250-315 Q&As

Administration of Symantec Endpoint Protection 12.1

Pass Symantec 250-315 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/250-315.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec Official Exam Center

QUESTION 1

Which action must a Symantec Endpoint Protection administrator take before creating custom Intrusion Prevention signatures?

A. change the custom signature order

B. create a Custom Intrusion Prevention Signature library

C. define signature variables

D. enable signature logging

Correct Answer: B

QUESTION 2

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

A. Block

B. Active Response

C. Quarantine

D. Log

E. Trace

Correct Answer: AD

QUESTION 3

In Symantec Endpoint Protection 12.1 Enterprise Edition, what happens when the license expires?

A. LiveUpdate stops.

B. Group Update Providers (GUP) stop.

C. Symantec Insight is disabled.

D. Content updates continue.

Correct Answer: D

QUESTION 4

An administrator is designing a new single site Symantec Endpoint Protection environment. Due to perimeter firewall bandwidth restrictions, the design needs to minimize the amount of traffic from content passing through the firewall.

Which source must the administrator avoid using?

A. Symantec Endpoint Protection Manager

B. LiveUpdate Administrator (LUA)

C. Group Update Provider (GUP)

D. Shared Insight Cache (SIC)

Correct Answer: B

QUESTION 5

A company plans to install six Symantec Endpoint Protection Managers (SEPMs) spread evenly across two sites. The administrator needs to direct replication activity to SEPM3 server in Site 1 and SEPM4 in Site 2.

Which two actions should the administrator take to direct replication activity to SEPM3 and SEPM4? (Select two.)

A. Install SEPM3 and SEPM4 after the other SEPMs

B. Install the SQL Server databases on SEPM3 and SEPM4

C. Ensure SEPM3 and SEPM4 are defined as the top priority server in the Site Settings

D. Ensure SEPM3 and SEPM4 are defined as remote servers in the replication partner configuration

E. Install IT Analytics on SEPM3 and SEPM4

Correct Answer: CD

QUESTION 6

An administrator is responsible for the Symantec Endpoint Protection architecture of a large, multi-national company with three regionalized data centers. The administrator needs to collect data from clients; however, the collected data must stay in the local regional data center. Communication between the regional data centers is allowed 20 hours a day.

How should the administrator architect this organization?

A. set up 3 domains

B. set up 3 sites

C. set up 3 locations

D. set up 3 groups

Correct Answer: B

QUESTION 7

An administrator is unable to delete a location. What is the likely cause?

A. The location currently contains clients.

B. Criteria is defined within the location.

C. The administrator has client control enabled.

D. The location is currently assigned as the default location.

Correct Answer: D

QUESTION 8

An administrator is re-adding an existing Replication Partner to the local Symantec Endpoint Protection Manager site.

Which two parameters are required to re-establish this replication partnership? (Select two.)

A. remote server IP Address and port

B. remote site Encryption Password

C. remote site Domain ID

D. remote server Administrator credentials

E. remote SQL database account credentials

Correct Answer: AD

QUESTION 9

A Symantec Endpoint Protection administrator is using System Lockdown in blacklist mode with a file fingerprint list. When testing a client, the administrator notices that at least one of the files on the list is allowed to execute.

What is the likely cause of the problem?

A. The application has been upgraded.

B. The Application and Device Control policy is in test mode.

C. A file exception has been added to the Exceptions policy.

D. The Application and Device Control policy is allowing the file to execute.

Correct Answer: A

QUESTION 10

Which task should an administrator perform to troubleshoot operation of the Symantec Endpoint Protection embedded database?

A. verify that dbsrv11.exe is listening on port 2638

B. check whether the MSSQLSERVER service is running

C. verify the sqlserver.exe service is running on port 1433

D. check the database transaction logs in X:\Program Files\Microsoft SQL server

Correct Answer: A

QUESTION 11

Which two sources can a Macintosh client use to download content? (Select two.)

A. Symantec Endpoint Protection Manager

B. Group Update Provider (GUP)

C. Internal LiveUpdate server

D. Default Management server

E. Symantec LiveUpdate server

Correct Answer: CE

QUESTION 12

Which policy should an administrator modify to enable Virtual Image Exception (VIE) functionality?

A. Host Integrity Policy

B. Virus and Spyware Protection Policy

C. Exceptions Policy

D. Application and Device Control Policy

Correct Answer: B

QUESTION 13

A company has a small number of systems in their Symantec Endpoint Protection Manager (SEPM) group with federal mandates that AntiVirus definitions undergo a two week testing period. After being loaded on the client, the tested virus definitions must remain unchanged on the client systems until the next set of virus definitions have completed testing. All other clients must remain operational on the most recent definition sets. An internal LiveUpdate Server has been considered as too expensive to be a solution for this company.

What should be modified on the SEPM to meet this mandate?

A. The LiveUpdate Settings policy for this group should be modified to use an Explicit Group Update Provider.

B. The LiveUpdate Content policy for this group should be modified to use a specific definition revision.

C. The SEPM site LiveUpdate settings should be modified so the Number of content revisions to keep is set to 1.

D. The SEPM site LiveUpdate settings should be modified so the Number of content revisions to keep is set to 14.

Correct Answer: B

QUESTION 14

Which tool should an administrator use to discover and deploy the Symantec Endpoint Protection client to new computers?

A. Unmanaged Detector

B. Client Deployment Wizard

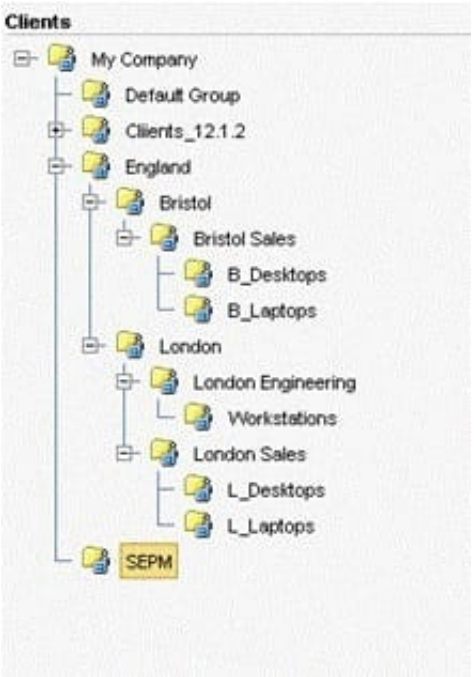
C. Communication Update Package Deployment

D. Symantec Endpoint Discovery Tool

Correct Answer: B

QUESTION 15

Refer to the exhibit.



A manufacturing company runs three shifts at their Bristol Sales office. These employees currently share desktops in the B_Desktops group. The administrators need to apply different policies/configurations for each shift.

Which step should the administrator take in order to implement shift policies after switching the clients to user mode?

A. create three shift policies for the Bristol group

B. create a group for each shift of users in the Bristol group

C. turn on inheritance for all groups in England

D. turn on Active Directory integration

E. modify the B_Desktops policy

Correct Answer: B