PassQueen
a.k.a dumpsqueen.com

Administration of Symantec Endpoint Protection 14

Symantec 250-428

Version Demo

Total Demo Questions: 20

Total Premium Questions: 203

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Planning and Designing a Symantec Endpoint Protection Environment	25
Topic 2, Installing and Configuring Symantec Endpoint Protection	33
Topic 3, Managing Symantec Endpoint Protection Clients	24
Topic 4, Managing Symantec Endpoint Protection Policies	83
Topic 5, Monitoring and Reporting	15
Topic 6, Maintaining and Troubleshooting Symantec Endpoint Protection	23
Total	203

QUESTION NO: 1

An administrator selects the Backup files before attempting to repair the Remediations option in the Auto-Protect policies.

Which two actions occur when a virus is detected? (Select two.)

A. Send the file to Symantec Insight

B. Check the reputation

C. Encrypt the file

D. Replace the file with a place holder

E. Store in Quarantine folder

ANSWER: C E

Explanation:

When *Backup files before attempting to repair* is enabled in an Auto-Protect remediation policy, Symantec Endpoint Protection preserves a recoverable copy of a detected file before making a repair attempt. The preserved content is encrypted, which prevents the infected content from being opened or executed as an ordinary file while it is retained. This safeguards the backup and avoids creating another accessible copy of the threat.

The backup is also placed in the local Quarantine folder. Quarantine is the protected holding area used by the client for detected items and retained backups, allowing an administrator to review or restore content when appropriate. Therefore, the actions that occur are *Encrypt the file* and *Store in Quarantine folder*. This behavior is specifically relevant to retaining the original file before remediation, rather than simply attempting a repair without maintaining a protected backup. Broadcom's Endpoint Protection documentation describes policy-based virus and spyware remediation and the client quarantine mechanism in the Symantec Endpoint Protection 14.3 documentation; product resources are also available through the Broadcom Symantec Endpoint Protection knowledge base.

QUESTION NO: 2

An administrator wants managed clients at a remote office to obtain content updates from a Group Update Provider (GUP) rather than directly from the Symantec Endpoint Protection Manager.

Which policy should the administrator configure?

A. LiveUpdate policy

B. Firewall policy

C. Intrusion Prevention policy

D. Client Control policy

ANSWER: A

Explanation:

LiveUpdate policy is correct because it controls how SEP clients obtain protection content, including virus definitions, intrusion prevention signatures, and other updates. The administrator configures the GUP as an update source in the LiveUpdate policy and assigns that policy to the client group that should use the GUP.

Using a GUP allows a remote office to download content once from the management infrastructure and then distribute it locally to other SEP clients. This reduces repeated WAN downloads and can reduce the content-delivery workload on the SEPM. See the Broadcom Symantec Endpoint Protection documentation for LiveUpdate and content-distribution configuration guidance.

QUESTION NO: 3 - (SIMULATION)

Match the following list of ports used by Symantec Endpoint Protection (SEP) to the defining characteristics by clicking and dragging the port on the left to the corresponding description on the right.

ANSWER: See the explanation for the answer

Explanation:

Match the SEP ports as follows:

`TCP 8443` — Secure HTTPS communication between Symantec Endpoint Protection clients and the Symantec Endpoint Protection Manager (SEPM); this is the normal/default secure client-management port. It is also used for SEPM console access/replication when applicable.
`TCP 8014` — HTTP (non-SSL) communication between SEP clients and SEPM.
`UDP 2967` — SEP client notification/wakeup traffic from SEPM. A notified client then contacts the manager rather than waiting for its next heartbeat.
`TCP 80` — HTTP access for LiveUpdate/content downloads when an HTTP LiveUpdate source is used.
`TCP 443` — HTTPS access for LiveUpdate/Symantec online content and services when a secure Internet connection is used.

The key SEPM client-management pairing is `8443 = HTTPS` and `8014 = HTTP`; `2967/UDP` is for client notification rather than the normal client heartbeat/content-management connection.

QUESTION NO: 4

Which two are policy types within the Symantec Endpoint Protection Manager? (Select two.)

A. Intrusion Prevention

B. Exceptions

C. Process Control

D. Shared Insight

E. Host Protection

ANSWER: A B

Explanation:

Symantec Endpoint Protection Manager uses policies to define and distribute endpoint security configuration to groups of managed clients. **Intrusion Prevention** is a policy type that configures network intrusion prevention behavior, including protection against known network-based attacks and suspicious traffic. Administrators assign this policy through a client group so that the configured prevention settings are consistently applied to its members.

Exceptions is also a policy type in the manager. It is used to create centrally managed exclusions for files, folders, processes, extensions, and other items that should be omitted from applicable protection scans or detections. Maintaining exceptions as a policy lets administrators target the exclusions to the appropriate groups and update them centrally rather than configuring each endpoint individually.

Both policy types are listed among the policies that can be created and assigned in the Symantec Endpoint Protection Manager console. The manager's policy-based design is central to administering protection settings across an enterprise environment. See Broadcom's Symantec Endpoint Protection documentation and the policy documentation reference.

QUESTION NO: 5

An administrator is troubleshooting a Symantec Endpoint Protection (SEP) replication.

Which component log should the administrator check to determine whether the communication between the two sites is working correctly?

A. Tomcat

B. Apache Web Server

C. Group Update Provider (GUP)

D. SQL Server

ANSWER: A

Explanation:

Tomcat is correct because Symantec Endpoint Protection Manager site-to-site replication communication is handled through the management server's Tomcat application service. The Tomcat logs record the web-application activity associated with replication requests, including connection attempts, authentication or certificate-related issues, HTTP processing errors, and failures communicating with a replication partner. Reviewing this component's logs lets an administrator confirm whether one management site is reaching the other and whether the replication transaction is being accepted and processed.

Replication depends on both sites having appropriate network connectivity and a healthy management-server web service. Therefore, Tomcat log entries are particularly useful for distinguishing a communication or application-service issue from a problem with replicated data after it arrives. Administrators should correlate relevant timestamps from each site while checking the logs, especially after forcing or waiting for a replication cycle. Broadcom's Endpoint Protection documentation describes management-server replication as a management-server function and provides the product documentation needed for replication administration and troubleshooting. See the Broadcom Symantec Endpoint Protection documentation portal and the Broadcom Knowledge Base for Endpoint Protection operational guidance.

QUESTION NO: 6

An administrator needs to increase the access speed for client files that are stored on a file server. Which configuration should the administrator review to address the read speed from the server?

A. Enable Network Cache in the client's Virus and Spyware Protection policy

B. Add the applicable server to a trusted host group

C. Enable download randomization in the client group's communication settings

D. Create a Firewall allow rule for the server's IP address.

ANSWER: A

Explanation:

Enable Network Cache in the client's Virus and Spyware Protection policy is correct because Network Cache is designed specifically to improve performance when Endpoint Protection clients access files over a network share. Without a cache, a file that is read from a file server can be scanned repeatedly by the client's Auto-Protect process each time it is accessed. Network Cache records information about files that have already been scanned, allowing the client to avoid unnecessary repeat scanning when the cached result remains valid. This reduces scanning overhead, network traffic, and the delay users can experience while opening or reading files stored on a server.

The setting is configured in the Virus and Spyware Protection policy because it controls behavior of the antivirus Auto-Protect component for network-file access. An administrator investigating slow read access to files hosted on a file server should therefore review whether Network Cache is enabled and ensure its settings are appropriate for the organization's security and performance requirements. Broadcom's Endpoint Protection documentation describes Network Cache as a performance feature for files accessed across the network. See the Virus and Spyware Protection policy documentation and the Symantec Endpoint Protection documentation portal.

QUESTION NO: 7

What are two supported Symantec Endpoint Protection Manager authentication types? (Select two.)

A. Microsoft Active Directory

B. MS-CHAP

C. RSA SecurID

D. Biometrics

E. Network Access Control

ANSWER: A C

Explanation:

Symantec Endpoint Protection Manager supports integration with Microsoft Active Directory for administrator authentication. This lets the manager validate administrator credentials against the organization's Active Directory domain, allowing existing directory identities and associated access controls to be used rather than requiring separate credentials for every administrator. Active Directory integration is a supported authentication choice when configuring or managing administrator accounts in the Symantec Endpoint Protection Manager console.

RSA SecurID is also a supported authentication type for Symantec Endpoint Protection Manager. It enables authentication through an RSA Authentication Manager environment, supporting organizations that use RSA SecurID token-based or other RSA-backed authentication mechanisms for administrative access. In both cases, the authentication service validates the administrator identity while Symantec Endpoint Protection Manager continues to apply the administrator role and permissions configured within the manager. Broadcom's Endpoint Protection documentation describes administrator authentication and directory-service integration features in the product documentation set. See the Symantec Endpoint Protection 14.3 documentation and the Endpoint Protection documentation portal.

QUESTION NO: 8

Which Symantec Endpoint Protection defense mechanism provides protection against threats that propagate from system to system through the use of autorun.inf files?

A. Host Integrity

B. SONAR

C. Application and Device Control

D. Emulator

ANSWER: C

Explanation:

Application and Device Control is correct because it includes controls designed to prevent malware propagation through removable media and the Windows AutoRun/AutoPlay mechanism. A common propagation technique used by worms is to place a malicious executable and an `autorun.inf` file on a USB drive, network share, or other removable device. When the media is accessed on another computer, AutoRun can launch the referenced program and continue the infection chain. In Symantec Endpoint Protection, an Application and Device Control policy can enforce AutoRun-related protection and device-access restrictions, reducing the opportunity for such media-borne threats to execute automatically. Administrators configure these controls centrally in Symantec Endpoint Protection Manager and apply the policy to the relevant client groups, enabling consistent protection across managed endpoints. This mechanism is specifically suited to controlling the operating-system and device behaviors that autorun-based threats rely on, rather than solely identifying a file after it has executed. Broadcom's Endpoint Protection documentation describes policy-based endpoint controls, including Application and Device Control capabilities: Broadcom Symantec Endpoint Protection documentation. Additional product and support resources are available from the Broadcom Endpoint Protection Security Center.

QUESTION NO: 9

Which two options are available when configuring DNS change detections for SONAR? (Select two.)

A. Log

B. Quarantine

C. Block

D. Active Response

E. Trace

ANSWER: A C

Explanation:

For SONAR DNS change detections, the available response choices are **Log** and **Block**. DNS settings are a valuable target for malware because changing a device's configured DNS server can redirect users to malicious infrastructure, interfere with security updates, or enable phishing and traffic interception. SONAR, Symantec Endpoint Protection's behavioral detection technology, can monitor for this type of suspicious system change.

Selecting **Log** records the DNS-change detection in the client logs and management reporting. This is appropriate when an administrator wants visibility into DNS-related behavior, wants to investigate the affected process, or is initially assessing the operational impact of the detection before enforcing it. Selecting **Block** instructs the client to prevent the detected DNS-change behavior, providing immediate protection when the activity is not expected in the environment. These actions allow administrators to choose between audit visibility and active enforcement while configuring SONAR behavior in an Endpoint Protection policy. Symantec's Endpoint Protection documentation describes SONAR as the component that detects suspicious application behavior and provides configurable responses through its policy settings. See the Broadcom Symantec Endpoint Protection documentation and the Broadcom knowledge base for Endpoint Protection policy and detection-management guidance.

QUESTION NO: 10

A company deploys Symantec Endpoint Protection client to its sales staff who travel across the country.

Which deployment method should the company use to notify its sales staff to install the client?

A. Unmanaged Detector

B. Client Deployment Wizard

C. Pull mode

D. Push mode

ANSWER: B

Explanation:

The correct answer is **Client Deployment Wizard**. In Symantec Endpoint Protection Manager, the Client Deployment Wizard can create a client-installation package and distribute it using an email notification. This is well suited to employees who are geographically dispersed, such as travelling sales staff, because each user can receive installation instructions and a link or package by email, then install the managed client when they have Internet or corporate-network access.

The wizard lets the administrator select the appropriate client package, include the required communication settings so the installed client can register with the designated management server, and prepare the notification for the intended recipients. This approach provides a practical, user-initiated installation workflow without requiring the administrator to be connected directly to every employee device at the time of installation. It also supports deployment to devices that may be off the internal network or unavailable during normal administrative deployment windows.

Broadcom's Endpoint Protection documentation describes the available client-installation and deployment workflows, including use of deployment packages and email-based distribution. See the Symantec Endpoint Protection documentation portal and the Client Deployment Wizard reference.

QUESTION NO: 11

Which ports on the company firewall must an administrator open to avoid problems when connecting to Symantec Public LiveUpdate servers?

A. 2967, 8014, and 8443

B. 21, 443, and 2967

C. 21, 80, and 443

D. 25, 80, and 2967

ANSWER: C

Explanation:

21, 80, and 443 is correct because Symantec Endpoint Protection clients and management components may use Symantec Public LiveUpdate locations that are available through the standard FTP, HTTP, and HTTPS protocols. TCP port 21 supports FTP access, TCP port 80 supports HTTP access, and TCP port 443 supports encrypted HTTPS access. Allowing outbound connectivity on these ports enables LiveUpdate to reach the applicable public content servers and retrieve virus definitions, product updates, and related update metadata without being blocked by the organization's perimeter firewall.

In practice, firewall policy should permit outbound connections from the relevant Endpoint Protection clients or the Symantec Endpoint Protection Manager/LiveUpdate source to Symantec's update infrastructure on these ports. The client initiates these sessions, so broad unsolicited inbound firewall rules are not required solely for this purpose. Symantec documentation describes LiveUpdate as using HTTP, HTTPS, or FTP to obtain updates and recommends ensuring that network security controls and proxy configuration permit that communication. See Symantec's network port requirements guidance and the Endpoint Protection content-update documentation.

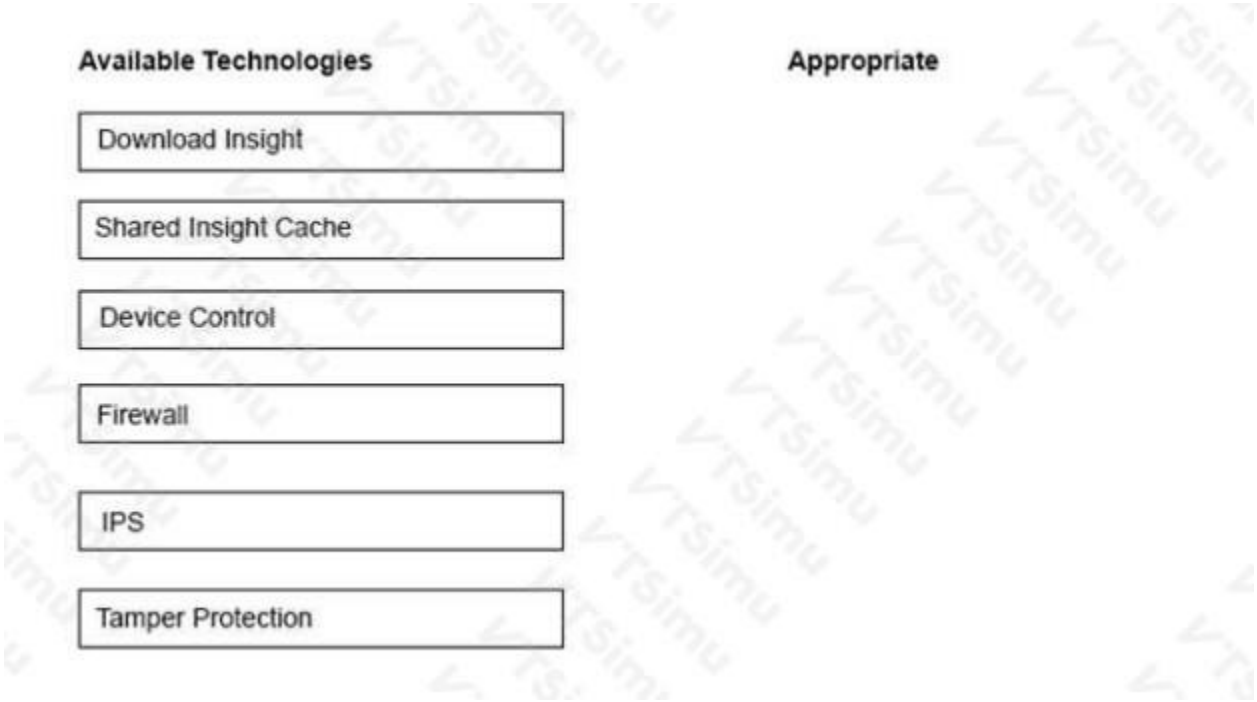
QUESTION NO: 12 - (DRAG DROP)

DRAG DROP

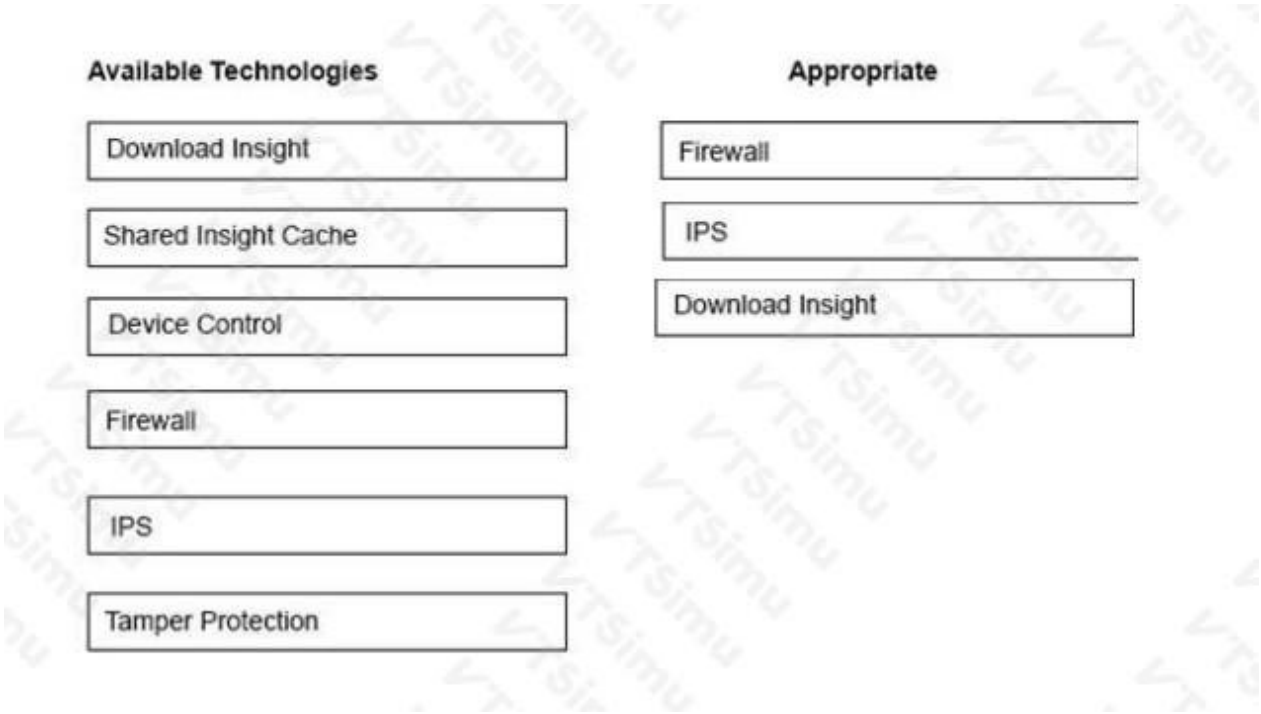
An administrator is unknowingly trying to connect to a malicious website and download a known threat within a .rar file. All Symantec Endpoint Protection technologies are installed on the client's system.

Drag and drop the technologies to the right side of the screen in the sequence necessary to block or detect the malicious file.

Select and Place:



ANSWER:



Explanation:

The appropriate protection sequence is Firewall, followed by IPS, followed by Download Insight. The process begins when the endpoint attempts to establish network communication with the website. Firewall is the first relevant protection layer because it applies the endpoint's network communication rules as traffic is initiated and received. This gives the client an opportunity to enforce the organization's network-access policy at the connection stage.

After the connection and web traffic are being processed, IPS provides network-threat inspection. SEP's intrusion-prevention capability examines network traffic for attack activity and malicious patterns associated with known threats. In a web-download scenario, this is the layer that can recognize and stop hostile traffic or exploitation attempts encountered while the client is communicating with the site. Broadcom's Endpoint Protection documentation describes Network Threat Protection as the component containing the firewall and intrusion-prevention protections; see the Symantec Endpoint Protection documentation portal.

If the download proceeds far enough for the archive to reach the endpoint, Download Insight is the next applicable technology. Download Insight evaluates downloaded executable content using reputation information and prevalence data, allowing the client to identify a known malicious download before the user can safely rely on it. This is especially relevant to a threat delivered in a downloaded archive because the download source and the file's reputation are central to the detection decision. The SEP administration documentation covers reputation-based protection and Download Insight within its Endpoint Protection administration resources. Thus, the displayed ordering follows the path of the event: network connection control, inspection of threatening traffic, and reputation assessment of the downloaded malicious content.

QUESTION NO: 13

A threat was detected by Auto-Protect on a client system.

Which command can an administrator run to determine whether additional threats exist?

A. Restart Client Computer

B. Update Content and Scan

C. Enable Network Threat Protection

D. Enable Download Insight

ANSWER: B

Explanation:

Update Content and Scan is the appropriate command because it first directs the managed endpoint to obtain the latest available protection content and then initiates a scan. A threat detected by Auto-Protect indicates that malicious or suspicious content was encountered during real-time monitoring, but it does not establish whether other files, locations, or dormant items on the endpoint are also affected. Running a scan after updating definitions provides a broader assessment of the client using current detection intelligence.

In Symantec Endpoint Protection Manager, this command is useful as an immediate administrative response for a client where a detection warrants further investigation. The content update is important because newly released definitions, reputation data, and other protection content can improve the scan's ability to identify related or newly recognized threats. The resulting scan status and detections can then be reviewed from the management console to determine the scope of remediation needed on that endpoint. Symantec documents client-command administration and scanning as part of Endpoint Protection management in the Broadcom Symantec Endpoint Protection documentation and its Endpoint Protection knowledge base.

QUESTION NO: 14

Which feature reduces the impact of Auto-Protect on a virtual client guest operating system?

A. Network Shared Insight Cache

B. Scan Randomization

C. Virtual Shared Insight Cache

D. Virtual Image Exception

ANSWER: D

Explanation:

Virtual Image Exception is correct because it is specifically designed to reduce Auto-Protect processing on virtual guest operating systems that were deployed from a common, trusted base image. In a virtual desktop infrastructure, many guest machines share identical operating-system and application files. Without a virtualization-aware exception, each guest can repeatedly scan those same unchanged base-image files, consuming processor, disk, and storage resources.

Virtual Image Exception identifies files that belong to the trusted virtual image and lets Symantec Endpoint Protection avoid unnecessary Auto-Protect scans of those files. This reduces the endpoint security client's performance impact while retaining protection for files that are not part of the approved base image, such as user-created, modified, or newly introduced content. The feature is therefore particularly useful where many virtual clients are started, updated, or scanned at similar times. Symantec's documentation describes Virtual Image Exception as a mechanism for minimizing scan activity and resource consumption associated with virtual images. See the official Symantec article, TECH172218: Virtual Image Exception, for configuration and operational guidance.

QUESTION NO: 15

What type of exceptions could an administrator create from the Symantec Endpoint Protection Manager for a Linux client? (Choose two.)

A. Trusted Web Domain

B. Security Risk Exceptions - File

C. Security Risk Exceptions - Extension

D. Known Risks

E. Security Risk Exceptions - Folder

ANSWER: C E

Explanation:

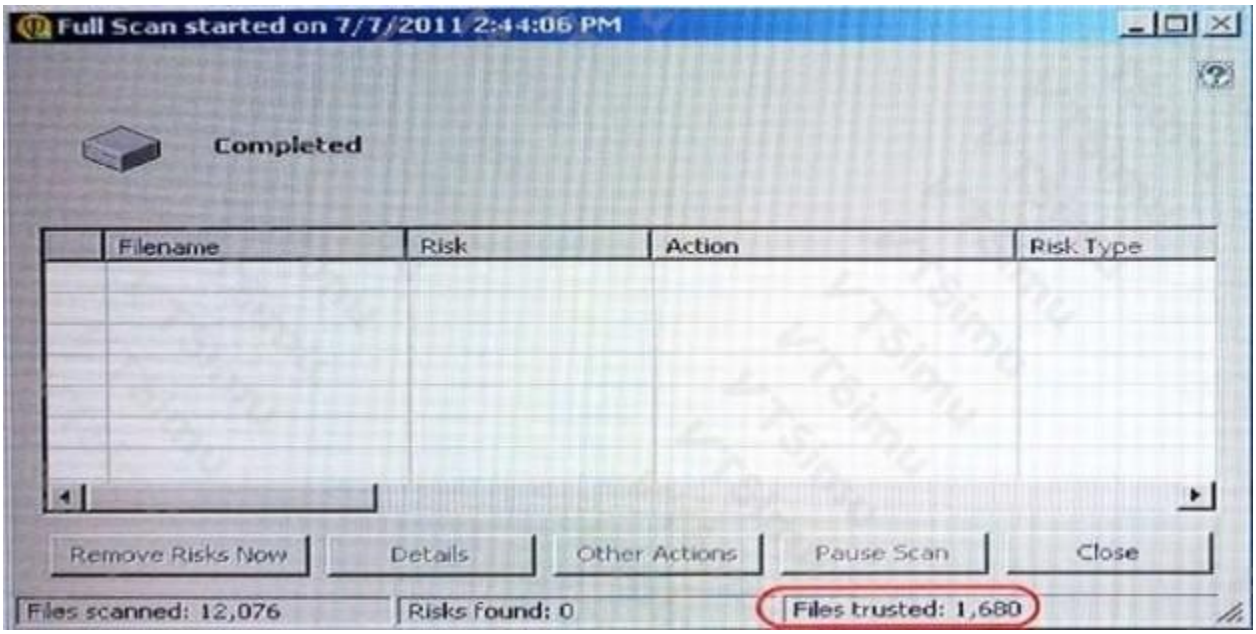
For a managed Linux client, Symantec Endpoint Protection Manager supports centralized security-risk exceptions based on a file extension and on a folder path. **Security Risk Exceptions - Extension** lets an administrator exclude files that match a specified extension from security-risk detection. This is useful when an organization has a known, approved application or workflow that produces files whose extension requires an exception. The exception is defined in the manager and delivered through policy, allowing consistent treatment across the Linux clients assigned to that policy.

Security Risk Exceptions - Folder lets the administrator define a directory location whose contents require exclusion. It is appropriate when an approved product, service, or operational process uses a designated directory for files that should not be evaluated as security risks. Central management is important because it makes the exception auditable, repeatable, and scoped through the relevant client group and policy assignment rather than relying on separately configured local-client settings.

Symantec's exception documentation identifies the exception types available by client platform, including the Linux-supported extension and folder security-risk exception types. Administrators should keep exclusions as narrow as possible and review them regularly to maintain effective endpoint protection. See Symantec support documentation on exception types.

QUESTION NO: 16

Which settings can impact the Files trusted count?



A. System Lockdown Whitelist in the Application and Device Control Policy

B. File Cache settings in the Virus and Spyware Protection policy

C. Insight settings in the Virus and Spyware Protection policy

D. SONAR settings in the Virus and Spyware Protection policy

ANSWER: C

Explanation:

Insight settings in the Virus and Spyware Protection policy can impact the Files trusted count because Insight is the Endpoint Protection reputation technology that evaluates files using community prevalence, age, source, and reputation information. When a file is determined to have a sufficiently trustworthy reputation, the client can classify it as trusted. The Files trusted value therefore reflects files that the client has identified and treated as trusted through this reputation-based process.

Administrators influence this behavior through the Insight configuration within the Virus and Spyware Protection policy, including the level at which reputation information is used to make trust decisions and the handling of files whose reputation is known. Changes to these settings can alter how many files qualify for trusted status on managed endpoints, which in turn affects the displayed count. This is distinct from ordinary scan-caching behavior: the meaningful relationship is that Insight supplies the reputation assessment on which the trusted-file classification is based.

Broadcom's Endpoint Protection documentation describes Insight as the component that uses file-reputation data to identify trusted and untrusted files. See the Symantec Endpoint Protection documentation and Broadcom's overview of Symantec Insight.

QUESTION NO: 17

Which two methods can an administrator use to deploy the Symantec Endpoint Protection client to Windows computers? (Select two.)

A. Client Deployment Wizard

B. Third-party software distribution

C. SEPM database replication

D. LiveUpdate Administrator

E. Risk Tracer

ANSWER: A B

Explanation:

Client Deployment Wizard and **third-party software distribution** are supported deployment methods. The Client Deployment Wizard can push the SEP client remotely to eligible Windows computers that meet the required network and credential prerequisites. It is useful when an administrator needs to deploy directly from the SEPM console.

An administrator can also export a client installation package and deploy it through an established third-party software distribution system. This method is appropriate for large-scale deployment or for organizations that use centralized deployment technologies. Broadcom provides client-deployment guidance in the Symantec Endpoint Protection documentation.

QUESTION NO: 18

In which two areas can host groups be used? (Select two.)

A. Locations

B. Download Insight

C. IPS

D. Application and Device Control

E. Firewall

ANSWER: C E

Explanation:

Host groups are reusable definitions of computers or network endpoints, typically organized by IP address, IP range, or hostname. In Symantec Endpoint Protection Manager, they support policy rules that need to identify a source or destination host set rather than applying the rule indiscriminately. **IPS** uses host groups to scope intrusion-prevention exceptions and rule behavior to defined network hosts. This enables administrators to tune IPS handling for specific systems while retaining protection for the rest of the environment. **Firewall** also uses host groups in firewall-rule criteria, such as defining the remote computers to which a rule applies. A single maintained host-group definition can therefore be reused in rules and updated centrally when the relevant systems change. Broadcom's Endpoint Protection documentation describes host groups as policy components used with firewall and intrusion-prevention policy configuration. See the Symantec Endpoint Protection 14.3 documentation and the Broadcom Endpoint Protection knowledge base for product administration guidance.

QUESTION NO: 19

An administrator exports a Windows client installation package from Symantec Endpoint Protection Manager for deployment through a software distribution system.

Which two items are included in the package configuration? (Select two.)

A. Management server communication settings

B. Client group assignment

C. SEPM database administrator password

D. Replication partner credentials

E. Administrator role permissions

ANSWER: A B

Explanation:

Management server communication settings are included so that a newly installed client knows how to contact the appropriate Symantec Endpoint Protection Manager. These settings include the management-server list used by the client after installation.

Client group assignment is also included in the package configuration. The assigned group determines the policies and settings that the client receives after it registers with the manager. This lets administrators deploy different packages to systems that require different policy sets. Client installation package configuration is described in the Broadcom Symantec Endpoint Protection documentation.

QUESTION NO: 20

An administrator plans to use the Client Deployment Wizard to push a Symantec Endpoint Protection client installation to remote Windows computers.

Which two conditions are required for the remote push deployment to succeed? (Select two.)

A. A Windows account with local administrator rights on the target computers

B. Administrative shares available on the target computers

C. A replication partnership with the target computers

D. A Group Update Provider installed on each target computer

E. SQL Server credentials for each target computer

ANSWER: A B

Explanation:

A Windows account with local administrator rights on the target computers is required because the deployment process must be authorized to copy installation files and start the remote installation. A standard user account does not have sufficient rights to perform these operations.

Administrative shares available on the target computers are also required because the remote deployment process uses the Windows administrative-share mechanism to transfer the installation package to the destination computer. If administrative shares are disabled or blocked, the manager cannot copy the installation files needed for the push deployment. Remote deployment requirements are described in the Broadcom Symantec Endpoint Protection documentation.