted

C. Deployment of the sensor failed

D. Sensor service is disabled after installation

E. The sensor is an exception

ANSWER: A C D

Explanation:

The sensor is unable to resolve the IP address for ePO, Deployment of the sensor failed, and Sensor service is disabled after installation are the relevant causes because an RSD Sensor must be successfully installed, have its sensor service running, and be able to communicate with its registered ePO server before it can submit discovery information. The deployment task installs the sensor remotely; if that task does not complete, the endpoint has no functioning sensor component available to report. After installation, the sensor relies on its service to perform network listening and discovery work. If that service is stopped or disabled, it cannot collect or send detection data. Finally, the sensor must be able to locate and reach ePO using the configured server information. Name-resolution or network-connectivity problems prevent the sensor from establishing the required communication path and checking in. These conditions should be investigated through deployment task status, the endpoint's service status, and connectivity/name-resolution tests to the ePO server. Trellix's ePO documentation describes managed-product deployment and agent/server communication requirements; see the Trellix ePolicy Orchestrator Product Guide and the Trellix knowledge base.

QUESTION NO: 7

What scheduling options are available when setting up a Product Deployment Task? (Choose three)

A. Enable Randomization

B. Stop the task if it runs for a specified amount of time

C. Run at every policy enforcement

D. Defer scan when using battery power

E. Run missed task at a specified time delay

ANSWER: A B E

Explanation:

Product Deployment Task scheduling includes controls that let an administrator manage when clients begin a deployment, how long the task is allowed to execute, and how to handle endpoints that were unavailable at the planned start. **Enable Randomization** distributes task start times across a configured window. This prevents a large managed population from simultaneously contacting the ePO server or repository, reducing avoidable load on network links and distribution infrastructure. **Stop the task if it runs for a specified amount of time** establishes a runtime limit, allowing the administrator to prevent an unusually long-running deployment from continuing indefinitely. **Run missed task at a specified time delay** provides catch-up behavior for systems that were powered off, disconnected, or otherwise unable to receive the scheduled task at its normal time; the delay helps avoid an immediate concentration of deferred deployments when those systems reconnect. These settings are part of the scheduling controls used to make client software deployment predictable and scalable. Consult the official Trellix product documentation portal and the Trellix Product Support site for the ePolicy Orchestrator Product Guide applicable to the deployed version.

QUESTION NO: 8

System properties are directly helpful for when creating which of the following? (Choose two)

A. Criteria-based tags

B. Server tasks

C. Client tasks

D. Assigned policies

E. Creating queries

ANSWER: A E

Explanation:

System properties are directly useful when creating **Criteria-based tags** and **Creating queries**. ePolicy Orchestrator collects and maintains properties for managed systems, including details such as the operating system, computer name, IP address, installed McAfee/Trellix products, product versions, and security-status information. Criteria-based tagging uses these reported system-property values as conditions. For example, an administrator can automatically apply a tag to systems matching a particular operating-system version, systems with a specified product installed, or systems whose properties meet a defined status criterion. This enables dynamic classification as endpoint information changes.

Queries also use system properties as reportable fields and filtering criteria. An administrator can construct a query that returns systems meeting selected property conditions, then display, sort, group, or export those results for operational reporting and investigation. Because both features rely on the endpoint data stored in the ePO database, system properties provide the factual attributes used to define tag membership and query output. Trellix identifies ePolicy Orchestrator as its centralized endpoint-security management platform; its documentation portal provides the applicable product guides and administration references: Trellix ePolicy Orchestrator and Trellix Documentation.

QUESTION NO: 9

Which of the following cannot be completed within the Policy Catalog?

A. Edit

B. Rename

C. Duplicate

D. Assign

ANSWER: D

Explanation:

Assign is correct because the Policy Catalog is the central repository for viewing and managing policy definitions, rather than the location where policies are applied to managed objects. Administrators use it to open a product's policy category, select a policy, and perform policy-management tasks such as editing its settings, creating a copy, or changing its name. Those operations affect the policy object stored in ePolicy Orchestrator.

Applying a policy is a separate administrative step because it determines the effective configuration for a particular System Tree group or managed system. Policy assignment is performed from the target group or system's policy-assignment area, where the administrator can select the desired product policy and control inheritance or assignment behavior. This separation lets one maintained policy be reused consistently across multiple groups while allowing assignment decisions to follow the organization's System Tree structure. Trellix describes ePolicy Orchestrator as a centralized platform for managing endpoint security policy and system administration; see the Trellix ePolicy Orchestrator product page and the Trellix documentation portal for product documentation and administration guidance.

QUESTION NO: 10

Which of the following is an available default notification rule?

A. Daily known category notification

B. Virus detected and not removed

C. Virus detected and removed

D. Non-complaint computer detected

ANSWER: D

Explanation:

Non-complaint computer detected is the available default notification rule, with the wording referring to a computer that does not meet the compliance requirements defined in ePolicy Orchestrator. ePO evaluates managed systems against assigned policies and can use compliance-related events or status changes as notification triggers. This default rule provides administrators with prompt visibility when a system becomes noncompliant, enabling them to investigate the system's policy status, remediation state, and recent events. The notification framework is designed to send an alert when the specified event occurs and can be configured with actions such as email delivery or execution of a response. This supports the central ePO workflow of identifying systems that have drifted from the organization's required security configuration and responding quickly from the management console. Administrators can review, enable, edit, and create notification rules in the ePO server settings, tailoring recipients and responses to their operational procedures. Trellix, the current provider of ePO, documents the product's centralized policy, compliance, and event-management capabilities at Trellix ePolicy Orchestrator. Product documentation and administration guidance are available through the Trellix Documentation portal.

QUESTION NO: 11

Which of the following are available within the Policy Catalog? (Choose three)

A. Share

B. Duplicate

C. Assign

D. View

E. Lock

ANSWER: A B D

Explanation:

Within ePolicy Orchestrator, the Policy Catalog is the central interface for working with product policies. It provides a view of the policy categories and policies supplied by managed products, letting an administrator open and inspect the policy definitions that are available for configuration and assignment. The catalog also supports creating a policy based on an existing one through duplication. Duplicating preserves the existing policy settings as a starting point while producing a separately named policy that can be tailored for a different group, system set, or operational requirement. Policy sharing is also available for supported policy-management workflows, allowing a policy to be made available beyond its initial owner or context so it can be reused by authorized administrators. These functions help administrators maintain consistent policy baselines while efficiently adapting settings for distinct endpoints or groups. Access to policy actions is governed by the administrator's assigned ePO permissions, so the available controls can vary by role. For product documentation and ePO administration guidance, see the Trellix Product Documentation portal and the Trellix ePolicy Orchestrator product page.

QUESTION NO: 12

How many managed machines are required before it is recommended to use a dedicated ePO server?

A. 50

B. 500

C. 5000

D. 50000

ANSWER: C

Explanation:

5000 is correct. McAfee ePolicy Orchestrator sizing guidance recommends that an ePO server be dedicated to ePO when the environment exceeds approximately 5,000 managed systems. At this scale, the server must handle frequent agent-server communications, policy enforcement and collection, event processing, reporting, database activity, repository-related operations, and scheduled server tasks. Giving ePO its own server helps reserve CPU, memory, disk I/O, and network capacity for those management functions, rather than competing with unrelated applications or infrastructure roles. This recommendation is a deployment best practice intended to maintain predictable console responsiveness, timely policy and event processing, and reliable management as the number of endpoints grows. The exact supported capacity can still depend on the ePO version, hardware specifications, SQL Server placement, enabled products, event volume, and task schedules; therefore, administrators should use the applicable sizing documentation when planning a production deployment. Trellix maintains the current ePO documentation library at Trellix Product Documentation, and its knowledge base contains ePO deployment and sizing guidance at KB51569.

QUESTION NO: 13

Which of the following is a file system filter driver?

A. Mfeapfk.sys

B. Mfeavfk.sys

C. Mfebopk.sys

D. Mfehidk.sys

ANSWER: B

Explanation:

Mfeavfk.sys is the McAfee VirusScan anti-virus file-system filter kernel driver. It operates in the Windows file-system I/O path so that VirusScan can inspect file activity, such as files being opened, created, modified, or executed, and apply on-access scanning before content is made available to applications. This kernel-level position is essential to real-time malware detection because it lets the anti-virus engine evaluate files at the point of access rather than relying only on scheduled or manual scans. The “av” portion of the driver name identifies its anti-virus function, while “fk” denotes the filter-kernel role. Windows supports this type of security integration through file-system filter drivers, which attach to the file-system stack and observe or process I/O operations. Microsoft’s overview of this architecture is available in Filter Drivers. McAfee VirusScan Enterprise is designed to provide on-access anti-virus protection on managed endpoints, a capability that depends on this file-system interception layer; see the vendor’s VirusScan Enterprise product information.

QUESTION NO: 14

Which of the following needs to be enabled to successfully deploy an Agent from the ePO server? (Choose three)

A. Framework service

B. Remote Registry service

C. File and Printer Sharing

D. Admin $ share

E. C$ share

ANSWER: B C D

Explanation:

Successful remote deployment of the McAfee Agent from ePolicy Orchestrator to a Windows system depends on the ePO server being able to discover, authenticate to, and copy the Agent installation files to the target. **Remote Registry service** must be enabled and running so that ePO can query required information from the remote Windows computer during deployment. The Windows firewall and system configuration must also permit **File and Printer Sharing**, which enables the SMB-based network access used for remote file operations. Finally, the **Admin $ share** must be available. This default administrative share maps to the Windows directory and provides the remote administrative path used by ePO to copy Agent deployment files and initiate installation on the managed endpoint. These requirements assume that the deployment credentials supplied in ePO have local administrator permissions on the target computer. Microsoft documents Remote Registry as a Windows service used for remote access to registry information, and its SMB documentation describes the file-sharing transport relied on for administrative shares and remote file access. See Remote Registry and SMB file sharing overview.

QUESTION NO: 15

What important property simplifies policy and task administration?

A. Hierarchy

B. Lock Policy

C. Inheritance

D. Enforcement

ANSWER: C

Explanation:

Inheritance simplifies policy and task administration in McAfee ePolicy Orchestrator by allowing groups lower in the System Tree to receive policy and client-task settings from their parent groups. An administrator can define a common configuration once at a higher level, then have that configuration apply automatically throughout the relevant part of the managed environment. This provides a consistent security baseline while substantially reducing repetitive configuration work.

Inheritance is especially useful when endpoints are organized into logical groups, such as by business unit, location, operating system, or security requirement. Administrators can maintain broad, organization-wide settings at a parent group and, where needed, create targeted configurations at lower levels. This model makes policy management more scalable: changes to an inherited policy can be distributed through the group structure without editing each individual system or group separately. It also helps ensure that newly added systems receive the appropriate administrative configuration based on where they are placed in the System Tree.

Trellix documentation describes ePolicy Orchestrator policy assignment and System Tree administration in its ePolicy Orchestrator Product Guide. Additional product documentation is available through the Trellix Documentation portal.

QUESTION NO: 16

Which of the following steps are needed for Policy Sharing? (Choose three)

A. Register the remote ePO servers

B. Share the individual policies

C. Configure Server Task

D. Enable Global Updating

E. Share default policies

ANSWER: A B C

Explanation:

Policy Sharing in McAfee ePolicy Orchestrator requires a trust relationship and an explicit sharing workflow between ePO servers. Administrators first register the remote ePO servers so that the participating servers can communicate securely and recognize one another as authorized sharing partners. Registration establishes the server-to-server relationship used for shared policy operations. The policies intended for use by another registered server must then be explicitly shared; sharing is performed for selected individual policies rather than automatically exposing every policy in the policy catalog. Finally, a Server Task is configured to perform the policy-sharing operation on a defined schedule or as needed, allowing the designated shared policies to be distributed to the registered remote server. Together, these actions establish connectivity, identify the policy content to distribute, and automate or initiate distribution. This feature supports consistent policy administration across separate ePO environments while retaining control over exactly which policies are made available. Trellix maintains ePolicy Orchestrator documentation and product resources at Trellix Product Documentation and provides product information at Trellix ePolicy Orchestrator.

QUESTION NO: 17

Which file found in the \Program Files\McAfee\ePolicy Orchestrator\Server\conf directory needs to be modified to change the default ePO Console session timeout?

A. server.xml

B. web.xml

C. tomcat-users.xml

D. context.xml

ANSWER: B

Explanation:

The correct file is **web.xml**. In ePolicy Orchestrator, the console is hosted by the embedded Apache Tomcat application server, and the web application's session behavior is controlled through its deployment descriptor. The `<session-config>` section in `web.xml` contains the `<session-timeout>` setting, expressed in minutes. Updating that value changes the period of console inactivity after which a user's web session expires. This is the appropriate configuration point because the setting governs HTTP application sessions rather than Tomcat connector settings, user-account definitions, or application context defaults. The ePO Server service should be restarted after the configuration is changed so Tomcat reloads the deployment configuration; administrators should also preserve a backup of the original file and account for the possibility that an ePO upgrade may replace customized configuration files. Trellix guidance for ePO configuration and support articles is available through the Trellix Knowledge Center. Apache Tomcat documents the standard `session-config` and `session-timeout` deployment-descriptor elements at Tomcat Session Configuration.